

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Обслуговування комп'ютерних систем і мереж»

Група: 4КС-55

Дипломний проект

здобувача освіти денної форми навчання

КС.55.07.000.ДП

**Дяченко Микити
Андрійовича**

**м. Одеса
2022 р.**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: **«Обслуговування комп'ютерних систем і мереж»**

Група: **4КС-55**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Розробка проекту безпеки об'єкту з позиції застосування технічних засобів охорони

Проектний матеріал складається з пояснювальної записки на _____ сторінках та графічного (презентаційного) матеріалу на _____ аркушах (слайдах).

Дипломник _____ (Дяченко М.А.)

Керівник _____ (Стайкуца С.В.)

Консультанти:

з економічної частини _____ (Копайгородська Т.Г.)

з охорони праці _____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Скорнякова О.В.)

До захисту допущений

Голова циклової комісії _____ (Скорнякова О.В.)

Завідувач відділення _____ (Суліма Ю.Ю.)

Захист « ____ » _____ 2022 р.

Протокол ДКК № _____

Оцінка ДКК _____

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення комп'ютерних систем Комісія КТ та Ш
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Обслуговування комп'ютерних систем і мереж»

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР _____

“ _____ ” _____ 2022 р.

ЗАВДАННЯ

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти _____ Дяченко Микиті Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Розробка проекту безпеки об'єкту з позиції застосування технічних засобів охорони

затверджена наказом по коледжу від “30” січня 2021 р. № 306-А2-ОД

2. Термін здачі закінченого проекту (роботи) _____

3. Вихідні данні до проекту (роботи):

Об'єкт дослідження – гіпотетичне підприємство в призмi впровадження ТЗО

Кількість базових складових ТЗО

Основні параметри системи відеоспостереження – глибина архіву, пропускна здатність

Бренд системи відеоспостереження - Dahua

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

ВСТУП.

- 1. ТЕХНОЛОГІЧНИЙ РОЗДІЛ**
- 2. ЕКОНОМІЧНИЙ РОЗДІЛ**
- 3. ОХОРОНА ПРАЦІ**
- 4. ВИСНОВКИ**

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Слайд 1 – Рубежі безпеки сучасного підприємства. Слайд 2 – Базовий склад технічних засобів охорони. Слайд 3 – Системи сигналізації. Слайд 4 – СКУД та системи охорони периметру. Слайд 5 – Проектування систем відеоспостереження. Слайд 6- Впровадження ТЗО. АСПС та АСПГ. Слайд 7 – Система охоронної сигналізації. Слайд 8 – Розрахунок параметрів системи відеоспостереження. Слайд 9 - Система відеоспостереження. Слайд 10 – Вибір ППКП в системах сигналізації. Слайд 11 - Ефективність функціонування ТЗО. Слайд 12 – Висновки

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Вступ, 1	Стайкуца С.В.		
2	Копайгородська Т.Г.		
3	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7. Дата видачі завдання _____

Керівник

(підпис)

Завдання прийняв до виконання

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	Огляд літератури. Огляд існуючих рішень.		
2.	Формування кінцевого завдання на розробку. Вступна частина дипломного проекту.		
3.	Технологічний розділ. Вибір елементної бази.		
4.	Технологічний розділ. Розробка структурної та принципової схеми пристрою.		
5.	Технологічний розділ. Розробка алгоритму та управляючої програми.		
6.	Економічний розділ.		
7.	Виконання розділу «Охорона праці».		
8.	Підготовка доповіді та презентації для захисту		
9.	Підготовка до попереднього захисту, підготовка до захисту		
10.	Отримання рецензії, відповіді на зауваження рецензента		
11.	Захист роботи		

Дипломник

(підпис)

Керівник

(підпис)

ЗМІСТ

ВСТУП	7
1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ	8
1.1 Базові відомості про технічні засоби охорони об'єктів	8
1.1.1 Система охоронно-тривожної сигналізації	9
1.1.2 Автоматизована система пожежної сигналізації	11
1.1.3 Автоматизовані системи пожежогасіння	12
1.1.4 Система відеоспостереження	15
1.1.5 Система контролю і управління доступом	16
1.1.6 Системи охорони периметра	18
1.2 Проектування систем відеоспостереження на об'єктах інформаційної діяльності	23
1.2.1 Етапи проектування	24
1.2.2 Щодо сумісності компонентів системи відеоспостереження	24
1.2.3 Розміщення прикінцевого обладнання систем відеоспостереження	26
1.3 Формування системи захисту підприємства на основі технічних засобів охорони	32
1.3.1 Вихідні дані для впровадження СЗІ на основі ТЗО	32
1.3.2 Впровадження технічних засобів захисту	33
1.3.3 Вибір приймально-контрольних приборів систем сигналізації в аспекті терміну експлуатації	44
1.3.4 Дослідження ефективності функціонування ТЗО	46
2 ЕКОНОМІЧНИЙ РОЗДІЛ	53
3 ОХОРОНА ПРАЦІ	58
ВИСНОВКИ	61
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	62

					КС.55.07.000.ДП ПЗ			
Изм.	Лист	№ докум.	Подпись	Дата				
Розробив	Дяченко М.А.				Розробка проекту безпеки об'єкту з позиції застосування технічних засобів охорони	Лит.	Лист	Листов
Перевірив	Стайкуца С.В.						5	1
Рецензент						ВСП ОТФК ОНТУ АКС-55		
Н. Контр.	Петрашова В.І.							
Затвердив	Скорнякова О.В.							

ВСТУП

Поняття безпеки включає безліч аспектів. В аспекті підприємства безпека може складатися з організаційної, кадрової, юридичної, мережевої, криптографічної, інженерної, стосуватися питань охорони праці та пожежної безпеки тощо. Важливу роль при цьому відіграє і застосування з велінням підвищення безпеки технічних засобів охорони.

Під технічною системою охорони (ТСО) у разі розуміється система раннього виявлення загроз фірмі від стихійних лих, несанкціонованого проникнення порушників і помилкових чи неправомірних дій обслуговуючого персоналу чи клієнтів фірми. При цьому виявлення, а найчастіше нейтралізація і навіть ліквідація загроз здійснюється за допомогою різних технічних засобів (ТС) і методів. Зазвичай до складу технічних засобів охорони (ТЗВ) входять:

1. Система відеоспостереження (відеоконтролю, охоронного телебачення) – СВК, СОТ
2. Система пожежної сигналізації – АСПС
3. Система аварійного оповіщення та управління евакуацією - СОУЕ
4. Система пожежогасіння – АСПГ
5. Система контролю та управління доступом - СКУД
6. Система охоронно-тривожної сигналізації - СОТС чи СОС
7. Система охорони периметра – СОП

На об'єктах малого та середнього масштабів пункти 2 та 3 можуть бути відсутніми. Оптимально, коли є можливість інтегрування на одній платформі кількох підсистем ТСО без необхідності побудови повноцінної та дорогої ІТС – інтегрованої системи безпеки. На сьогодні, наприклад, є такі рішення, орієнтовані на технологічність, масштабованість, простоту монтажу, використання бездротових технологій. Застосування СТО на об'єктах ставить собі просту і зрозумілу мету – виявити нарушителя на ранніх етапах, створювати йому кожному з рубежів затримку у часі, інформувати мобственника і служби безпеки оперативно на момент виявлення інциденту. ТСО є важливим та ефективним компонентом у складі загальної структури безпеки об'єкта.

					КС.55.07.000.ДП ПЗ	Лист
						7
Изм.	Лист.	№ докум.	Подп.	Дата		

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Базові відомості про технічні засоби охорони об'єктів

Поняття безпеки включає в себе не тільки захист від кримінальних посягань, але ще більшою мірою створення запобіжних заходів забезпечення захисту від пожежі, вибуху та інших надзвичайних подій. Тому для охорони об'єктів використовують різноманітні системи захисту, які наведені у рис. 1.1.

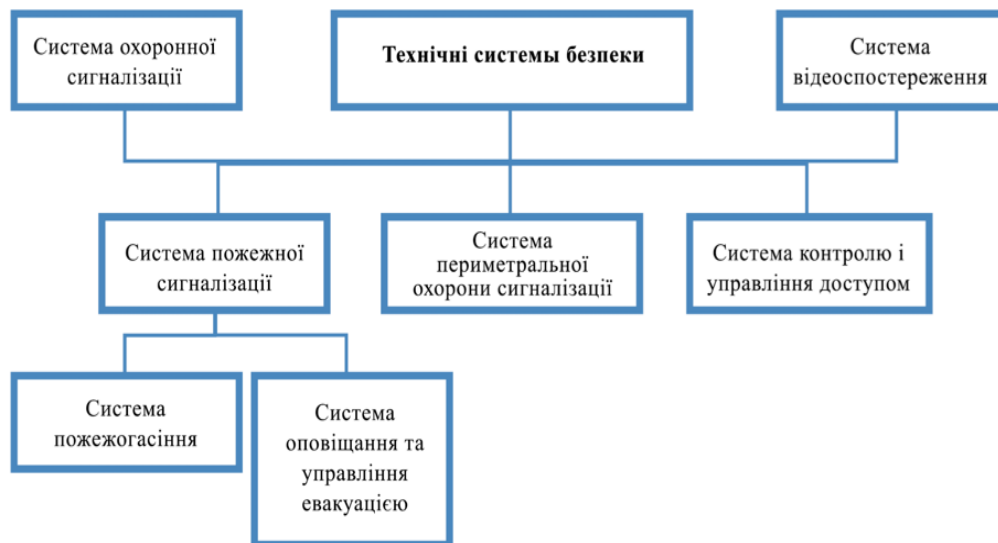


Рисунок 1.1 - Технічні системи безпеки

Технічні засоби охорони - це сукупність апаратних і програмних засобів, що забезпечують контроль, збереження та протипожежну безпеку території, приміщень, сховища та ін. об'єктів і суб'єктів контролю.

Вони включають: периметрові та об'єктові засоби виявлення, технічні засоби попередження і впливу, апаратуру збору і обробки інформації, засоби управління (контролю) доступом на об'єкт, технічні засоби спостереження, системи електроживлення, кабельні та проводові лінії, засоби зв'язку системи охорони об'єктів, а також засоби забезпечення експлуатації технічних засобів охорони. Розглянемо більш детально базовий склад і класифікацію технічних засобів охорони.

1.1.1 Система охоронно-тривожної сигналізації

Основне завдання охоронної сигналізації полягає у визначенні факту несанкціонованого проникнення на територію, що охороняється, і активація попереджувальних пристроїв (сирена, маячок) або сповіщення власника і центру спостереження (наприклад, позавідомчої охорони).

Загальні елементи систем тривожної сигналізації наведено на рис. 1.2 [2]



Рисунок 1.2 – Загальні елементи систем тривожної сигналізації

Основним елементом системи є сповіщувач. Вибір сповіщувача для блокування елементу приміщення проводиться відповідно до обраною моделлю порушника і вимогами, що пред'являються до приміщення (банк, магазин, кімната зберігання зброї та ін.)

Система охоронної сигналізації, як правило, складається з трьох основних частин:

- сповіщувач;
- охоронний датчик (сенсорний пристрій);
- приймально-контрольний прилад;
- радіоканальний пристрій;
- контрольна панель.

Система охоронної сигналізації виконує завдання своєчасного сповіщення служби охорони про факт вторгнення або спробу проникнення людей в будівлю або його окремі приміщення з фіксацією дати, часу і місця порушення. Загальна структура охоронної сигналізації представлена на рис. 1.3.



Рисунок 1.3 – Структурна схема охоронної сигналізації

Датчик представляє собою чутливий елемент, що перетворює контрольований параметр в електричний сигнал. Особливість датчиків полягає в тому, що вони реєструють, в основному, неелектричні величини. Вимір неелектричних величин – складне завдання й при цьому датчики повинні забезпечувати високу надійність і вірогідність контролю. Надійність датчиків забезпечується, в основному, цифровими методами обробки сигналів.

Датчики поєднуються в зони. Під зоною мається на увазі один або кілька датчиків, що охороняють певний об'єкт або ділянку об'єкта. В системах охоронної сигналізації використовуються датчики наступних типів:

- пасивні інфрачервоні датчики руху;
- датчики розбиття скла;
- активні інфрачервоні датчики руху й присутності;
- фотоелектричні датчики;
- мікрохвильові датчики; ультразвукові датчики;

- вібраційні датчики;
- датчики температури; датчики наявності пар і газів;
- магнітні датчики;
- шлейфи.

По взаємодії з загрозою ці системи поділяються на пасивні та активні. Дія пасивних спрямована на привернення уваги власника майна або охоронних служб, а активні призначені для запобігання проникнення на об'єкт.

1.1.2 Автоматизована система пожежної сигналізації

Стан безпеки підприємства, об'єднання підприємств, окремої галузі визначає система управління - спосіб організації (встановлення і підтримання порядку взаємодії) майна, матеріалів, праці і капіталу в процесі виробництва (бізнесу).

Враховуючи, що однією з найважливіших складових загальної безпеки будь-якого сучасного об'єкту є його надійний захист від пожеж, то і система управління пожежною безпекою має посісти відповідне місце у сфері загального управління.

Пожежна сигналізація – це сукупність технічних засобів, призначених для виявлення пожежі, обробки та надання в заданому вигляді повідомлення про пожежу на об'єкті, що захищається, для видачі команд на включення автоматичних установок пожежогасіння та управління іншими технічними засобами.

В склад будь-якої установки пожежної сигналізації входять пожежні сповіщувачі, приймально-контрольні прилади, світлові і звукові оповіщувачі, технічні засоби передачі інформації до пультів централізованого спостереження, пультів зв'язку пожежних частин та інше.

При плануванні та побудові пожежної сигналізації необхідно враховувати велику кількість чинників. Уявлення оператора, який проводить проектно-пошукові роботи з проектування автоматичного протипожежного захисту, повинні співпадати з вимогами відповідних регіональних контролюючих

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		11

органів, нормативних документів, відомчих норм і рекомендацій. На рис. 1.4 зображено загальну схему системи пожежної сигналізації.



Рисунок 1.4 – Загальна схема системи пожежної сигналізації

Площу, що підлягає захисту, потрібно визначати разом з фахівцем підприємства, виходячи з характеру експлуатації будівлі.

У процесі обстеження об'єкта захисту необхідно встановити, в яких частинах об'єкту існує підвищена небезпека для людей і майна, і визначити, які заходи повинні бути прийняті для запобігання небезпеки та попередження людей про пожежу, а також захисту людей від небезпечних факторів пожежі.

1.1.3 Автоматизовані системи пожежогасіння

Існує декілька видів класифікації автоматичних установок, або комплексів пожежогасіння : по виду вогнегасної речовини (вода, газ, порошок, аерозоль), за способом гасіння (за об'ємом або по поверхні), за способом організації (модульні або централізовані), за способом керування (автономні або комплексні) і ін. Обмежимося в нашій роботі розглядом лише найбільш поширених типів установок, що часто зустрічаються. На рис. 1.5 представлена загальна класифікація систем пожежогасіння.

Система пожежогасіння повинна виконувати усього дві функції:

- забезпечення збереження життя та здоров'я людей;
- забезпечення збереження матеріальних цінностей.



Рисунок 1.5 – Загальна класифікація систем пожежогасіння.

Проте, існуючі типи систем пожежогасіння виконують вказані вище функції з різною ефективністю, що зображено в табл.1.1

В якості вогнегасної речовини в газових установках застосовується зріджений або стислий газ, який зберігається в спеціальних ізотермічних ємкостях чи балонах. Фізичний принцип гасіння в таких установках заснований на витісненні кисню важчим газом, що не підтримує горіння. В цьому випадку гасіння відбувається або локально за об'ємом, або за усім обсягом приміщення.

Таблиця 1.1 – Ефективність систем пожежогасіння

Тип системи пожежогасіння	Забезпечення збереження життя та здоров'я людей	Забезпечення збереження матеріальних цінностей
Водяне	так	ні
Пінне	ні	ні
Газове	ні	так
Порошкове	ні	ні
Аерозольне	ні	ні
Тонко-розпилена вода	так	так

Як правило, такий спосіб гасіння застосовується для захисту приміщень певних категорій, що мають достатню міру герметичності і, найголовніше, з обмеженим перебуванням людей. Робота газової установки в автоматичному режимі повинна унеможливлювати випуску вогнегасної речовини у разі

присутності в приміщенні людей, при цьому робота самої установки в тривожному режимі повинна супроводжуватися звуковою і світловою сигналізацією, що змушує людей покинути приміщення.

Головною перевагою газового гасіння є повна відсутність матеріального збитку. Недоліками газового гасіння є висока вартість вогнегасного газу і небезпека для здоров'я людини. В той же час головним його достоїнством є повна відсутність матеріального збитку предметам і устаткуванню, що знаходиться в приміщенні. Для ліквідації наслідків гасіння досить простого провітрювання.

Наступною по поширеності категорією установок є установки порошкового гасіння. Ці установки можуть використовуватися для локального або централізованого гасіння, а також в приміщеннях з присутністю людей, оскільки вживаний в них порошок нетоксичний і не може завдати прямої шкоди здоров'ю людини. Фізичний принцип гасіння полягає в утворенні порошкової хмари, яке накриває певну площу приміщення, що захищається. При цьому частки порошку охолоджують поверхню, а газоподібні продукти його термічного розкладання розбавляють горюче середовище, перешкоджаючи розвитку пожежі. Крім того, утворення порошкової хмари у вузьких проходах або каналах має певний вогнестримувальний ефект. У централізованих (чи агрегатних) установках порошок зберігається в загальній місткості, а кількість порошку, що подається в загальний колектор, визначається площею приміщення. Кількість порошкових модулів і їх тип визначаються площею і особливостями приміщення, що захищається, а також способом їх кріплення.

Перевагами порошкових установок перед газовими є: нижча вартість, менший час відновлення і відносна безпека для людей. Недоліком – досить велика трудомісткість прибирання після спрацьовування установки.

Останніми розглянемо установки водяного пожежогасіння. Історично склалося так, що системи водяного пожежогасіння набули найбільш широкого поширення. Вода - найдешевша і безпечніша анти пожежна речовина, що дозволяє ефективно захищати об'єкти, для яких характерне велике скупчення

					КС.55.07.000.ДП ПЗ	Лист
						14
Изм.	Лист.	№ докум.	Подп.	Дата		

людей,; торговельні центри, офісні приміщення, готелі. Як протипожежна речовина, вода не представляє безпосередній небезпеки для людини і інших живих істот. Системи водяного пожежогасіння застосовуються також для захисту відкритих (негерметичних) об'єктів, таких як багаторівневі автостоянки, гаражі, бокси, де системи газового і порошкового пожежогасіння виявляються малоефективними.

Системи водяного пожежогасіння, як і газового, можуть подавати вогнегасну речовину локально до місця займання (спринклерна секція) або робити гасіння по загальній площі простору (дренчерна секція), що захищається. Спринклери розкриваються локально, при спрацьовуванні температурного замку над місцем можливого займання. Дренчерні секції складаються з набору відкритих зрошувачів. Подача вогнегасної речовини в них здійснюється при відкритті загального електромагнітного клапана, керованого приймально-контрольним приладом системи пожежної сигналізації. У шлейфи такого приладу підключаються пожежні сповіщувачі, при спрацьовуванні яких формується команда "Управління клапаном".

1.1.4 Система відеоспостереження

Цілями систем відеоспостереження можуть бути:

- фіксація тривожних ситуацій;
- попередження неправомірних дій;
- виявлення та розслідування злочинів;
- контроль персоналу;
- візуальний контроль периметрів і площі об'єкту.

Системи здатні вирішувати наступні завдання:

- приймають і передають відеосигнали за допомогою прямих з'єднань радіочастотним кабелем, локальної комп'ютерної мережі, інтернету, телефонних ліній або радіоканалів від всіх відеокамер, встановлених на об'єкті;

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		15

- забезпечують відеозапис безперервно, за розкладом і/або на основі сигналів з датчиків руху, зміни обсягу і будь-яких інших детекторів охоронної та пожежної підсистем, СКУД, по команді оператора;
- дають можливість перегляду зображення на будь-якому з вхідних в систему дисплеїв від будь-якої встановленої відеокамери або від декількох одночасно (мультиекранний режим);
- циклічно архівують зображення від всіх телекамер з інтервалом автоматичного поновлення відеозапису від 1 дня до декількох місяців;
- здійснюють збільшення обраних зображень або їх фрагментів, швидкий пошук потрібних фрагментів запису за часом, роздруківку окремих кадрів; виробляють самотестування окремих компонентів і всієї системи в цілому на декількох рівнях самоконтролю;
- надають можливість повного віддаленого контролю і управління системою.

Деякі типи камер мають технологію відеоаналітики, для спостереження, розпізнавання об'єктів та людей, прогнозування.

Самі відеокамери за місцем монтажу розподіляються на вуличні та внутрішні. Вуличні камери мають захист від різних погодних умов, антивандальні механізми захисту, інфрачервону підсвітку а також можуть мати велику дальність обзору та зазвичай більше внутрішніх. Внутрішні вже не мають такого захисту та розмірів як зовнішні але мають необхідні функції для виконання поставлених задач. Також за способом передачі їх можна поділити на провідні та бездротові.

1.1.5 Система контролю і управління доступом

Системою контролю і управління доступом (СКУД) називають сукупність програмно-технічних засобів і організаційно-методичних заходів, за допомогою яких чоловік може вирішувати завдання контролю відвідування співробітниками окремих приміщень, управління цим процесом, оперативного контролю переміщення персоналу і за часом його знаходження на території об'єкту. СКУД

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		16

не лише апаратура і програмне забезпечення, це продумана система управління руху персоналу.

Традиційні методи ідентифікації особистості, в основі яких перебувають різні ідентифікаційні карти, ключі або унікальні дані, такі як, наприклад, пароль не є надійними в тім ступені, що потрібно на сьогоднішній день. Природним кроком у підвищенні надійності ідентифікаторів стали спроби використання біометричних технологій для систем безпеки.

- забезпечувати контроль доступу і управління ним на різних типах контрольно-перепускних пунктів (людських, автомобільних, з/д);
- захищати від провезення в ті або інші місця заборонених предметів (зброї, вибухових речовин, матеріалів, що діляться, і т. п.);
- затримувати потенційних порушників;
- підтримувати різні способи посвідчення осіб, що проходять, у тому числі біометричні;
- мати відкриту для цілей інтеграції програмно-апаратну платформу;
- мати високі адаптивні властивості;
- забезпечувати автоматизацію процесів керування службами безпеки об'єкту і координацію їх діяльності;
- функціонувати в умовах поразки компонентів системи і в інших надзвичайних ситуаціях.

До основних технічних характеристик відносяться:

- рівень ідентифікації;
- кількість контрольованих місць;
- пропускна спроможність;
- кількість користувачів.

Основні компоненти системи контролю та керування доступу:

- ідентифікатор - ідентифікатор, або ключ, служить для визначення прав володіє їм людини. У ролі ключа може виступу «далласовская таблетка», безконтактна картка або брелок, карта з магнітною смугою і т.п. Ідентифікатором може бути також і код, що набирається на клавіатурі, і ряд

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		17

біометричних ознак людини - відбиток пальця, малюнок сітківки або веселкової оболонки ока, тривимірне зображення обличчя;

– контролер обладнання, що зберігає у своїй пам'яті коди ідентифікаторів зі списком прав кожного з них, приймає рішення, пропустити чи ні даної людини в дану двері. Коли ви пред'являєте ідентифікатор, лічений з нього код порівнюється з зберігаються в пам'яті, на підставі чого приймається рішення про те, відкрити двері або ворота, або не відкривати;

– зчитувач - це пристрій, який вміє отримати код ідентифікатора і передати його контролеру. Залежно від принципів роботи ідентифікатора змінюється і технологія зчитування коду. Найбільш стійкими характеристиками можуть володіти зчитувачі безконтактних карт. Такі пристрої дозволяють розпізнавати персональний код доступу при піднесенні ідентифікатора до зчитувача на певну відстань;

– замки - якщо завдання СКУД полягає в обмеженні проходу через звичайні двері, то виконавчим пристроєм буде електричний керований замок або клямка;

– турнікети - турнікети бувають двох основних типів: поясні й повноростові. При правильному налаштуванні всієї системи турнікет дозволяє пропустити по одній карті тільки однієї людини. Повноростовий турнікет дорожче поясного, однак, його не можна перестрибнути.

1.1.6 Системи охорони периметра

Система охорони периметра ефективно працює тоді, коли до її розробки, підбору та встановлення підійти з розумом і тверезим розрахунком. Технологічні процеси, що забезпечують безпеку об'єктів, постійно удосконалюються, а апаратура, яка реалізує їх, стає все більш складною, розгалуженою і багатофункціональною, що представляє собою широкий комплекс різноманітних технічних засобів. Тому все більш актуальною стає задача передачі частини функцій, які виконуються оператором, технічним засобам. Ступінь такого перерозподілу визначається конкретними умовами, але повинна збільшуватися в

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		18

міру ускладнення як структури всього технологічного комплексу безпеки в цілому, так і локальних технічних засобів.

Граничним випадком є повна автоматизація, коли управління ходом процесу здійснюється без втручання людини. Однак, в реальних умовах застосування технічних засобів охорони, існує потреба залишити право прийняття найбільш відповідальних рішень по ліквідації загроз і аварійних ситуацій за оператором системи технічних засобів охорони.

Охорона периметра грає важливу роль в ТЗО. Так, системи охорони периметру виступають першим рубежем при формуванні системи безпеки. Саме на СОП покладається першочергове завдання по виявленню порушника. Крім того, використання систем охорони периметра спільно з іншими системами охорони (наприклад, системами відеоспостереження), дозволяє істотно підвищити ефективність охоронної системи та ймовірність виявлення зловмисника.

Система охорони периметра може складатися з підсистем зображених на рис 1.6.

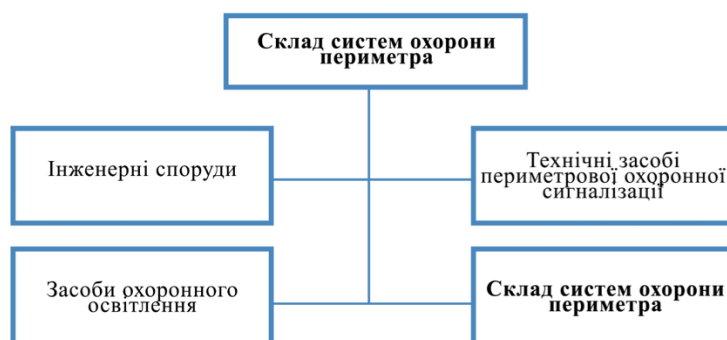


Рисунок 1.6 – Склад систем охорони периметра

Інженерні споруди використовують для сповільнення зловмисника та ускладнення перетину периметра (загородження, протитаранні пристрої, контрольно-пропускні пункти, ворота, протипідкопні конструкції).

До засобів периметрової сигналізації відносяться різноманітні датчики, які використовують для інформування про зловмисника.

Засоби охоронного освітлення забезпечують спроможністю оглядати периметр у нічний час.

А засоби охоронного сповіщення представляють собою гучномовці, сирени, звукову сигналізацію.

В основі розробки різних СЗ і організації її функціонування лежить принцип створення замкнутих, послідовних рубежів, що починаються за межами контрольованої зони і концентрично стягуються до особливо важливих приміщень.

На кожному рубежі загрози порушення безпеки повинні бути виявлені та, за можливістю, ліквідовані. В разі, коли ліквідація загрози неможлива, потрібно на максимальний час затримати порушника та задіяти щодо перешкоджання загрозам наступні рубежі безпеки. Основу планування і обладнання контрольованих зон (організованих рубежами) складають принципи рівнопотужності і комплексності.

Використання рубіжної СЗ обумовлено тим, що система дозволяє забезпечити належний рівень безпеки: при наявності широкого спектру різнорідних загроз (від тероризму до витончених спроб проникнення в обчислювальну систему); при використанні різних технологій обробки інформації шляхом глобального контролю; за критерієм оптимального розподілу ресурсів СЗ з урахуванням пріоритету загрози.

Слід зазначити, що чим складніше захист кожного рубежу, тим більше часу буде потрібно зловмиснику для його подолання і тим імовірніше буде його виявлення. З цього випливає, що захист кожного рубежу повинен взаємно доповнювати один одного. Тоді ефективність всієї системи захисту буде оцінюватися як мінімальний час, який зловмисник повинен затратити на подолання всіх її рубежів. За цей час (безпечне час) він повинен бути виявлений і знешкоджений співробітниками служби охорони.

Основу планування та обладнання зон (рубежів) безпеки становить принцип рівномірності їх кордонів. Якщо при обладнанні зони (рубежу) 2 (периметр будівлі) на одному з вікон першого поверху не буде металевих ґрат

					КС.55.07.000.ДП ПЗ	Лист
						20
Изм.	Лист.	№ докум.	Подп.	Дата		

або їх конструкція ненадійна, то міцність і надійність інших ґрат на вікнах цього поверху не має ніякого значення - зона буде досить легко і швидко подолана зловмисниками через незахищене (або слабкозахищене) вікно.

Розглянемо кожен рубіж окремо, отже:

Рубіж 1 – Периметр території

Периметр – перший і найбільш відповідальний рубіж охорони. Захист периметра території об'єкта є комплексним завданням. Його ефективне рішення можливе при оптимальному поєднанні механічних перешкод, що ускладнюють і уповільнюють дії порушника, із засобами сигналізації, що забезпечують найбільш раннє виявлення факту проникнення, системами відображення і додатковими засобами.

Основне завдання охорони периметра території: Виявити порушника під час підходу і подолання лінії периметра та локалізувати (знешкодити) порушника до того, як його дії зможуть завдати шкоди об'єкту, що охороняється.

Рубіж 2 – периметр будівлі

Периметр будівлі можна віднести так само до найбільш відповідального рубежу захисту. Проникнувши в будинок, зловмисник підвищує свої можливості нанесення шкоди об'єкту і особам, які знаходяться всередині. Завданням охорони периметра будівлі є недопущення зловмисника в середину приміщення для недопущення нанесення шкоди об'єкту.

Рубіж 3 – прийом відвідувачів

Приміщення використовується відвідувачами (клієнтами) об'єкта. Завданням таких приміщень є контроль відвідувачів, їх ідентифікація та аутентифікація. Тут можуть як надати так і відмовити суб'єкту в допуску до тієї чи іншої інформації або відвідуванні співробітника підприємства.

Рубіж 4 – службові приміщення

Службове приміщення - це приміщення, які найчастіше закриті для сторонніх осіб, що не є співробітниками підприємств. Доступ залежить від класу приміщення, грифу інформації, наявності матеріальних цінностей тощо. Через

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		21

службові приміщення можуть проходити шляхи проникнення до головної мети порушника.

Рубіж 5 – особливо важливі приміщення

Особливо важливі приміщення - це приміщення, які можуть бути метою порушника. До таких приміщення відносяться переговорні, кабінети осіб керівних посад. В таких приміщеннях можливе встановлення закладних пристроїв, що може завдати підприємству репутаційної, матеріальної або фізичний шкоди. У подальшому це може призвести до великих проблем, тривалого терміну відновлення інформаційних систем, репутації суб'єктів і об'єктів, стану здоров'ю співробітників.

Рубіж 6 – сховища

Сховища є метою зловмисника при проникненні його на об'єкт. Сховищем можна назвати сервера, реєстратори, склади, сейфи, особливо важливі приміщення (кабінети керівних осіб). Це останній рубіж охорони, який може зіграти важливу роль в запобіганні нанесенні зловмисником шкоди об'єкту або суб'єкту знаходиться на ньому. Візуалізація рубежів безпеки наведена на рис. 1.7.

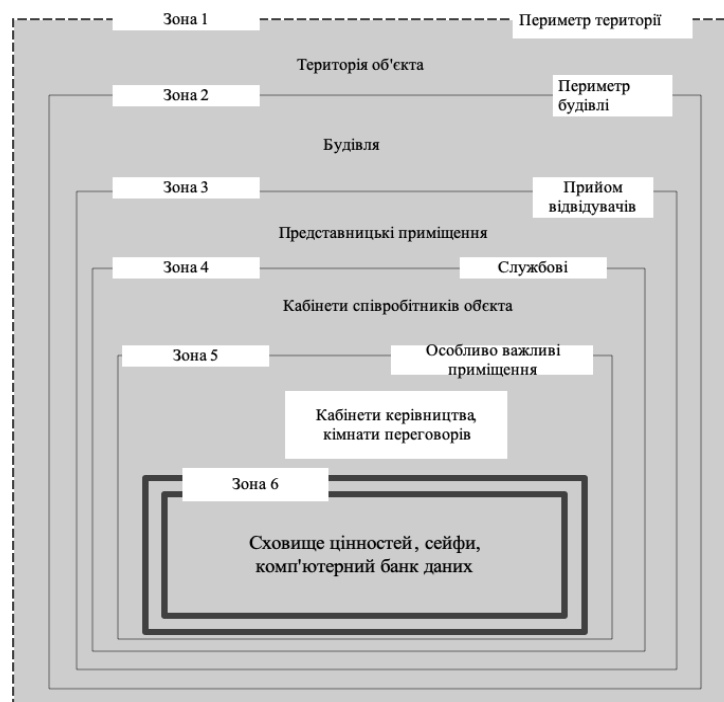


Рисунок 1.7 – Візуалізація рубежів і зон безпеки

Можливість порушника знайти маршрут, що не блокований системою охорони, повинна бути виключена. Для запобігання проходу порушника повинні бути блоковані всі можливі маршрути руху порушника. Стан фізичних перешкод, що мають велику стійкість і в зв'язку з цим не блокованих системами, повинно періодично контролюватися патрулями з особового складу охорони або з використанням телевізійних засобів спостереження.

З метою підвищення стійкості рубежів охорони до подолання вони повинні бути обладнані системами охорони, що працюють на різних фізичних принципах дії (радіохвильові, ІК, сейсмічні). Комбінування даних систем повинно проводитися за схемою М з N. Наприклад, при $M = 2$, $N = 3$, якщо спрацювали не менше двох з трьох встановлених систем, то приймається рішення про видачу сигналу "Тривога". Числа М і N визначаються в ході проектування КТСО індивідуально для кожного рубежу охорони об'єкта. [4]

1.2 Проектування систем відеоспостереження на об'єктах інформаційної діяльності

Однією з особливостей систем охоронного телебачення виявляється унікальність побудови і реалізації практично кожної проектованої відеосистеми. Поза сумнівом, що в різних реалізаціях систем охоронного телебачення є багато схожого (і що навіть повторюється), та все ж кожне нове технічне завдання (ТЗ) - це інша конфігурація, інші кути огляду відеокамер, інша освітленість об'єкту, інші рівні сигналів і перешкод і тому подібне, інакше кажучи, це нова відеосистема.

Проектування системи охоронного телебачення включає:

- розробку концепції безпеки об'єкту з твердженням сценарію дій охорони в різних ситуаціях і утвердженням ТЗ;
- первинний вибір конфігурації системи охоронного телебачення відповідно до вимог ТЗ;
- підбір необхідного відеоустаткування і аксесуарів з використанням каталогів і прайс-листів компаній;

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		23

– вибір варіанту підключення приладів і коригування конфігурації відеосистеми відповідно до параметрів реально існуючого на ринку систем безпеки устаткування (наприклад, з урахуванням числа відеовходів у приладів обробки відеосигналів або відеореєстрації).

1.2.1 Етапи проектування

Проектування системи охоронного телебачення складається з декількох етапів:

1. Визначення параметрів периферійного устаткування, в першу чергу, кількості і місць розміщення відеокамер, їх орієнтації в просторі, вибору об'єктивів;

2. Визначення кількості постів охорони, одержуючих візуальну інформацію відносно обстановки на об'єкті у зв'язку з їх повноваженнями і пріоритетами;

3. Вибір складу устаткування для постів охорони, здатного в результаті його оптимальної конфігурації вирішувати завдання визначувані концепцією безпеки об'єкту;

4. Рішення завдань передачі сигналів від відеокамер на пости охорони;

5. Вибір допоміжного устаткування.

Найменш вивченими нині являються питання оптимізації розташування відеокамер, вибір їх об'єктивів, оскільки саме ці параметри визначають потрібну дозволяючу здатність конкретної системи охоронного телебачення і швидкість оновлення візуальної інформації при рішенні цієї задачі. Точність розрахунків, а також облік тих, що становлять похибку визначають точність вибору устаткування, витратних матеріалів і правила виконання монтажу.

1.2.2 Щодо сумісності компонентів системи відеоспостереження

В системі відеоспостереження, як правило, використовується обладнання різних виробників. Щоб з різних приладів, як з кубиків, створити єдину, функціонально закінчену і надійно працюючу відеосистему, усі її составні

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		24

частини повинні обладати наступними видами сумісності – конструктивною, електричною, інформаційною. Конструктивна сумісність визначається габаритними, установочними і приєднувальними розмірами. Електрична сумісність різних приладів відеосистем припускає, зокрема, що їх вхідні і вихідні відеосигнали повинні мати стандартний вигляд: повний телевізійний сигнал розмахом $1\text{ В} \pm 0,2\text{ В}$ на навантаженні 75 Ом . Крім того, важливо, щоб розмах синхроімпульсів був $0,3\text{ В}$, а їх вершина плоскої, без викидів. Інформаційна сумісність визначається протоколами передачі даних, форматами представлення інформації і тому подібне. Відсутність єдиного стандарту в цій області приводить, до того, що приймачі сигналів телекерування виробництва деяких фірм можуть управлятися тільки у разі використання клавіатур того ж виробника.

На етапі проектування повинна закладатися можливість розширення і модернізації системи охоронного телебачення, котра багато в чому також визначається сумісністю використаного устаткування.

Реальне проектування системи охоронного телебачення слід розпочинати з вибору кількості відеокамер і місць розміщення їх на об'єкті, що охороняється. Варіантів рішень цієї задачі може бути досить багато, вони відрізняються і об'ємом використаного устаткування, і ціною. Зазвичай в цьому випадку говорять про необхідну достатність, оскільки з одного боку кількість відеокамер однозначно впливає на вартість системи охоронного телебачення, а з іншого боку, їх кількість має бути не менше того, яке потрібне для забезпечення заданого рівня безпеки об'єкту.

Сказане можна пояснити таким чином. Недостатня кількість відеокамер призводить до наявності в просторі так званих "мертвих зон", зображення котрих не видиме на екрані монітора, тобто подібна система охоронного телебачення не дозволяє повноцінно контролювати обстановку на об'єкті.

З іншого боку, надмірна кількість відеокамер призводить до не виправданого повторення схожих зображень, що веде до зростання ціни устаткування (відеокамери, об'єктиви, кронштейни, кожухи, кабелі),

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		25

ускладнення устаткування обробки відеосигналів, тобто до невиправданого дорожчання системи охоронного телебачення. Більше того, збільшення числа відеоканалів призводить до зменшення часу спостереження по кожній зоні, до зменшення розмірів зображення при мультисценовому представленні зображень на екрані, і замість очікуваного підвищення інформативності відеосистеми відбувається її пониження.

Місця кріплення відеокамер багато в чому визначають інформативність і ефективність проекрованої системи охоронного телебачення. При виборі місць розміщення відеокамер слід прогнозувати вплив можливих перешкод. Слід виключити попадання у поле зору відеокамери джерел світла, а також відбиття від тих, що створюють відблиски поверхонь. При цьому повинен забезпечуватися необхідний для нормальної роботи відеокамери рівень освітленості.

1.2.3 Розміщення прикінцевого обладнання систем відеоспостереження

Зони огляду відеокамери

Як було сказано, проектування системи охоронного телебачення розпочинається з чіткого формулювання конкретного завдання, котре в першу чергу повинне містити опис того, що повинен бачити оператор для адекватної оцінки ситуації. Після цього слідує вибір просторових областей об'єкта, визначення їх найбільш інформативних представлень оператору. Потім робиться вибір варіантів представлення візуальної інформації операторові. На закінчення здійснюється вибір приладів, забезпечуючи рішення цієї задачі.

Таким чином, проектування системи охоронного телебачення складається з декількох етапів:

- визначення параметрів периферійного устаткування, в першу чергу, кількості і місць розміщення відеокамер, їх орієнтації в просторі, вибору об'єктів;
- визначення кількості постів охорони, одержуючи візуальну інформацію про обстановку на об'єкті відповідно до їх повноважень і пріоритетів;

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		26

- вибір складу устаткування для постів охорони, здатного в результаті його конфігурації вирішувати завдання, визначувані концепцією безпеки об'єкту;
- рішення завдань передачі сигналів від відеокамер на пости охорони;
- вибір допоміжного устаткування.

При подальшому розгляді зоною огляду відеокамери будемо називати простір усередині чотирикутної піраміди, основою якої (площиною спостереження) є прямокутник ABCD з відношенням сторін 3 : 4; у вершині цій піраміди розташована відеокамера VC1 (Рисунок 1.8).

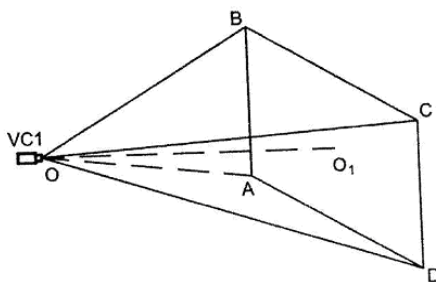


Рисунок 1.8 - Просторова модель зони огляду

Спочатку розглядатимемо варіант, коли висота піраміди (оптична вісь об'єктиву OO1) проектується на середину основи.

Якщо виконати переріз цієї піраміди горизонтальною площиною по осі OO1, то отриманий рівнобедрений трикутник FOE відповідатиме зоні огляду відеокамери в горизонтальній площині (Рисунок 1.9)

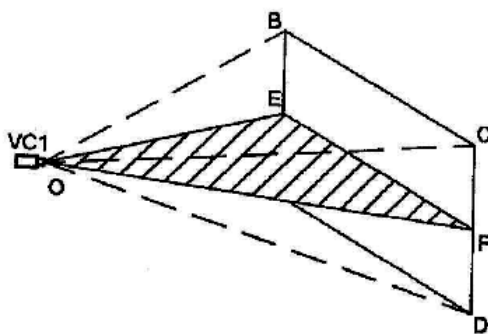


Рисунок 1.9 - Зона огляду в горизонтальній площині.

Отримання зображення на ПЗС-матриці відеокамери VC1 ілюструється на рисунку 1.10.

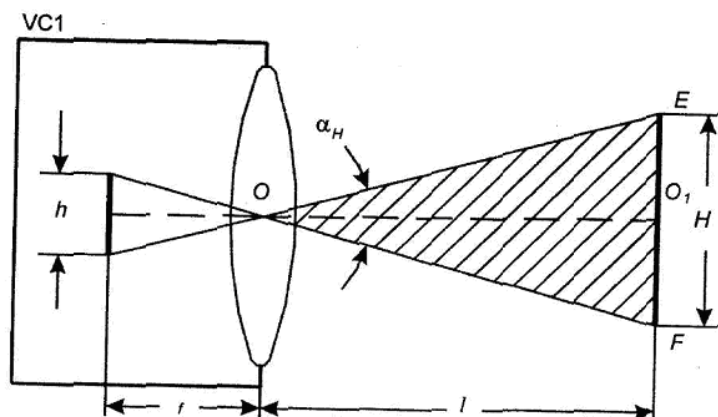


Рисунок 1.10 - Отримання зображення на ПЗС-матриці.

З очевидних геометричних співвідношень можна отримати наступні вирази:

$$\frac{f}{l} = \frac{h}{H}; \quad (1.1)$$

$$\frac{h}{2f} = \operatorname{tg}\left(\frac{\alpha_H}{2}\right); \quad (1.2)$$

$$f = \frac{h}{2\operatorname{tg}\left(\frac{\alpha_H}{2}\right)}; \quad (1.3)$$

де f - фокусна відстань об'єктиву; h - ширина ПЗС-матриці; H - горизонтальне поле зору (EF); l - відстань від центру об'єктиву до площини спостереження (OO1); α_H - кут огляду в горизонтальній площині.

Реальна зона огляду відеокамери в горизонтальній площині є не трикутником, а трапецією, підстави якої визначають так названі ближню і далеку зони.

Ближня зона визначається простором зблизька відеокамери, де відеоспостереження і відеореєстрація неефективні. Далека зона відповідає максимально можливому видаленню площини спостереження від відеокамери. Це необхідно враховувати при проектуванні систем охоронного телебачення.

Якщо виконати переріз вказаної піраміди вертикальною площиною по осі OO1, то отриманий рівнобедрений трикутник NOG відповідатиме зоні огляду у вертикальній площині (Рис.1.11).

По аналогії з раніше отриманими виразами для зони огляду у вертикальній площині справедливі наступні співвідношення:

$$\frac{f}{l} = \frac{v}{V}; \quad (1.4)$$

$$\frac{v}{2f} = \operatorname{tg}\left(\frac{\alpha_v}{2}\right); \quad (1.5)$$

де v - висота ПЗС-матриці; V - вертикальне поле зору (GH);

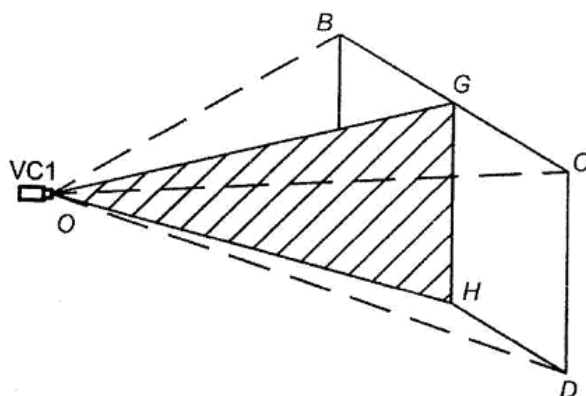


Рисунок 1.11 - Зона огляду у вертикальній площині.

Відеоспостереження поза будівлею

Охоронне телебачення може успішно використовуватися для відеоспостереження за територією у безпосередній близькості у стін будівлі, за вікнами, входами, пожежними сходами і тому подібне. Переважним є використання попарно-зустрічного розміщення відеокамер (Рисунок 1.12).

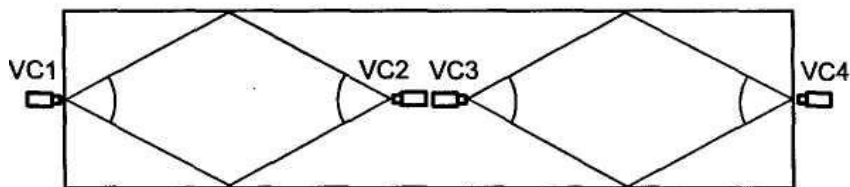


Рисунок 1.12 - Діаграма фокусування при попарно зустрічному розташуванні відеокамер

Деякі фахівці в цілях економії кабелів і спрощення кріплення використовують парну установку відеокамер, спрямованих в протилежні сторони (Рисунок 1.13)

Дійсно, така установка має ряд переваг :

- економиться довжина кабелів;
- спрощується кріплення відеокамер;
- потрібно об'єктиви з меншою фокусною відстанню (тобто менше мертва зона під відеокамерою, умовно мертва зона; більше глибина різкості);
- у разі використання ІЧ-прожекторів їх потужність може бути менше.

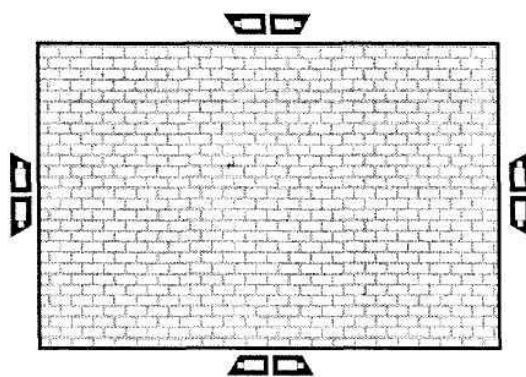


Рисунок 1.13 - Попарне розміщення відеокамер

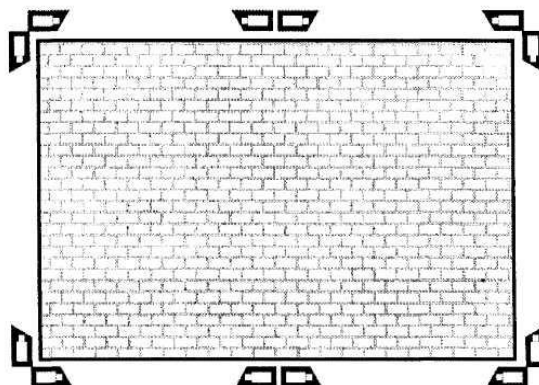


Рисунок 1.14 - Попарно зустрічне розміщення відеокамер

Проте слід пам'ятати, що в цьому випадку мертва зона в горизонтальній і у вертикальній площинах утворюється в місці встановлення відеокамер, такі відеокамери легше пошкодити або викрасти. Тому подібну установку не можна рекомендувати у випадку окремого використання двох відеокамер. Подібне кріплення можливо як варіант неодноразового попарно-зустрічного розміщення відеокамер, коли в одній точці встановлюють дві відеокамери, спрямовані в протилежні сторони, але ті що відносяться до різних зустрічно спрямованих пар (Рисунок 1.14).

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		30

Для контролю входу у будівлю слід уникати установку відеокамер у безпосередній близькості від нього: прагнення захистити відеокамеру від вандалізму примушує монтувати її достатньо високо, проте в цьому випадку ракурс зображення виявляється малоінформативним. Кращі результати виявляються, якщо розмістити відеокамеру в деякому видаленні від входу і застосувати довгофокусний об'єктив (при цьому слід враховувати обмеження за рахунок кінцевої глибини різкості).

Відеоспостереження периметра території

Для відеоспостереження периметра території, наприклад, обстановки поблизу огорожі, можливе різне розміщення відеокамер – поперечне, подовжнє, проміжне.

Слід мати зважаючи на характер території, що охороняється. Наприклад, якщо огорожа відноситься до приватного володіння, то важливіше спостерігати обстановку із зовнішнього боку огорожі - щоб перешкоджати проникненню на територію зовні. Якщо ж необхідно охороняти територію промислового підприємства або складу, то не менш важливо контролювати і внутрішню частину території поблизу огорожі (для відвертання перекидання через огорожу матеріальних цінностей). У випадку якщо огорожа оточує будівлю, розміщення відеокамер на стінах цієї будівлі дає наступні переваги:

- відеоспостереженням охоплюється не лише сама огорожа, але і частина внутрішньої території, а головне, частина території за парканом, що дозволяє контролювати злочинні задуми зловмисників на самій ранній стадії, до їх реалізації (а це дає охороні істотні переваги);
- на екрані відеомонітора огорожа відображається більше інформативно в порівнянні з переглядом уздовж огорожі (завдяки телевізійному формату 4 : 3 на екрані поміщається в 1,33 разу більше довжини огорожі).

Недоліком такої установки відеокамер слід назвати більше їх число, в порівнянні з варіантом подовжньої установки. У першому наближенні кількість відеокамер при поперечній установці дорівнює довжині периметра, що ділиться на горизонтальне поле зору на межі далекої зони.

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		31

1.3 Формування системи захисту підприємства на основі технічних засобів охорони

1.3.1 Вихідні дані для впровадження СЗІ на основі ТЗО

Об'єктом для впровадження комплексної системи захисту інформації обрано офісні приміщення комерційного підприємства, як одного з самих поширених суб'єктів господарської діяльності на території України. Саме комерційні підприємства щомісячно виплачують досить велику кількість зборів та податків в державу. На рис. 1.15 представлено план приміщень обраного нами об'єкту захисту.

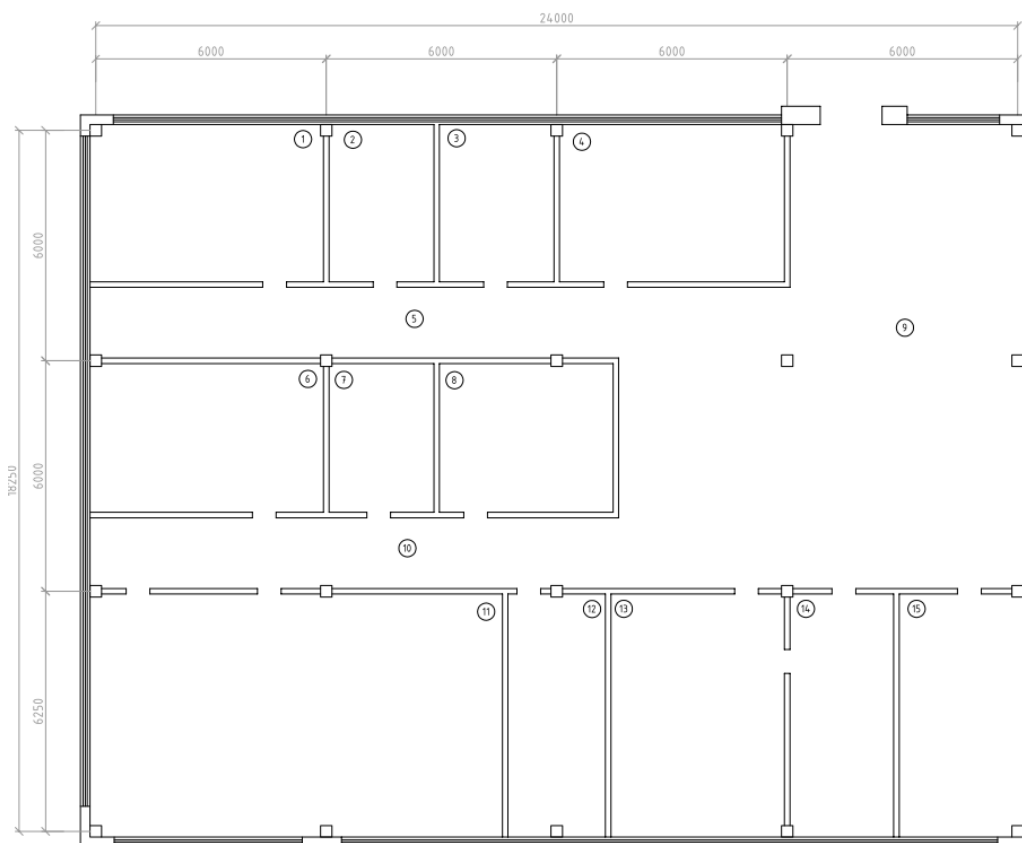


Рисунок 1.15 – План приміщень офісу приватного підприємства

В табл. 1.2 представлено експлікацію приміщень офісу

Таблиця 1.2 – Експлікація приміщень офісу

№	Найменування приміщення	Площа приміщення, м ²
1	Офісне приміщення	24,90
2	Офісне приміщення	11,17
3	Офісне приміщення	12,67
4	Офісне приміщення	17,42
5	Коридор	25,33
6	Офісне приміщення	23,60
7	Серверна	10,56
8	Електрощитова	17,39
9	Хол	108,41
10	Коридор	25,18
11	Зал переговорів	67,71
12	Операторська	16,06
13	Офісне приміщення	28,45
14	Офісне приміщення	17,28
15	Офісне приміщення	18,74

1.3.2 Впровадження технічних засобів захисту

Автоматизована система пожежної сигналізації та пожежогашіння

При виборі сповіщувачів (ПС) для виявлення пожежі необхідно враховувати ступінь пожежної небезпеки об'єкта, категорію виробництва, особливості технологічного процесу, ймовірність виникнення загоряння та динаміку його розвитку. Вибір автоматичних пожежних сповіщувачів повинен бути обумовлений:

- ймовірним проявом пожежі на його початковій стадії;
- висотою приміщення;
- умовами навколишнього середовища.

Можливою наявністю на контрольованій площі чинників, які призводять до перешкод. Розміщення та встановлення таких типів сповіщувачів регламентується їх технічною документацією. Додатково до цього їх розміщення

регламентується вимогами ВСН 25-09.68-85 "Установки охоронної, пожежної та пожежно-охоронної сигналізації. Правила виробництва і приймання робіт ":

1) Залежно від призначення оптико-електронні сповіщувачі можуть встановлюватися:

- поблизу уразливих місць або над ними;
- над місцями з підвищеною пожежонебезпекою або під стелею.

При установці оптико-електронних сповіщувачів повинні бути забезпечені умови, які виключають вплив на оптичну систему прямих сонячних променів і променів від інших світлових джерел. Простір між випромінювачем і приймачем повинен бути вільним від сторонніх тіл.

2) Розміщення блоків ультразвукових сповіщувачів доцільно проводити в місцях, позбавлених вентиляційних пристроїв, батарей центрального опалення, нагрівальних приладів та інших джерел руху потоків повітря, а також звукових перешкод, допустимий рівень, яких вказаний в експлуатаційній документації.

Схема розміщення елементів системи АСПС приведена на рисунку 1.16. Враховуючи той факт, що на плані нашого офісу присутнє приміщення серверної, задамося необхідними нормативними документами, вимогами та методичними вказівками щодо його захисту. На плані приміщення серверної позначено номером 7 з загальною площею трохи більше 10 метрів. Згідно вимог в даному приміщенні треба впровадити систему пожежогасіння.

Автоматичні установки (системи) і модулі газового пожежогасіння є одним з оптимальних способів протипожежного захисту об'єктів, т. к. призначені для ліквідації горіння твердих, рідких, газоподібних речовин, а також електрообладнання. Конструктивно автоматичні установки газового пожежогасіння (АУГП) складаються з технологічної та електротехнічної частини.

Технологічна частина АУГП містить судини з газовим вогнегасною речовиною, трубопроводи та насадки. Електротехнічна частина АУГП являє собою автоматичну пожежну сигналізацію, інформація від сповіщувачів якої надходить на пожежний прилад керування, формує сигнал на запуск ЗПП

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		34

(запірно-пусковий пристрій). Модулі та батареї газового пожежогасіння є основною частиною автоматичних установок газового пожежогасіння і призначені для зберігання та випуску у приміщення, що газових вогнегасних складів для гасіння пожеж об'ємним і локальним способом.

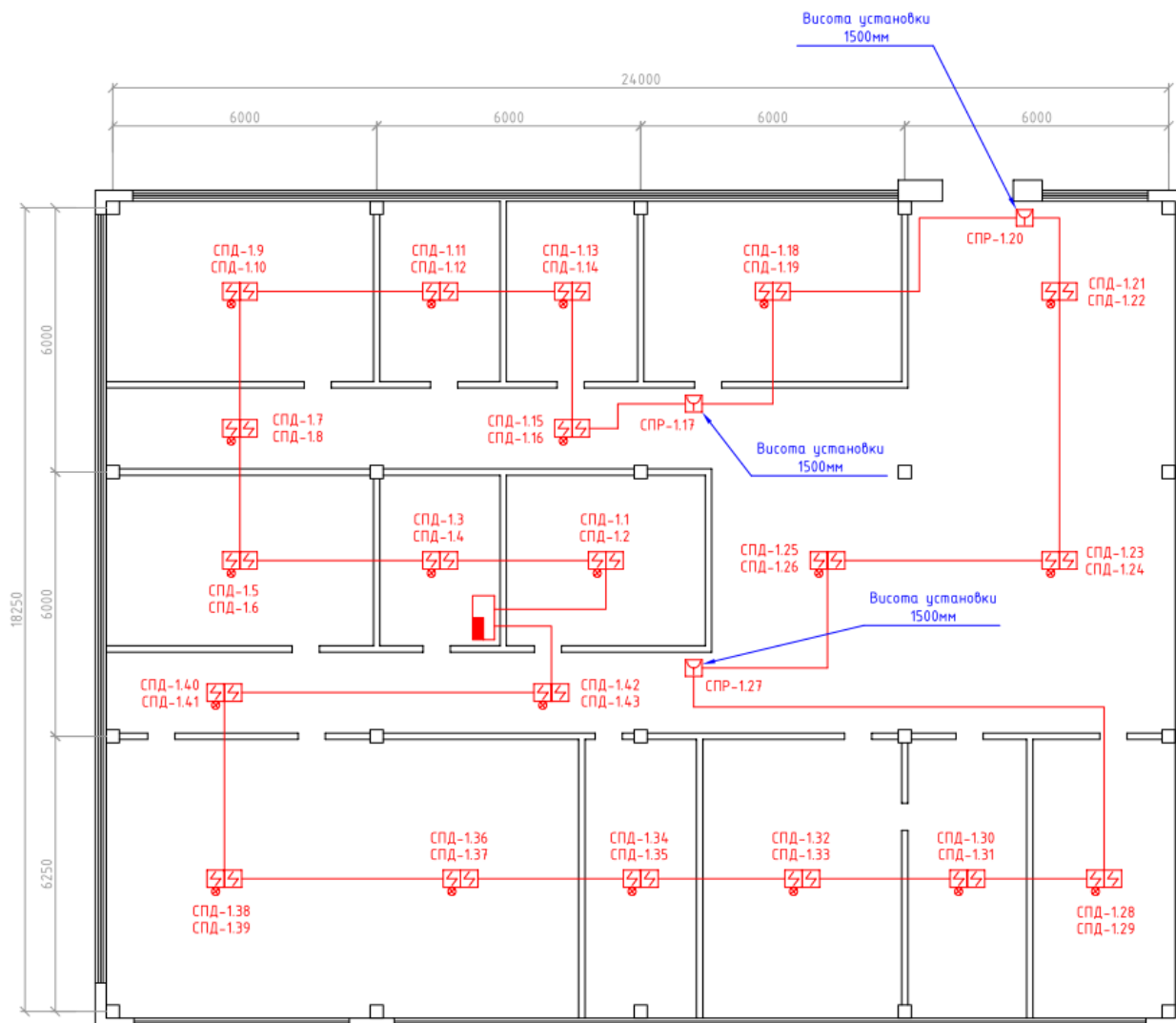


Рисунок 1.16 – Схема розташування елементів АСПС на плані приміщення

В нашому випадку приймально-контрольним пристроєм обрано обладнання Гамма-102САТ, комбіновані сповіщувачі типу СПД-3,5, світлозвукові пристрої ОСЗ-3 та ОСЗ-4, сповіщувач магнітоконтатний СОМК 3-4, модуль газового пожежогасіння МГП-1-60 та вогнегасна речовина CO₂ в кількості 42 кг. Також для формування системи пожежогасіння застосовано необхідну кількість матеріалів. Згідно з законодавством додатково проведено

формування ЗІП. На рисунку 1.17 представлено склад та розташування обладнання системи пожежогасіння в приміщенні серверної.

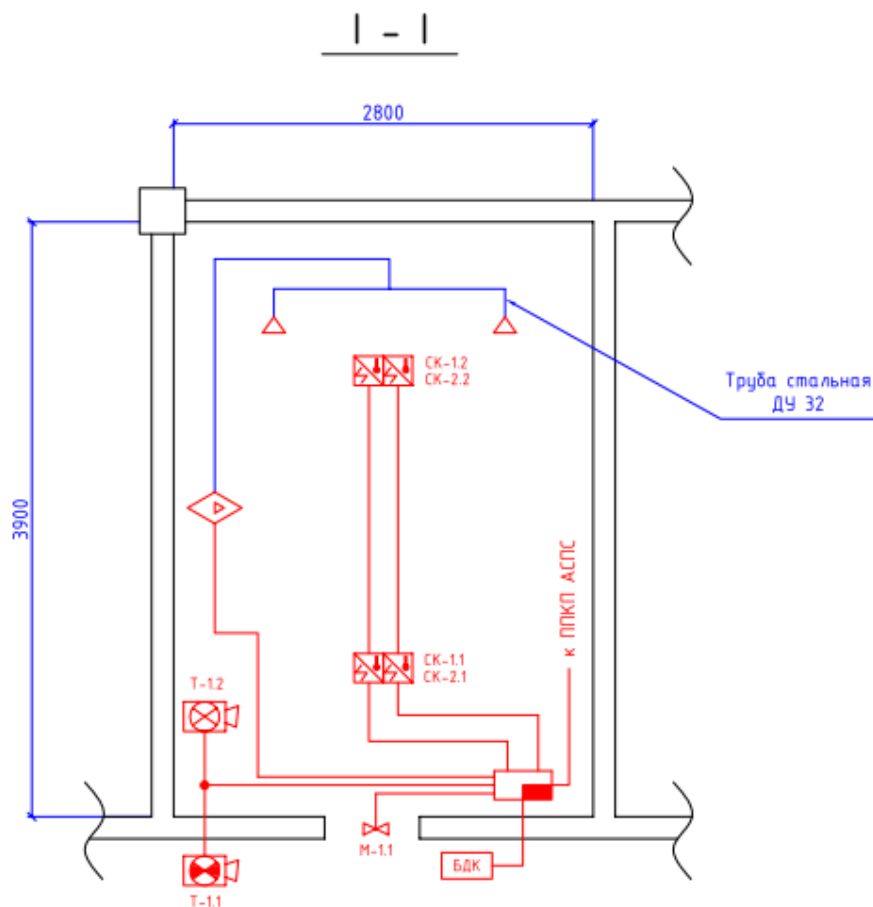


Рисунок 1.17 - Склад та розташування обладнання системи пожежогасіння в приміщенні серверної

Охоронно-тривожна сигналізація

ППКП - це центр управління системою охоронно-пожежної сигналізації, пов'язаний з периферійним обладнанням адресною лінією, до якої підключені пристрої з апаратними адресами..

Адресний блок КОДОС А-07/8 призначений для контролю стану пожежних шлейфів («КЗ», «Тривога», «Норма», «Обрив»), підключених до струмоспоживаючих пожежних датчиків, та передачі інформації в лінію зв'язку з основним приладом.

Для захисту приміщень обрано цифровий пасивний ПЧ-сповіщувач зі здвоєним піроелементом та цифровим алгоритмом руху - AQUA Plus від Satel.

					Лист	
					36	
Изм.	Лист.	№ докум.	Подп.	Дата	КС.55.07.000.ДП ПЗ	

Завдяки застосуванню двоканального аналізу сигналу від піроелемента (за значенням та за кількістю) та функції компенсації температури сповіщувач може працювати у широкому діапазоні температур. Він відрізняється високою чутливістю та стійкістю до перешкод. Можливість заміни лінзи Френеля і триступінчасте регулювання чутливості дозволяють оптимально конфігурувати пристрій відповідно до потреб користувача та об'єкта, що охороняється. Сповіщувач має функцію попередньої тривоги та тамперний контакт, а також вбудовані кінцеві резистори, які полегшують встановлення та підключення до системи. AQUA Plus відповідає вимогам стандарту Grade 2 EN-50131.

Також у системі передбачено застосування акустичних сповіщувачів розбиття скла, обрано модель INDIGO від бренду Satel. Акустичний сповіщувач розбивання скла INDIGO призначений для захисту приміщень зі скляними поверхнями. Він виявляє розбиття скла: звичайного, загартованого та багат шарового. Сповіщувач аналізує акустичний сигнал низької (удар) та високої (розбиття скла) частоти. Тільки у разі виявлення цієї послідовності сигналів буде викликано тривогу. Чутливість виявлення можна регулювати. Додатково датчик обладнаний тамперним контактом і сигналізацією стану батареї. Для перевірки роботи акустичних сповіщувача розбиття скла рекомендується використовувати TESTER INDIGO.

На рисунку 1.18 представлена схема охоронно-тривожної сигналізації, що впроваджена на підприємстві.

Система відеоспостереження

В основі системи відеоспостереження - відеореєстратор, на який відбувається запис відеопотоків з камер відеоспостереження. Вибраний 16-канальний AI мережевий відеореєстратор із PoE Dahua DHI-NVR2216-16P-I. Крім множини інтелектуальних функцій, реєстратор має вбудований PoE комутатор, що дозволяє не купувати його як додатковий пристрій. В загальній системі передбачено 6 зовнішніх та 4 внутрішніх відеокамер. При виборі зовнішніх відеокамер задавалися такі умови:

Розподільна здатність – до 4 МП

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		37

Дальність ІЧ – до 40 метрів

Тип живлення – PoE

Тип корпусу – циліндрична

Клас захисту – IP67

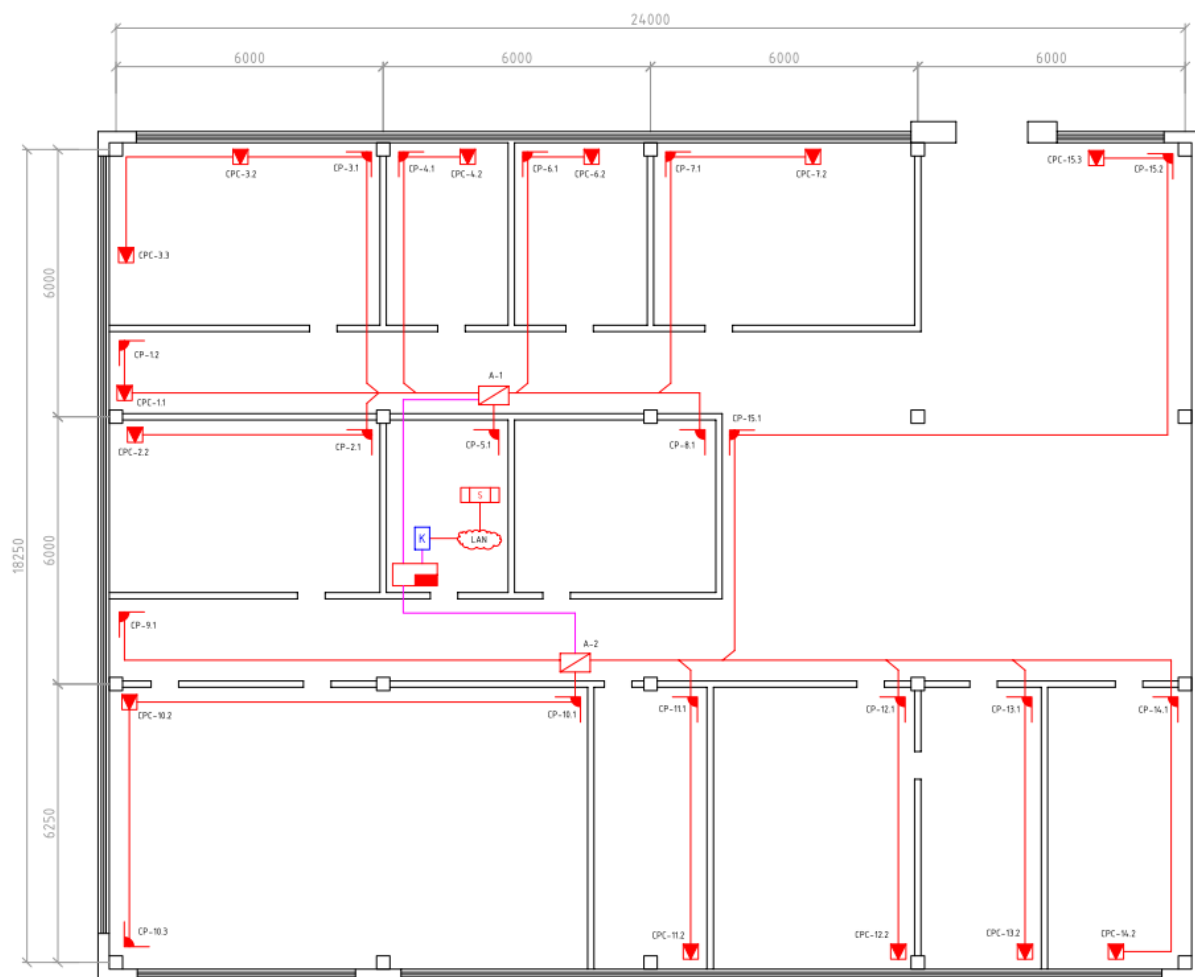


Рисунок 1.18 – План розміщення системи охоронної сигналізації

На підставі ТЗ вибрано IP відеокамеру Dahua DH-IPC-HFW2439SP-SA-LED-S2. З основних переваг – це наявність WDR 120dB та підтримка Smart функцій (IVS). Камера оснащена сенсором 1/3" з чутливістю 0.004Люкс. Максимальна роздільна здатність 4МП (2688x1520px) і швидкість запису 25 кадрів/с, підтримка розподільної здатності 3МП, 1080p і 720p - 25 кадрів/с. Моторизований об'єкт огляду по горизонталі 81 ° Автоматична зміна режиму день / ніч, підсвічування з дальністю до 30 м. Технологія відеостиснення на базі

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		38

кодека H.265 допоможе істотно знизити навантаження на локальну мережу і заощадити простір на жорсткому диску.

При виборі зовнішніх відеокамер задавалися такими умовами:

Розподільна здатність – до 3 МП

Дальність ІЧ – до 30 метрів

Тип живлення – PoE

Тип корпусу – купольна

Кодек– H.264

На основі ТЗ вибрано IP відеокамера Dahua DH-IPC-HDW1320SP-S3 (2.8 мм). Організація комутації полягає в застосуванні технології PoE – застосуванням PoE-комутаторів. Комутація проводиться провідним способом на основі мережевого кабелю OK-NET UTP CAT.5E 305M (U/UTP-CAT.5E) (КПВ-ВП (350) 4*2*0,50). Детальна специфікація обладнання та матеріалів представлена в табл.1.3.

Таблиця 1.3 - Специфікація обладнання та матеріалів підсистеми відеоспостереження підприємства на основі бренду Dahua

№	Найменування	Кількість	Ціна, грн.	Вартість, грн.
1	Відеореєстратор Dahua DHI-NVR2216-16P-I	1	14400,00	14400,00
2	Жорсткий диск WD Purple 3.5" 4TB WD (WD40PURZ)	1	3306,00	3306,00
3	Зовнішня IP-відеокамера Dahua DH-IPC-HFW2439SP-SA-LED-S2	6	3996,00	23976,00
4	Внутрішня IP-відеокамера	4	2340,00	9360,00
5	Кабель UTP, бухта 305 м.	1	3750,00	3750,00
6	Комплект витратних матеріалів	1	850,00	850,00
Усього, грн.				55642,00

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		39

Проведемо порівняння при застосуванні обраних нами відеокамер, які налаштуємо на різні параметри. Отже, подивимось, як буде змінюватися глибина архіву відеосервера при встановленні різного типу якості картинки. Додатково подивимось, які залежності пропускної здатності мережі при різних характеристиках якості зображення. Результати представимо в графічній формі.

Розглянемо, як змінюються базові параметри системи відеоспостереження за умов зміни характеристик сцени. Мається на увазі, що характеристики сцени можуть такі, як жвава вулиця, офісні приміщення, периметральне спостереження та коридори бізнес-центру. Заповнимо таблицю, де розрахуємо обсяг відеоархіву та пропускну здатність мережі залежно від якості зображення відеокамери. Для розрахунків застосуємо калькулятор проектувальника систем відеоспостереження.

Вихідні дані: кодек - H.264 (1), складність - 1 - 80% руху, 2 - 60% руху, 3 - 50% руху, 4 - 40% руху, кадрів на секунду – 12, годин запису – 24, кількість діб запису – 1, камер – 1

Таблиця 1.4 – Робочий екран розрахунок таблиці обсяг відеоархіву та пропускну здатність мережі залежно від якості зображення відеокамери.

Параметри налаштування IP-камери		Складність кадру			
Розподільна здатність	Розрахункові параметри	1 - висока	2 - вище середньої	3 - середня	4 - низька
		Жвава вулиця	Офісні приміщення	Периметральний нагляд	Коридори бізнес-центру
CIF 352×288	Об'єм архіву	3,26	1,897	1,19	1,016
	Канал, Мбіт/с	0,29	0,17	0,11	0,09
2CIF 704×288	Об'єм архіву	6,49	3,89	3,08	2,032
	Канал, Мбіт/с	0,59	0,35	0,28	0,18
4CIF 704×576	Об'єм архіву	12,98	7,77	6,18	4,07
	Канал, Мбіт/с	1,17	0,7	0,56	0,37
D1 720×576	Об'єм архіву	13,27	7,95	6,33	4,17
	Канал, Мбіт/с	1,2	0,72	0,57	0,38
HD 1280×720	Об'єм архіву	29,5	17,68	14,04	9,26
	Канал, Мбіт/с	2,67	1,6	1,27	0,84
Full HD 1920×1080	Об'єм архіву	66,37	39,77	31,6	20,83
	Канал, Мбіт/с	6	3,6	2,86	1,88
5 Мп 2592×1944	Об'єм архіву	191,27	96,64	76,79	50,63
	Канал, Мбіт/с	14,58	8,74	6,94	4,58

Графічна форма даних, відображених у таблиці, представлена на рис.1.19.

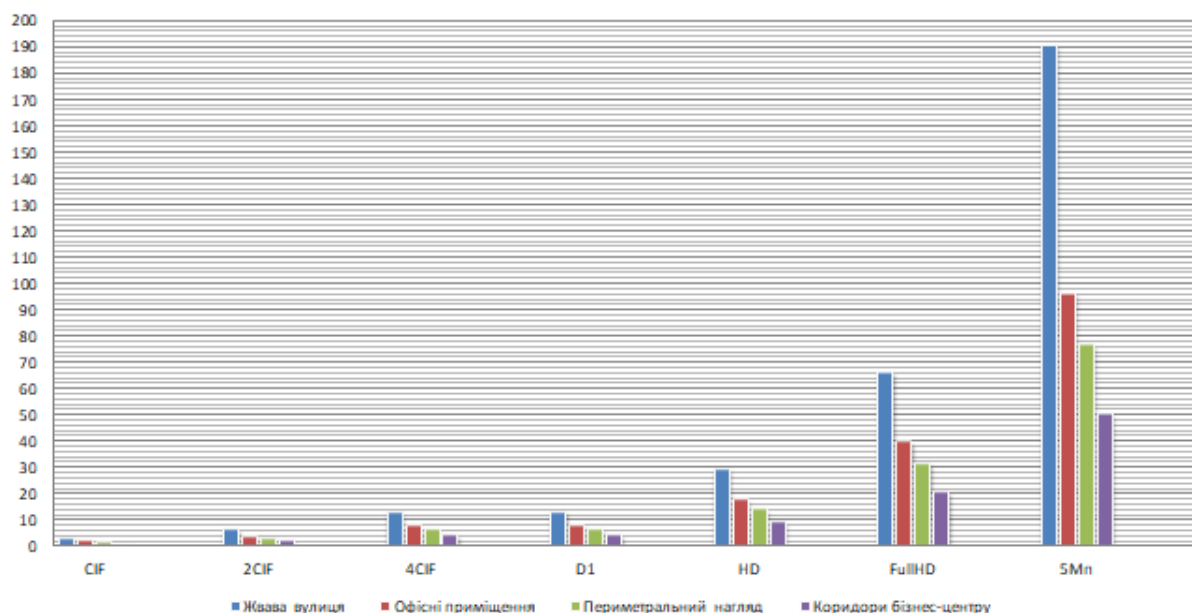


Рисунок 1.19 – Зависимость глубины архива от характеристик сцены

На графіку видно, що форматами якості нижче HD сьогодні можна знехтувати, т.к. Вибране обладнання дозволяє користуватися якісними параметрами (внутрішні камери – до 3 Мп, зовнішні – до 4 Мп). Видно, що чим більше руху в кадрі, тим більше записується архіву на вінчестери відеореєстратор системи. Щодо пропускної спроможності системи відеоспостереження, то вимоги до мережі також зростають зі збільшенням якості відеозображення, як показано на рис. 1.20. Як видно, для якості HD (1 мегапіксель) при спостереженні за вулицею потрібна пропускна здатність 2,67 Мбіт/с. Зі збільшенням якості зображення, наприклад, до 2-х Мп, пропускна спроможність мережі збільшується до 6,0 Мбіт/с.

При проектуванні системи відеоспостереження необхідно вибирати оптимальні параметри під час налаштування реєстратора. Так, наприклад, вибір типу запису істотно впливає на глибину архіву. У матеріальному еквіваленті - це кількість накопичувачів та їх параметри, а також вимоги до реєстратора. На рисунку 1.21 показано зміну глибини архіву при 3-х типах запису – за детекцією, за розкладом та за постійного запису.

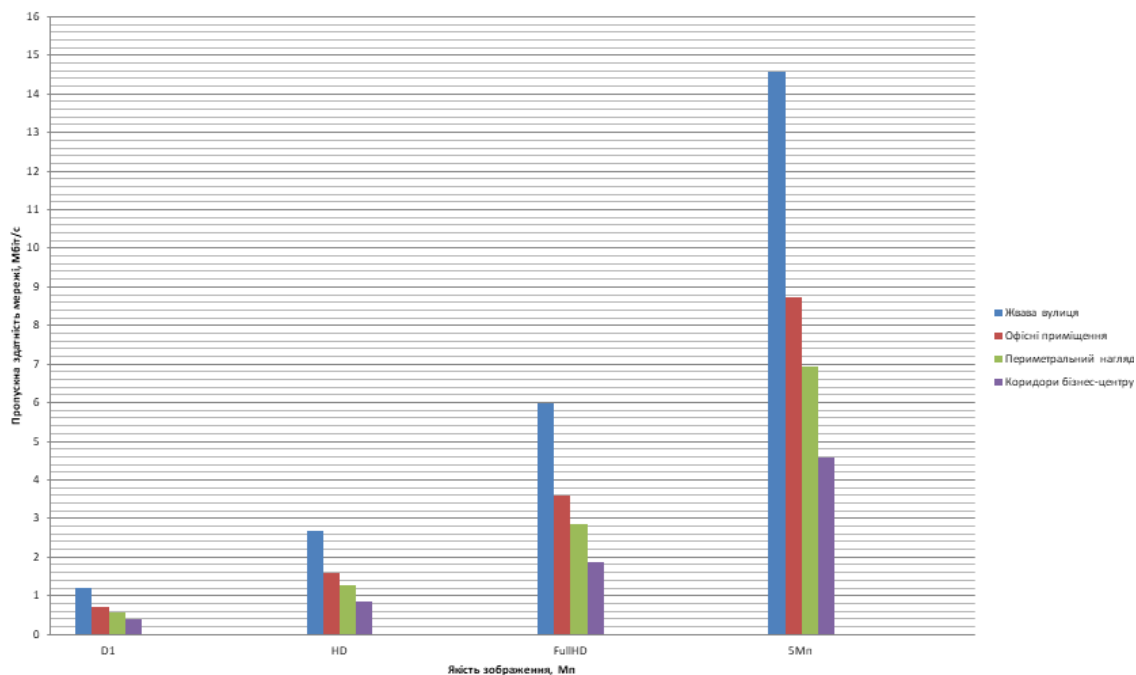


Рисунок 1.20 – Залежність пропускної спроможності мережі від зміни типу сцени

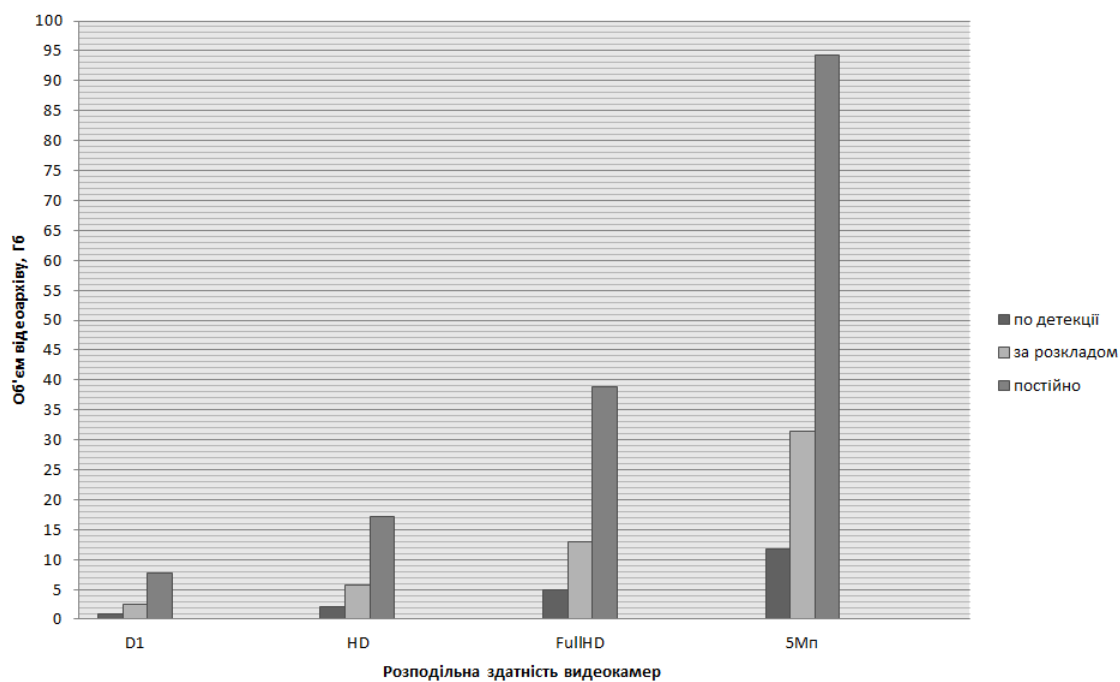


Рисунок 1.21 – Залежність глибини архіву системи відеоспостереження від типу запису архіву

Як видно з рисунку 1.21, оптимальним є застосування запису архіву детектором. Так, якщо взяти за основу типову якість 2 Мп, то різниця між записом по детекції та постійним записом становить 8 разів. Також варто

звертати увагу на такий параметр, як тип кодека системи відеоспостереження. Різницю застосування видно за даними, наведеними в табл. 1.5.

Таблиця 1.5 - Зміна вимог до каналу зв'язку під час використання різних типів кодеку в системі відеоспостереження.

Якість	Тип кодеку	Канал, Мбіт/с
Full HD (1920x1080)	H.264	3,9
	MPEG4	12,52
	MJPEG	39,67
	JPEG2000	32,41
	Без стиску	569,53

На рисунку 1.22 представлений план із розміщенням камер системи відеоспостереження.

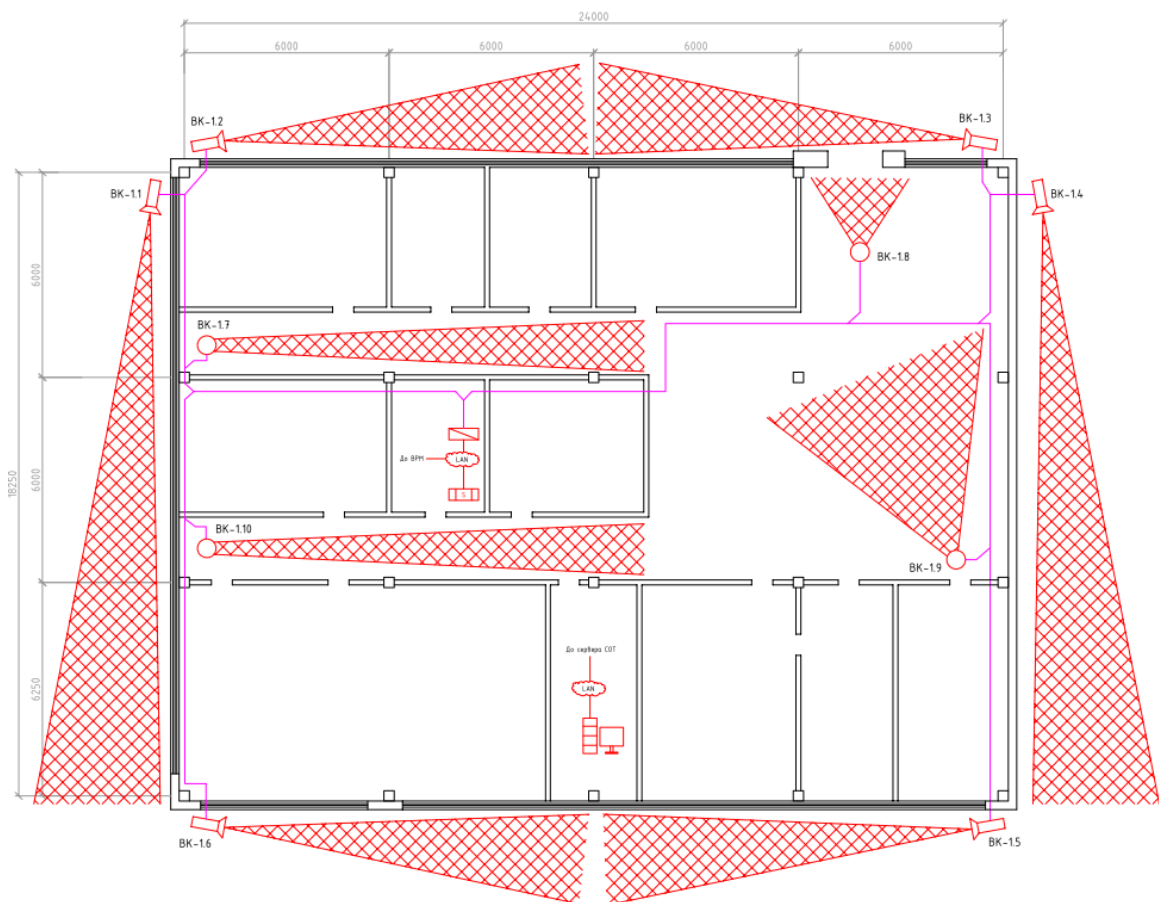


Рисунок 1.22 – Схема розташування системи охоронного телебачення

1.3.3 Вибір приймально-контрольних приборів систем сигналізації в аспекті терміну експлуатації

Нехай попередньо є два ППКО однакового класу (наприклад, малої інформаційної ємності, рівної інформативності) -ППКО-1 і ППКО-2. В документації на кожен з них наведено значення середнього напрацювання на відмову T_{01} і T_{02} відповідно. Відома ціна кожного з них: Π_1 і Π_2 .

За результатами експлуатації практично завжди можна оцінити середню вартість одного ремонту. Її величина визначається за формулою:

$$C_{p.сep.} = \frac{\sum_{i=1}^{n_0} C_{pi}}{n_0}, \quad (1.6)$$

За даними експлуатації середня вартість одного ремонту ППКО оцінюється приблизно як:

$$C_{p.сep.} \approx (0,1 - 0,12)\Pi$$

За формулою

$$\lambda = \frac{1}{T_0}, \quad (1.7)$$

визначаються значення інтенсивностей відмов для ППКО-1 і ППКО-2: λ_1 та λ_2 відповідно.

З документації на кожен прилад відомі їхні терміни служби (зазвичай 5-8 років).

Вважаємо, що протягом установленого терміну служби прилад експлуатується безперервно (цілодобово). Один рік дорівнює 8760 год, отже, за період терміну служби (наприклад, 5 років) прилад напрацює $5 \times 8760 = 43800$ ч.

За наведених умов вирішується завдання оцінки витрат на ремонти приладів в залежності від показників їх надійності, вартості ремонту і встановленого терміну служби. Складається система рівнянь середніх витрат на ремонти ППКО-1 і ППКО-2: Z_{p1} і Z_{p2} відповідно:

					КС.55.07.000.ДП ПЗ	Лист
						44
Изм.	Лист.	№ докум.	Подп.	Дата		

$$З_{P1} = \lambda_1 C_{p.cep.1} \times t + Ц_1, \quad (1.8)$$

$$З_{P2} = \lambda_2 C_{p.cep.2} \times t + Ц_2$$

Вирішуючи систему щодо аргументу t , отримаємо точку відліку часу, правіше якої з'являється ефект.

$$t_{ef.} = \frac{Ц_2 - Ц_1}{\lambda_1 C_{p.cep.1} - \lambda_2 C_{p.cep.2}} \approx \frac{10(Ц_2 - Ц_1)}{Ц_1 \lambda_1 - Ц_2 \lambda_2}, \quad (1.9)$$

Рішення про вибір можна приймати, побудувавши ряд діаграм виду, показаного на рис.1.23, де $t_{ef.}$ - час оцінки ефективності, $t_{тс}$ - термін служби.

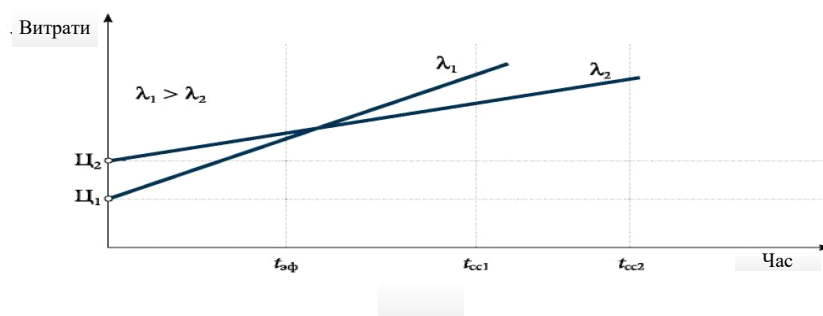


Рисунок 1.23 – Оцінка ефективності ОС від терміну служби

Для даного прикладу рисунку можна зробити висновок, що до часу $t \leq t_{тс.}$ доцільніше встановити і експлуатувати більш дешевий і менш надійний ППКО.

Якщо $t_{ef.} \rightarrow t_{тс1}$, $t_{тс1} \rightarrow t_{тс2}$, то висновок однозначний, необхідно застосовувати ППКО-1 як більш дешевий.

Таблиця 1.6 – Вибір ППКО

№ варіанта	Ц	λ	$t_{сс}$	Вибір ППКО
1	$Ц_1 = Ц_2$	$\lambda_1 = \lambda_2$	$t_{сс1} = t_{сс2}$	Необхідно скористатися іншими критеріями, наприклад "час доставки"
2			$t_{сс1} > t_{сс2}$	ППКО-1
3			$t_{сс1} < t_{сс2}$	ППКО-2
4		$\lambda_1 > \lambda_2$	$t_{сс1} = t_{сс2}$	ППКО-2

5			$t_{cc1} > t_{cc2}$	ППКО-2
6			$t_{cc1} < t_{cc2}$	ППКО-2
7		$\lambda_1 < \lambda_2$	$t_{cc1} = t_{cc2}$	ППКО-1
8			$t_{cc1} > t_{cc2}$	ППКО-1 (вибір не однозначний)
9			$t_{cc1} < t_{cc2}$	ППКО-1

Розглядаючи таким чином ППКО, можна з достатнім ступенем точності обґрунтувати вибір. Для більш обґрунтованого вибору необхідна інформація про середні витрати на ремонт приладу $C_{p\text{ ср}}$, яку можна отримати тільки в тому випадку, якщо є система збору та аналізу інформації про відмови.

1.3.4 Дослідження ефективності функціонування ТЗО

Для оцінки ефективності ТЗО існують методи, на основі яких можна порівнювати конкуруючі варіанти СБ, оцінювати і обґрунтовувати забезпечення заданих замовником характеристик. Без цих методів замовник часто знаходиться під «гіпнозом» ціни (чим дешевше, тим краще), а питання забезпечення ефективності відходять на другий план.

Ефективність СБ характеризує ймовірність виконання системою своєї основної цільової функції щодо забезпечення захисту об'єкту від загроз, джерелами яких є навмисні протиправні (несанкціоновані) дії фізичних осіб (порушників).

Враховуючи складність вирішуваних завдань, виходячи з принципів раціонального та ефективного використання коштів, створення системи захисту повинно базуватися на наступних принципах:

- розумної достатності заходів;
- чіткої правової основи;
- організованою службі фізичної охорони;
- оптимальному складі технічних засобів захисту.

Система вважається ефективною, якщо виконуються такі вимоги:

1) в заданих умовах експлуатації повністю і у встановлені терміни виконує поставлені перед нею завдання (технічна ефективність);

2) витрати на створення та експлуатацію системи не перевищують позитивного ефекту від її використання (економічна ефективність).

Оптимізацію структури СБ можна розглядати як вибір найкращого варіанта з безлічі альтернатив. При цьому основним критерієм вибору є задоволення СБ вимогам ефективності при мінімальному рівні витрат. Тому питання кількісної оцінки ефективності функціонування СБ є актуальним, але стосовно до СБ він розроблений слабо.

Застосування загальних критеріїв до СБ утруднено з кількох причин. До них слід віднести різноманіття загроз об'єкту, способів їх реалізації; різноманітність об'єктів з точки зору конфігурації і просторового розташування, режиму функціонування, режиму забезпечення безпеки; структурну та організаційну складність СБ.

Проте загальні методи оцінки ефективності систем різного призначення можна з відповідними змінами застосовувати до СБ. Прийнято використовувати економічні, імовірнісні, комбіновані і надійніші методи для оцінки ефективності СБ.

При визначенні економічної ефективності СБ розглядається співвідношення позитивного економічного ефекту (E) від використання системи і загальних витрат (Z), що включають вартості її створення та обслуговування протягом терміну експлуатації. При цьому оцінюється відносна ефективність системи, яка може бути представлена у вигляді:

$$E_o = \frac{B - Z}{B_z} = Z_B - \frac{Z}{B_z}, \quad (1.10)$$

де

$B = B_z \times Z_B$ - запобігання втрат в результаті використання системи;

B_z - загальні можливі втрати;

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		47

Z_B - відносний відвернений збиток в результаті використання системи безпеки ($0 < Z_B < 1$).

Величина збитку складається з наступних складових:

- вартості, спрямованої на відшкодування наслідків події (компенсація);
- вартості викраденого або знищеного пожежею майна, (ремонт об'єкта тощо);
- вартості додаткових тимчасових витрат (відновлення працездатності ділянки, якому завдано збитків);
- відносної вартості, визначеної збитками через того, що сталося розкрадання або пожежі (простою обладнання, штрафами за зрив термінів постачання тощо);
- розміру матеріальних витрат і робочого часу, витрачених на розслідування пригод.

Перераховані види вартості утворюють так звану «групу ризику». Різниця між можливими збитками і прямими витратами становить умовну прибуток по даній системі. Величина умовного прибутку визначає величину капіталовкладень в устаткування об'єкта комплексом ТЗО.

Аналіз формули (1.10) показує, що система тим ефективніше ($E_0 > 0$), чим вище умовний відвернена нею збитки і чим нижче відносні витрати на її створення і експлуатацію, тобто якщо виконується співвідношення $Z_B > Z / B_z$.

Наведемо приклад використання цього методу. Хай вартість СБ становить 20 % від суми загальних можливих втрат, тобто $C_0 = 0,2 B_z$, термін служби СБ становить $T = 10$ років, витрати на експлуатацію СБ протягом періоду T складають 5% від вартості системи $C_E = 0,05 \times 10 C_0$. Тоді загальні витрати на створення системи будуть рівні

$$Z = C_0 + C_E = 0,23 + 0,05 \times 10 C_0 = (0,2 + 0,05 \times 10 \times 0,2) \times B_z = 0,3 B_z$$

Таким чином, система буде ефективна, якщо відносний відвернений збиток Z_B складе не менше 30 % загальних можливих втрат від реалізації загроз.

Імовірнісні методи включають такі параметри як ймовірності реалізації загроз; виявлення загроз; помилкових тривог; заходу несанкціонованих дій та ін.

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		48

Зазначені параметри можуть бути отримані на основі статистичних даних та експертних оцінок.

Додаткову складність зазначених методів створює те, що практично відсутня статистичний матеріал за ймовірностями реалізації загроз, імовірнісним характеристикам устаткування забезпечення безпеки, а експертні оцінки представляються досить суб'єктивними.

Надійність системи можна розрахувати за формулами, які дозволяють визначити ефективність тих чи інших методів затримки порушника.

Зазначені критерії можуть бути застосовані як до СБ в цілому, так і до окремих підсистем, оскільки систему безпеки, як складну ієрархічну систему, можна декомпонувати.

Прийнято розглядати два підходи до оцінки ефективності, які використовують принципово різні методи:

- 1) Метод безпосереднього підрахунку значення ефективності, якщо відома аналітична залежність (як правило, аналітична залежність не відома, оскільки кожен об'єкт унікальний);
- 2) Метод з використанням експертних оцінок (метод може бути ефективний в умовах обмеженості часу на прийняття рішення по обладнанню комплексу СОТ, крім того, частину інформації про СОТ не піддається кількісній оцінці).

При цьому необхідно визначати вплив кожного елемента СБ на реалізацію конкретної загрози (сприяння, незалежність, конфлікт) для отримання значень коефіцієнтів ефективності кожної ПСБ.

Комплексний показник ефективності технічних рішень СБ можна оцінити функціональною залежністю:

$$K_{E\Phi} = f(k_1, k_2 \dots k_n), \quad (1.11)$$

де k_1, k_2, k_n - значення приватних показників ефективності, які характеризують основні і допоміжні підсистеми СБ Перерахуємо ці підсистеми:

- 1) надійність обладнання периметра об'єкта засобами сигналізації;

2) інженерна підготовка місцевості (підступів до об'єкта, зовнішньої смуги відчуження, внутрішньої забороненої зони) і периметра;

3) характеристики і параметри ССОІУ;

4) характеристики і параметри СКУД;

5) характеристики і параметри СОТ;

6) характеристики системи тривожного освітлення (СТО);

7) характеристики системи оперативного зв'язку (СОС);

8) системи резервного безперебійного електропостачання, кліматичної та вандалозахищеність (СЕС);

9) заходи з протидії технічній розвідці організованих злочинних груп, незаконних збройних формувань та іноземних спецслужб (ПДТР).

Кожен приватний показник ефективності підсистеми є комплексним, тому що включає в себе такі параметри, як ймовірності виявлення і помилкової тривоги або напрацювання на відмову.

Група експертів формується з метою вибору тих чи інших технічних пропозицій по обладнанню об'єкта комплексом ТЗО або для вироблення експертних оцінок ефективності різних системах оцінки їх параметрів. Методом оцінки може бути метод групової експертизи, так як групові оцінки дозволяють компенсувати зміщення оцінок окремих членів експертної групи.

При відборі експертів використовують спеціальні анкети для визначення рівня компетентності методом самооцінок потенційних експертів за п'ятибальною системою. Після отримання індивідуальних самооцінок експертів формується групова середня самооцінка експертної групи в кожній галузі знань, необхідної для проведення експертизи. Чисельність експертної групи впливає на точність оцінок і може залежати від складності та масштабності оцінюваної СБ. Група експертів може налічувати від 3 до 7 фахівців різного профілю.

В анкетах експертам пропонується виставити оцінку в балах по кожному з приватних показників ефективності. Після обробки результатів експертних оцінок отримують усереднені приватні показники ефективності комплексу СБ (табл.1.7).

					КС.55.07.000.ДП ПЗ	Лист
						50
Изм.	Лист.	№ докум.	Подп.	Дата		

Таблиця 1.7 - Значення приватних показників ефективності ПСБ

Периметр	ССОИУ	Інжен. облад.	СОТ	СКУД	СЕС	СОС	ПДТР	СТО
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9

Обґрунтування оптимального вибору СБ виконується методом узагальнених параметрів оптимізації. У методі переходять від абсолютних значень приватних показників, що мають свій фізичний зміст і розмірність, до безрозмірно узагальненої функції бажаності Харрінгтона (Desirability Profile), яка визначається наступним чином (3.7):

$$d = 1 / \left(e^{\sqrt{x}} \right), \quad (1.12)$$

де e - основа натурального логарифма;

x - наведене значення досліджуваного показника.

Функція визначена в інтервалі 0...1 і використовується як безрозмірною шкали, названої шкалою бажаності або перевагу, для оцінки рівнів порівнюваних показників підсистем (рис. 1.24).

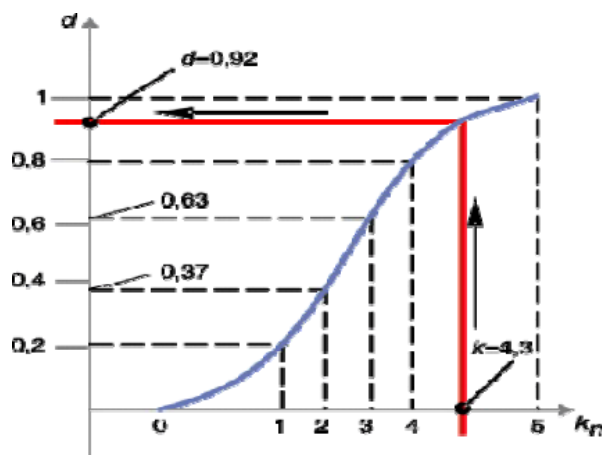


Рисунок 1.24 - Значення узагальненої функції бажаності

Шкала бажаності встановлює співвідношення між натуральним значенням приватного показника (k_n) і значенням функції бажаності (d). При цьому значення $d=0$ відповідає абсолютно неприйнятному значенням приватного показника, а $d=1$ - самому кращому його значенню. Ступінь важливості приватного показника можна врахувати крутизною функції бажаності. Маючи

оцінки рівнів приватних показників підсистем СОТ, можна розрахувати узагальнену функцію бажаності того чи іншого технічного рішення як середнє геометричне значень узагальненого приватного показника ефективності підсистеми. При цьому шукану узагальнену функцію бажаності можна розглядати як комплексний показник ефективності $K_{ЕФ}$ згідно з формулою (1.13):

$$K_{ЕФ} = \sqrt[n]{S_1, S_2 \dots S_n}, \quad (1.13)$$

де $S_n = d_n \times g_n$, - значення узагальненого приватного показника ефективності підсистеми з урахуванням його значущості;
 g_n - коефіцієнт значущості підсистеми (рис. 1.25).

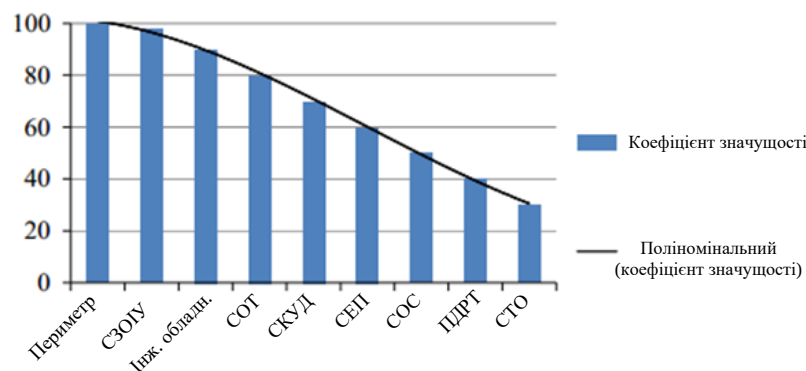


Рисунок 1.25 - Значення коефіцієнтів значущості підсистеми

де СЗОІУ (система збору і обробки інформації та управління)

СЭС (система електропостачання)

СОС (система охоронної сигналізації)

СОТ (система охоронного телебачення)

СКУД (система контролю та управління доступом)

ПДТР (система протидії технічній розвідці)

СТО (система тривожного освітлення)

2 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даних розрахунків є обчислення вартості виконання науково-дослідного проекту по об'єкту безпеки з позиції застосування технічних засобів охорони. Під технічною системою охорони (ТСО) у разі розуміється система раннього виявлення загроз фірмі від стихійних лих, несанкціонованого проникнення порушників і помилкових чи неправомірних дій обслуговуючого персоналу чи клієнтів фірми. Даний вид проекту відноситься до науково-дослідницької розробки. Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення.

Розрахунок трудомісткості НДР здійснений в наступній послідовності:

1) Складений перелік всіх етапів і видів робіт, які необхідно виконати в ході даної НДР. Після узгодження з керівником проекту допущено виключення, доповнення, об'єднання окремих етапів і видів робіт;

2) По кожному виду робіт визначений кваліфікаційний рівень виконавців. Перелік етапів і робіт, що виконуються при проведенні НДР, приведений в таблиці 2.1.

Таблиця 2.1 - Розподіл робіт по етапах і видах виконавців

Етап проведення НДР	Вигляд робіт	Посада виконавця
Розробка технічного завдання (ТЗ)	1.Складання і затвердження ТЗ для НДР по розробці «Проектування безпеки об'єкту з позиції застосування технічних засобів охорони»	Дипломник, керівник
Вибір напрямку дослідження	1. Збір і вивчення науково-технічної літератури. 2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка. 3. Вибір напрямку проведення досліджень 4. Розробка плану проведення досліджень для подальшої розробки.	Дипломник керівник

Теоретичні і експериментальні дослідження	1. Базові відомості про технічні засоби охорони об'єктів 2. Проектування систем відеоспостереження на об'єктах інформаційної діяльності 3. Формування системи захисту підприємства на основі технічних засобів охорони	Дипломник керівник консультанти
Узагальнення і оцінка результатів досліджень	1. Узагальнення результатів 2. Оцінка повноти вирішення поставлених завдань. 3. Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття результатів в цілому.	Дипломник керівник консультанти

Оцінка тривалості виконання робіт розраховується на основі вірогідних оцінок робіт, що задаються виконавцями.

Таблиця 2.2 - Очікувана трудомісткість робіт

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР «Проектування безпеки об'єкту з позиції застосування технічних засобів охорони».	1
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	3
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	3
4. Розробка плану проведення досліджень для подальшої розробки.	2
5. Технологічний розділ 5.1 Базові відомості про технічні засоби охорони об'єктів 5.2 Проектування систем відеоспостереження на об'єктах інформаційної діяльності 5.3 Формування системи захисту підприємства на основі технічних засобів охорони	12
Всього:	21

Розрахунок собівартості і ціни виконання НДР. Виходячи з особливостей створення науково – технічної продукції і її залежності від інтелектуальної праці, розрахунок собівартості і ціни виконання НДР включає наступні статті витрат: витрати на матеріали, основна і додаткова заробітна

плата, відрахування до єдиного соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями, і деякі інші.

1) Витрати на матеріали складають 170 грн.

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної зарплати встановлюється виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за один робочий день. Відповідно до статті 8 «Закону про Державний бюджет України на 2021» встановлено мінімальну заробітну плату у місячному розмірі з 1 січня 2022 року - 6500 гривень; мінімальну погодинну тарифну ставку – 39,26 грн.

Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

$$\text{Зден} = \text{п.т.с.} * 8;$$

де п.т.с – погодинна тарифна ставка, грн.;

8 – тривалість робочого дня, год.

$$\text{Зден дипломника} = 39.26 * 8 = 314,08 \text{ грн.}$$

$$\text{Зден керівника} = 65.00 * 8 = 520 \text{ грн.}$$

$$\text{Зден консультантів} = 62.00 * 8 = 496 \text{ грн.}$$

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в таблиці 2.3.

Таблиця 2.3 - Витрати на основну заробітну плату

Виконавець	Погодинна тарифна ставка, грн	Денна ставка, грн	Трудомісткість робочих днів	Сума основної зарплати, грн
Дипломник	39,26	314,08	22	6909,76
Керівник	65,00	520	1	520
Консультант по економічній частині	62,00	496	0,25	124
Консультант по охороні праці	62,00	496	0,25	124

Нормоконтроль	62,00	496	0,25	124
Всього (Зо)				7801,76

3) Витрати на додаткову заробітну плату визначаються у відсотках від основної. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

$$Зд=11\%Зо;$$

$$Зд= 7801,76*0,11 = 858,19 \text{ грн}$$

4) До складу собівартості НДР включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Відрахування до єдиного соціального внеску складає:

$$Зєсв=0,22*(Зо+Зд);$$

$$Зєсв=0,22*(7801,76+858,19) = 1905,19 \text{ грн.}$$

5) До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР.. У наукових закладах накладні витрати складають 40 -120% від основної і додаткової заробітної плати.

$$Рнакл= (Зо+Зд)*0,5;$$

$$Рнакл= (7801,76+858,19)* 0,5 = 4329,97 \text{ грн.}$$

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 2.4.

Таблиця 2.4 - Калькуляція планової собівартості

Статті витрат		Сума, грн.
1.	Матеріали	170,00
2.	Основна заробітна плата	7801,76
3.	Додаткова заробітна плата	858,19
4.	Відрахування до єдиного соціального внеску	1905,19
5.	Накладні витрати	4329,97
Планова собівартість (Спл)		15065,11

Плановий прибуток визначений по формулі:

$$\text{Ппл} = 0,1 * \text{Спл} = 0,1 * 15065,11 = 1506,51 \text{ грн}$$

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції.

Договірна ціна визначається по формулі

$$\text{Цнір} = \text{Спл} + \text{Ппл} = 15065,11 + 1506,51 = 16571,62 \text{ грн.}$$

Ціну реалізації встановлюємо з урахуванням ПДВ

$$\text{ПДВ} = 0,2 * \text{Цнір} = 0,2 * 16571,62 = 3314,32 \text{ грн.}$$

Звідси ціна реалізації становить:

$$\text{Цр} = \text{Цнір} + \text{ПДВ} \quad \text{Цр} = 16571,62 + 3314,32 = 19885,94 \text{ грн.}$$

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		57

3 ОХОРОНА ПРАЦІ

Вступ

Сучасний розвиток технічного та технологічного стану виробництва передбачає постійну автоматизацію та оптимізацію виробничих процесів. Сьогодні, напевно, важко уявити компанію, господарська діяльність в якій здійснювалась би без використання комп'ютерної техніки.

Через масовий характер робіт, що виконуються працівниками за допомогою комп'ютера, законодавством України чітко врегульовано норми та вимоги до використання комп'ютерної техніки на підприємстві, безпосередньо й охорона праці при роботі з комп'ютером.

Життєвий цикл побудови систем безпеки - відеоспостереження, сигналізації, охорони периметра або СКС для їх взаємозв'язку містить важливий етап, який називається "побудова системи безпеки". Саме на цьому етапі триває реалізація проекту. При цьому при виконанні монтажних робіт працівник може мати справу з низкою небезпечних та шкідливих виробничих факторів.

Аналіз умов праці й забезпечення безпеки при виконання основних видів робіт на об'єкті дипломного проектування

Монтажник слаботочних систем безпеки може працювати різних кліматичних умовах, тобто. бути схильний до впливу високих і низьких температур, різної вологості і т.д.

Для підготовки та прокладання трас систем безпеки потрібне проведення робіт з електроінструментом (перфоратори, шуруповерти, болгарки), на різних висотах (із застосуванням сходів та настилів), часто - проводячи підключення до діючих електроустановок.

Розробка заходів з охорони праці

До роботи в якості інженера (наладчика) засобів зв'язку відеоспостереження допускаються особи, які досягли 18 років, придатні за станом здоров'я, що пройшли вступний інструктаж і первинний інструктаж на

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		58

робочому місці, навчання і перевірку знань вимог охорони праці в установленому порядку.

Під час проведення робіт на об'єктах працівникам необхідно:

- Знати шляхи евакуації при аваріях або пожежі, місця розміщення первинних засобів пожежогасіння, вміти їх застосовувати;
- Знати місце розташування засобів надання першої (долікарської) допомоги, вміти надавати першу (долікарську) допомогу потерпілим при нещасному випадку;
- Знати і дотримуватися правил особистої гігієни.

Вимоги безпеки при роботах на висоті

Перед початком робіт на висоті слід оглянути використовувані майданчики, драбини, настили і інші допоміжні засоби підмоцнування, перевірити їх справність. Переносні засоби повинні мати непрострочену дату періодичних випробувань, неслизькі підстави і допуск до експлуатації

Робочий одяг, взуття та інших засобів індивідуального захисту повинні бути справні, надіті без звисаючих частин, застебнуті на всі кріплення, відповідати кліматичним умовам в день роботи.

До початку робіт необхідно оглянути робочі місця, перевірити їх підготовленість до роботи, наявність достатнього освітлення, евакуаційних шляхів, відсутність захащеності. Підготувати необхідний інструмент, пристосування, матеріали та засоби (тару) для їх перенесення.

При роботах на висоті слід керуватися інструкцією з охорони праці при виконанні робіт на висоті, виконувати відповідні вимоги, в тому числі:

- дотримуватися вимог дій на висотних майданчиках (відступи від країв майданчиків, застосування запобіжних поясів, інформування розташованих нижче працівників про небезпеки і небезпечних зонах, огороження небезпечних зон і т.д.);
- дотримуватися вимог роботи з переносних драбин (стійке розташування підстави, кут нахилу сходів, максимальна висота і умови роботи з драбин, підняття вантажу, місця використання цих коштів і т.д.).

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		59

– забороняється передоручати або залучати до своєї роботи інших працівників без дозволу безпосереднього керівника.

– електромонтажні роботи на висоті необхідно проводити з риштувань з настилами шириною не менше 1 м, що мають надійне огородження у вигляді поручнів висотою не менше 1 м, а також з справних драбин і приставних драбин.

– забороняється підкидання будь-яких предметів для подачі працюючим нагорі. Інструменти, матеріали та інші предмети необхідно подавати за допомогою мотузки, до середини якої їх прив'язують. Другий кінець мотузки повинен знаходитися в руках у стоїть внизу працівника, який утримує піднімаються предмети від розгойдування.

– при виконанні монтажних робіт дозволяється застосовувати тільки справний ручний інструмент. Ручний інструмент не повинен мати пошкоджень (тріщин, сколів, вибоїн) робочих крайок, задирок і щербин в місці захоплення інструменту рукою працюючого, тріщин і задирок на потиличній частині рукояток.

Електробезпека

При роботі в електроустановках напругою до 1000 В, до яких відносяться і системи безпеки, без зняття напруги на струмопровідних частинах і поблизу них необхідно обгородити розташовані поблизу робочого місця інші струмопровідні частини електроустановки, що знаходяться під напругою, до яких можливий випадковий дотик, працювати в діелектричних калошах або стоячи на ізолюючій підставці або на діелектричному килимку, застосовувати інструмент з ізолюючими рукоятками (у викруток, крім того, повинен бути ізольований стрижень). При відсутності такого інструменту користуватися діелектричними рукавичками, працювати в головному уборі і в одязі.

Безпечне виконання робіт на об'єкті, відсутність травматизму та збереження людського життя завжди засноване на знанні та бездоганному дотриманні правил охорони праці, пожежної безпеки та електробезпеки. Це важливо пам'ятати і без порушень проводити будівництво та експлуатацію об'єктів.

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		60

ВИСНОВКИ

Будь-яке підприємство, незалежно від сфери господарської діяльності, масштабу та інших параметрів постійно перебуває у середовищі загроз та ризиків. Це неминуче. У цьому ризики може бути як внутрішніми, і зовнішніми. Якщо розділити комплексну систему захисту на складові, можна виділити одне з напрямів захисту – застосування технічних засобів охорони. Під технічною системою охорони (ТСО) у разі розуміється система раннього виявлення загроз фірмі від стихійних лих, несанкціонованого проникнення порушників і помилкових чи неправомірних дій обслуговуючого персоналу чи клієнтів фірми. Включення до складу системи захисту ТСО значно підвищує ефективність загальної системи захисту. Так, з загрози типу пожежі, спалахів блокуються застосуванням автоматичних систем пожежної сигналізації та, по необхідності, пожежогасіння та димовидалення. Захист від крадіжок, грабежів, розкрадань та несанкціонованого досуту забезпечать системи охоронної сигналізації. Контроль за персоналом, контроль доступу загалом, захист від НСД – застосування систем контролю та управління доступів. Системи відеоспостереження як один з найпоширеніших компонентів ТСО дозволяють вести віддалений контроль за будь-яким об'єктом, а також інтегруватися з іншими підсистемами ТСО. В цілому, застосування технічних засобів охорони на різних рубежах об'єкта – запорука безпечної роботи та прагнення побудови системи безперервності бізнесу (BSM).

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		61

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дворський М.Н., Палатченко С.Н., – Безпека об'єктів підприємництва, том 1, Київ, видавництво А-Депт, 2006
2. Сенилов В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации: учебник для нач. проф. Образования / В. Г. Сенилов – Москва: Издательский центр «Академия», 2010. – 512 с.
3. А. Лыткин. IP - видеонаблюдение. Наглядное пособие // Издательство “Авторская книга”, 2011. – 200 стр.
4. А. Маркевич. Расчет видеоархива и сети [электронный ресурс]. Режим доступа: <http://markevich.by/raschet-videoarxiva-propusknoj-sposobnosti-seti>
5. ГСТУ 78.11.001-98 Укріпленість об'єктів, що охороняються за допомогою пультів централізованого спостереження державної служби охорони - Київ, 1998 р. - 19 с.
6. ДБН А.2.2-2-96. Державні будівельні норми України. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.—Держкоммістобудування України.— К., 1996.
7. ВБН.В.2.5.-78.11.01 – 2003 Інженерне обладнання будинків і споруд. Системи сигналізації охоронного призначення - Київ, 2003 р. - 56 с.
8. Д.Р.Рыжова Проектирование и исследование комплексных систем безопасности Учебное пособие Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, 2012 г.
9. Лідньов А. О. Інструкція з охорони праці для техніки кабельних систем
Джерело: <https://www.sop.com.ua/article/1107-nstruktsya-z-ohoroni-prats-dlya-tehnka-strukturovano-kabelno-sistemi> Повне або часткове копіювання будь-яких матеріалів сайту, цитування, публікація їх а [Електронний ресурс] / Анатолій Олександрович Лідньов // МСFR - довідник спеціаліста з охорони праці. – 2020.

– Режим доступу до ресурсу: <https://www.sop.com.ua/article/1107-nstruktsya-z-ohoroni-prats-dlya-tehnika-strukturovano-kabelno-sistemi>.

10. Стайкуца С. В. Анализ и обоснование выбора периметральных систем охраны / С. В. Стайкуца, С. А. Дигол, К. С. Седов. // Сборник тезисов третьей всеукраинской научно-практической конференции "Перспективные направления защиты информации", ОНАС им. А.С.Попова. – 2017. – С. 72–76.

11. IP видеокamera Dahua DH-IPC-HFW2439SP-SA-LED-S2 [Электронный ресурс] // Dahua-technology. – 2021. – Режим доступу до ресурсу: <https://dahua-technology.com.ua/dahua-dh-ipc-hfw2439sp-sa-led-s2>.<https://dahua-technology.com.ua/ip-videokamera-dahua-dh-ipc-hdw1320sp-s3-28-mm>

12. AI сетевой видеорегиcтpатор Dahua DHI-NVR2216-16P-I [Электронный ресурс] // Dahua-technology. – 2021. – Режим доступу до ресурсу: <https://dahua-technology.com.ua/dahua-dhi-nvr2216-16p-i>.

13. КАБЕЛЬ МЕРЕЖЕВИЙ ОК-NET UTP CAT.5E [Электронный ресурс] // Brain. – 2021. – Режим доступу до ресурсу: https://brain.com.ua/ukr/Kabel_merejheviy_OK-Net_UTP_305m_cat5e_KPV-VP_350_4_2_0_50-p375372.html?utm_content=shopping&gclid=CjwKCAjw4ayUBhA4EiwATWYBrvKWFlhmAgPyV6FE6VmI-OgxmB-52BrkxfOFquQYtoRuN5TIM5uxihoCmmkQAvD_BwE.

					КС.55.07.000.ДП ПЗ	Лист
Изм.	Лист.	№ докум.	Подп.	Дата		63