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

Автоматика та телекомунікації
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри

_____

_____
(підпис) (ініціали, прізвище)

"___"_____2021 р.

Випускна кваліфікаційна робота

магістра
(освітньо-кваліфікаційний рівень)

на тему Дослідження та розробка мультифункціональної мережі для системи безпеки периметра об'єкта

Виконав : студент 2 курсу, групи ТКРзм-19
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)

Дриль Д.О. _____
(прізвище та ініціали) (підпис)

Керівник к.т.н., доц. Воропаєва А.О. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Покровськ – 2021 р.

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

Автоматика та телекомунікації
(повна назва кафедри)

Захист відбувся_____
(дата)
з оцінкою _____
секретар ДЕК_____
(підпис)

Випускна кваліфікаційна робота

магістра
(освітньо-кваліфікаційний рівень)

на тему Дослідження та розробка мультифункціональної мережі для системи безпеки периметра об'єктав

Виконав студент групи ТКРзм-19 Дриль Д.О.
(підпис, дата) (ініціали, прізвище)

Керівник Воропаєва А.О.
(підпис, дата) (ініціали, прізвище)

Зав. каф. автоматики та телекомунікацій _____.
(підпис, дата) (ініціали, прізвище)

Консультанти _____
(підпис, дата) (ініціали, прізвище)

_____.
(підпис, дата) (ініціали, прізвище)

_____.
(підпис, дата) (ініціали, прізвище)

Нормоконтролер Д.О.Жуковська
(підпис, дата) (ініціали, прізвище)

Покровськ – 2021 р.

ДВНЗ «Донецький національний технічний університет»

Факультет комп'ютерно- інтегрованих технологій, автоматизації електроінженерії та радіоелектроніки
Кафедра автоматика та телекомунікації
Освітній ступінь магістр
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ:
Завідувач кафедри
_____ /_____/
"____" _____20___року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІАЦІЙНУ РОБОТУ СТУДЕНТУ

Дрилю Денису Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження та розробка мультифункціональної мережі для системи безпеки периметра об'єктав

керівник роботи: к.т.н., доц. Воропаєва Анна Олександрівна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом від " " 20 року №
2. Строк подання студентом роботи _____
3. Вихідні дані до роботи: результати науково-дослідної роботи, магістерської практики.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1) Зв'язок питань безпеки об'єктів з телекомунікаційними технологіями;
2) Характеристика об'єкту, для якого буде спроєктована система;
3) Класифікація охоронних систем периметру;
4) Класифікація систем відеоспостереження;
5) Опис технологичного рішення системи охорони периметру;
6) IP-проектування
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
1) план об'єкту ;
2) типова схема організації;
3) монтажна схема;
4) схема розподілу адресного простору;
5) імітаційна модель;

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1			
2			
3			
4			

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Проходження практики	01.02-14.02.2021	
2	Визначення об’єкту дослідження	01.02-14.02.2021	
3	Дослідження предметної області	15.02-28.02.2021	
4	Класифікація систем охорони периметру	01.03-21.03.2021	
5	Розробка технологічного рішення	22.03-11.04.2021	
6	IP-проектування	12.04-25.04.2021	
7	Охорона праці та безпека життєдіяльності	26.04-05.05.2021	
8	Написання пояснювальної записки	06.05-10.05.2021	

Студент _____ **Дриль Д.С.**
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ **Воропаєва А.О.**
(підпис) (прізвище та ініціали)

Лист зауважень

Посада П.І.Б.	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Дриль Д.О. Дослідження та розробка мультифункціональної мережі для системи безпеки периметра об’єкта / Випускна кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 172 «Телекомунікації та радіотехніка». – ДВНЗ ДонНТУ, Покровськ, 2021.

Робота містить 106 сторінок, складається з вступу, чотирьох розділів, висновків, переліку використаних джерел з 13 найменувань, 14 рисунків, 11 таблиць, 1 додатку

Магістерська робота направлена на дослідження та розробку мультифункціональної мережі для системи безпеки периметра об’єкта.

В роботі проведено аналіз підходів до реалізації систем безпеки та охорони периметру. Визначено роль телекомунікаційних технологій при побудові мереж для таких систем. При розробці рішення проаналізовані основні технологічні рішення, обрані необхідні технології, мережа що була запропонована є мультифункіцональною, і окрім охоронних функцій ще надає послуги зв’язку між постами охорони а також є базовою для системи відеоспостереження. Окремим розділом розглянуті питання кіберзахисту та кібербезпеки.

Практична цінність отриманих результатів полягає в можливості використання проектного технічного рішення для подальшого впровадження в телекомунікаційну інфраструктуру для об’єктів що потребують охорони периметру.

Ключові слова: МРЕЖА, БЕЗПЕКА, КІБЕРЗАХИСТ, ОХОРОНА, МОДЕЛЬ, ІНФРАСТУРКТУРА, ГОЛОСОВИЙ ЗВ’ЯЗОК, IP-КАМЕРА, КІБЕРБЕЗПЕКА, СХЕМА.

ABSTRACT

Drill D.O. Research and development of a multifunctional network for the security system of the perimeter of the object / Graduation qualification work for the degree of "master" in the specialty 172 "Telecommunications and Radio Engineering". - SHEI DonNTU, Pokrovsk, 2021.

The work contains 106 pages, consists of an introduction, four sections, conclusions, a list of sources used with 13 titles, 14 figures, 11 tables, 1 appendix

The master's thesis is aimed at research and development of a multifunctional network for the security system of the perimeter of the object.

The paper analyzes the approaches to the implementation of security systems and perimeter protection. The role of telecommunication technologies in the construction of networks for such systems is determined. During the development of the solution, the main technological solutions are analyzed, the necessary technologies are selected, the proposed network is multifunctional, and in addition to security functions, it also provides communication services between security posts and is the basis for video surveillance. A separate section addresses issues of cybersecurity and cybersecurity.

The practical value of the obtained results lies in the possibility of using the design technical solution for further implementation in the telecommunications infrastructure for facilities in need of perimeter protection.

Keywords: NETWORK, SECURITY, CYBER PROTECTION, SECURITY, MODEL, INFRASTRUCTURE, VOICE COMMUNICATION, IR CAMERA, CYBER SECURITY, SCHEME.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CELP	- codebook excited linear prediction
DSP	- digital signal processor
MGCP	- Media Gateway Control Protocol
MP-MLQ	- multipulse, multilevel quantization
QoS	- Quality of Service
SIP	- Session Initiation Protocol
SNMP	- Simple Network Management Protocol
ToS	- Type of Service
ПЗ	- програмне забезпечення
ТфЗК	- телефоні мережі загального користування

ВСТУП

В сучасному світі будь-яка виробнича діяльність або надання послуг населенню неможливі без відповідної інформаційно-комунікаційної інфраструктури та особливо без належного рівня охорони. Корпоративні телекомунікаційні мережі стають необхідною складовою бізнес-організацій, що забезпечує можливість ефективного функціонування. Разом з тим, витрати на створення і функціонування такої мережі, мають бути науково обґрунтовані.

Питання забезпечення безпеки на сьогоднішній день як ніколи актуальні в організації будь-якого масштабу і області роботи.

Метою даної роботи є забезпечення рівня безпеки пермитру об’єкту з використанням телекомунікаційних технологій.

Об'єктом дослідження є інфраструктура об’єкту охорони

Предмет дослідження – технології захисту периметру.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Обрати та проаналізувати структури організації корпоративної мережі.
2. Виявити вузькі місця і критично вразливі мережеві елементи.
3. Провести аналіз можливих методів організації захисту.
4. Розробити рекомендації до побудови захищених мереж.
5. Перевірити прийняті рішення на імітаційної моделі.

Дослідження параметрів та розробка імітаційних моделей базувалась на реальній корпоративній мережі Індустріального парку Біла Церква..

В результаті виконання роботи був розроблений і перевірений комплекс заходів щодо підвищення рівня захисту критично важливих елементів Індустріального парку Біла Церква, поставлена мета була досягнута. Отримані результати можуть бути впроваджені на підприємстві.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ. ПОСТАНОВКА ЗАДАЧІ ТА ВИЗНАЧЕННЯ ОБ'ЄКТУ

1.1 Зв'язок питань безпеки об'єктів з телекомунікаційними технологіями

Питання безпеки останнім часом набувають все більшої актуальності. Слід зазначити що все більше технологій, продуктів, розробок та об'єктів ще на стадії проектування повинні забезпечувати необхідний рівень захисту незалежно від типу джерела загрози. Головний принцип комплексних систем безпеки – забезпечення заданого рівня захисту від загроз за умови мінімального рівня витрат на охорону та безпеку. На сьогоднішній день галузь безпеки умовно можна представити на наступній діаграмі (Рисунок 1.1).

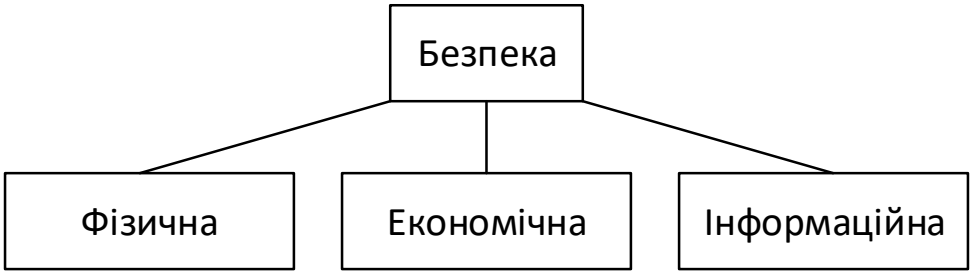


Рисунок 1.1 – Галузь безпеки

Кожен з заявлених напрямів має історичне підґрунтя і напрацьовувався роками. Беззаперечно, безпека об'єкту першочергово передбачає саме фізичну безпеку об'єкту.

За дотримання фізичної цілісності відповідають комплексні рішення які мають в собі як технічні так і фізичні засоби охорони. До таких засобів зазвичай відносять:

- наряди швидкого реагування;
- системи периметриальної охорони;
- системи відеоспостереження;

- підсистеми контрольно-пропускних пунктів;
- системи аерофотозйомки;
- системи фізичних засобів з обмеження до території об’єктів охорони.

Галузь економічної безпеки більш складна ніж попередня, і включає в себе кілька відокремлених напрямів, які мають як суто економічне спрямування так і технічне. До економічного напряму відносять дослідження кон’юнктури ринку, де працює підприємство та своєчасне реагування на виклики, які формуються цим ринком та конкурентами. До технічного напряму економічної безпеки відносять застосування криптографічних технологій, технологій захисту банківської таємниці, технічного захисту об’єктів інтелектуальної власності і т.д.. Метою цього напрямку є саме використання технічних та технологічних рішень захисту від крадіжки або втручання у будь які процеси на об’єкті охорони, що в перспективі може призвести економічний крах об’єкта охорони.

Інформаційна безпека – найбільш актуальна та всеоохоплююча галузь безпеки у світі, що сьогодні дуже динамічно розвивається. Забезпечення інормаційної складової безпеки надає значні переваги для кінцевих замовників комплексних послуг. Ці переваги полягають в розробці як інфраструктурних так і методологічних рішень та політик, що мають вплив як на персонал об’єктів так і на всю організаційну структуру підприємства.

Всі три складові будь-яких безпекових рішень сьогодні дуже тісно пов’язані з телекомунікаційними рішеннями, а саме для забезпечення фізичної, економічної та інформаційної безпеки використовується телекомунікаційна інфраструктура та мережі передачі даних.

Приведемо прості приклади:

- політика фізичного захисту об’єктів охорони забезпечується використанням технічних засобів, таких як камери, системи контрольно-пропускних пунктів, системи ідентифікації, системи стаціонарного та радіозв’язку. Задля організації можливості доступу до інформації та швидкого реагування і прийняття рішенн використовуються мережі зв’язку. Саме від коректності їх

проєктування та правильності впровадження залежить цілісність даних та швидкість їх передачі;

- політика економічного захисту передбачає використання телекомунікаційної інраструктури підприємтсва для ведення аналітичної та звітної роботи з економічного аналізу, бухгалтерського обліку та інших задач, що пов’язані з функціонуванням підприємства. Так само як і в попередньому випадку надійність та захищеність телекомунікаційної інфраструктури надає впенвненість в тому, що критично важливі дані будуть убезпечені та цілісні для подальшого їх використання дозволеним колам осіб;
- інформаційна складова безпеки передбачає розробку комплексних рішень в області функціонування підприємства. Тут має місце і реалізація політик кіберзахисту і політики поведінки співробітників об’єкту охорони у публічному інформаційному просторі, незалежно від того чи то мережа Інтернет, чи то звичайне спілкування. Важливим чинником успіху в інформаційній безпеці є саме телекомунікаційна мережа, бо вона на сьогоднішній тісно переплилась з будь-якими процесами на будь-яких підприємствах та установах.

Саме забезпечення надійності, стійкості та захищеності телекомунікаційної інфраструктури дає можливість реалізувати безпекові рішення за всіма напрямками. Від коректності прийнятих рішень на стадії проектування залежить наскільки швидко будуть передаватись інформаційні потоки у системах контролю доступу, як будуть проходити транзакції та банківські розрахунки, як буде забезпечуватись інформаційна цілісність на об’єкті охорони, і як саме буде захищена територія підприємства, організації або установи від зовнішніх вторгненнь. Саме мультифункціональна телекомунікаційна мережа є вагомою складовою безпеки об’єкту охорони.

1.2 Постановка задачі дослідження та розробки

Наведена до вашої уваги кваліфікаційна робота магістра присвячена розробці мультифункціональної мережі для системи безпеки периметру об’єкта охорони. Як зазначалось і було доведено у попередньому пункті поточної глави, саме мережеві рішення є залогом коректно працюючої системи охорони об’єктів, тому в данній роботі, на прикладі одного з об’єктів буде реалізована та досліджена комплексна система безпеки периметру, яка повинна включати в себе такі складові:

- система відеоспсотереження;
- система зв’язку;
- система контролю цілісності пермитриальної огорожі.

На першій стадії дослідження необхідно обрати об’єкт, для якого буде розроблятись мультифункціональна мережа безпеки. Виходячи з ключових параметрів, що потрібно контролювати в магістерській кваліфікаційній роботі слід дослідити існуючі рішення в галузі побудови систем безпеки периметрів територіально розподілених об’єктів, визначити такі, що найбільш підходять до конкретного обраного об’єкту. Вже на підставі обраних рішень з забезпечення безпеки провести синтез мультифункціональної телекомунікаційної мережі, обрати необхідні протоколи та технології роботи, виконати апаратний синтез, та окремо провести розробку політики кібербезахисту для розробленої мультифункціональної мережі. Розробка політики кіберзахисту включатиме в себе кілька основних етапів:

- моделювання роботи мережі;
- пошук вузьких місць в мережі, усунення цих місць;
- перевірка гіпотез щодо вразлиовстей від зовнішніх чинників.

Отже перейдемо до наступного етапу, а саме опису об’єкту, для якого будуть проводитись вишуківальні роботи з розробки мультифункціональної мережі.

1.3 Характеристика об’єкту, для якого буде спроєктована система

Для проведення якісного дослідження слід обрати великий територіально-розподілений об’єкт. Таковим може стати або промислове підприємство, або ж індустріальний парк. Найбільш цікавим до розгляду може стати індустріальний парк, через те що це зазвичай абсолютно нове будівництво або ж докорінна модернізація існуючих старих промислових забудов. В чим полягає саме оптимальність вибору саме індустріального парку, так у тім, що даний клас об’єктів зазвичай містить велику кількість контрольно-пропускних пунктів, має складні логістичні ланки як зовнішні так і внутрішні, а також велику кількість окремих юридичних осіб, інформаційні та логістичні потоки яких повинні бути ізольованими, і не перетинатись з іншими структурами, що знаходяться на території індустріального парку. В якості такого об’єкту серед різноманіття новоутворених парків буде обрано «Індустріальний Парк – Біла Церква». На рисунку 1.2 наведено розташування парку на карті та його географічні переваги.

Рисунок 1.2 – Розташування індустріального парку

Індустріальний парк або промисло́вий парк — територія, виділена для промислового розвитку. Зазвичай індустріальні парки розташовані на території колишніх промислових зон, або ж будуються з нуля, за умови наявності інфраструктури водопостачання та водовідведення, достатньої потужності електромережі, можливості підключення до розподільчих газових мережі та близькості до логістичних хабів. Якщо більш конкретизувати визначення індустріального парку, то це визначена нормативними документами певна територія, облаштована технологічною інфраструктурою, у межах якої учасники індустріального парку можуть здійснювати господарську діяльність у сфері промислового виробництва, науково-дослідну діяльність, діяльність у сфері інформації і телекомунікацій [3]. У якості додаткового і вагомого бонусу підприємства, що працюють в індустріальному парку, мають низку податкових і законодавчих пільг. Метою створення таких парків є забезпечення підприємств спільною розвиненою інфраструктурою та забезпечення контролю над виробництвом та впливом на довкілля. Порядок створення, діяльності індустріальних парків на території України регламентується законом України про «Індустріальні парки»[1]. Промислові парки зазвичай розташовуються на околицях міст або поза основними житловими районами міста, зазвичай забезпечується гарною транспортною доступністю, в тому числі автомобільним і залізничним транспортом.

Промислові парки часто створюються навколо портів, аеропортів, залізниць та інших транспортних вузлів, що дозволяє зменшити транспортні витрати. Часто створення промислових парків проводиться в рамках програм з економічного розвитку, а підприємствам у них надаються певні пільги.

Ініціаторами створення індустріальних парків можуть бути органи державної влади, органи місцевого самоврядування, юридичні або фізичні особи, які мають право на створення індустріальних парків на землях державної, комунальної чи приватної власності. Індустріальний парк створюється на строк не менше 30 років, Для надання державної підтримки, уповноважений

державний орган створює, веде та розміщує на своєму офіційному веб-сайті реєстру індустріальних парків.

Такий тип освоєння території заснований на декількох концепціях:

- є можливість зосередитися для розгортання спеціалізованої інфраструктури (залізничні під'їзні шляхи, порти, потужні електричні джерела, джерела подачі газу), що часто не по силу окремому підприємству;
- розгортання нового бізнесу стає більш дешевим, якщо використовується інтегрована інфраструктура в одному місці;
- суміжні підприємства (особливо хімічної промисловості) можуть проектуватись так, що в виробничому ланцюгу вони можуть взаємно доповнювати ланцюг виробництва товарів;
- відокремлені райони для промислових цілей більш легко контролювати з точки зору екології [2].

Саме виходячи з цих приорітетів в був організований Індустріальний парк – Біла Церква. Розташування парку проілюстровано на рисунку 1.3.

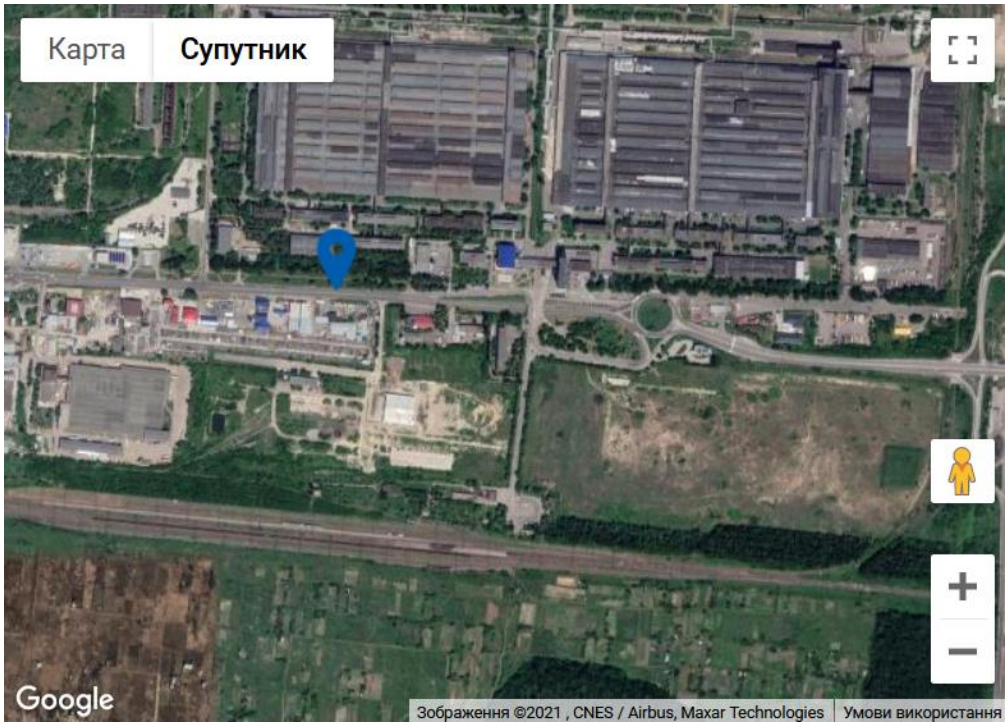


Рисунок 1.3 – Розташування ІП-Біла Церква

Індустріальний парк "Біла Церква" розташований на відстані 75 км від Києва, у місті Біла Церква. Наявність аеродрому, двох залізничних станцій та міжнародної автомагістралі створює зручну логістику та дозволяє легко отримати доступ до найбільших ринків країни. Основні логістичні маршрути та канали у безпосередній близькості до Індустріального парку:

- траса Е95 - Гельсінкі – Київ – Одеса – Димитровград – Александруполіс;
- траса Р32 - Кременець — Біла Церква;
- залізнична гілка на території парку;
- залізнична станція Роток;
- міжнародний аеропорт "Бориспіль";
- білоцерківський вантажний авіаційний комплекс.

Індустріальний парк "Біла Церква" створено на території Шкарівської селищної ради Білоцерківського району Київської області та включено до Реєстру індустріальних (промислових) парків 13.04.2018 року.

Ініціатор створення – ТОВ "Індустріальний парк "Біла Церква 1".

Загальна площа – 35,6 га.

Строк, на який створюється індустріальний парк – 50 років.

Основною метою створення є забезпечення економічного розвитку та підвищення конкурентоспроможності регіону, активізація інвестиційної діяльності, підвищення рівня зайнятості населення, розвиток сучасної виробничої та ринкової інфраструктури.

Функціональне призначення: машинобудування та металообробка; легка та харчова промисловість; деревообробна та меблева промисловість; інші галузі, сумісні із вищезазначеними.

Для створення необхідної інженерної інфраструктури індустріального парку необхідно залучити орієнтовно 117,4 млн. грн. та на проведення будівництва й облаштування об'єктів індустріального парку – 2 740 млн. грн. за рахунок коштів ініціатора створення, керуючої компанії, учасників парку, інвесторів, банківського фінансування.

Відповідно до очікуваних результатів функціонування індустріального парку передбачається створення близько 3000 нових робочих місць.

Впродовж 2018 – III кварталу 2019 року ініціатором створення забезпечено виконання ряду заходів:

- розроблено і затверджено детальний план території, отримано містобудівні умови і обмеження;
- отримано технічні умови, розроблено та погоджено проекти газопостачання, водопостачання та водовідведення (узгоджені інженерні потужності: водопостачання/водовідведення – 800 м3/добу, газопостачання – 2000 м3/год, електропостачання – 2 мВт з можливістю збільшення за необхідності);
- здійснюється будівництво зовнішніх мереж водопостачання та водовідведення;
- розробляється проект електропостачання.

Також розроблено проектну документацію об’єкта "Нове будівництво швейно-в’язальної фабрики", здійснено комплексну експертизу проекту та отримано позитивний висновок за результатами експертизи.

На зазначені роботи ініціатором створення індустріального парку залучено коштів на 2,87 млн. грн.

У зв'язку з будівництвом офісного приміщення площею 1,4 тис. м2 (з якої вільною залишається 1,1 тис. м2) для задоволення потреб потенційних учасників індустріального парку вільна площа парку зменшилась на 2 га та становить 22,05 га [4].

На рисунку 1.4 наведено схематичне розташування та наповнення Індустріального парку. Як виходить з даного рисунку, територія об’єкту доволі складна. Загальна довжина огорожі об’єкту становить майже 5,5 кілометрів, і вона представлена двома прямокутниками з розмірами 0,4х1,1 км.

Рисунок 1.4 – Схематичний план розташування об’єкту

1.4 Особливості впровадження систем периметральної охорони

Система охорони периметра забезпечує спробу проникнення в особу, що охороняється, на першій лінії безпеки, тобто по периметру. Таким чином, пімметричні пристрої безпеки є найефективнішим засобом запобігання несанкціонованому проникненню, оскільки зловмисник подасть сигнал тривоги задовго до того, як зловмисник потрапить у найважливіші зони.

Системи безпеки по периметру займають особливе місце в тканині систем безпеки. Функція захисту периметра, як правило, ідентифікується як специфічна технічна функція. Для початку важливо визначитися з концепцією периметра. У нашому випадку периметр можна вважати межею заповідної зони об’єкта, і несанкціоноване перетинання призведе до сигналу тривоги з більш-менш точним сигналом.

Конструктивні особливості системи безпеки периметра пов’язані з тим, що територія охороняється, як правило, вона велика за довжиною, а інспектори охорони охоплюють великі площі (від 30 до 500 метрів на одного інспектора). Датчики встановлені на різних конструкціях і вимагають важких будівельних робіт під час монтажу. Методи безпеки периметра працюють цілий рік за зовнішніх умов, і їх слід враховувати при виборі обладнання.

Ефективність системи охорони периметра може бути збільшена в рази і в той же час експлуатаційні витрати можуть бути зменшені, якщо система відеоспостереження встановлена системою охорони периметра. Механічні бар’єри (стіни, огорожі) дозволяють загарбнику проникнути і охолодитися, дзвін-розбійник допомагає ідентифікувати загарбника за короткий час, а система відеоспостереження усуває помилкову тривогу і бачить справжню причину [5].

Системи охорони периметру можуть проходити і монтуватись на кількох типах меж:

- паркан із залізобетону, цегли, профнастилу, жорсткої металевої решітки, сітки, живоплоти;
- глуха стіна будівлі або споруди;

- стіна з вікнами, воротами, дверима, виходами вентиляційних шахт
- покрівля;
- водні об'єкти та берегова лінія;
- ворота, КПП, хвіртки, інші елементи з огорожею і у вигляді відкритої території.

Через різнорідності меж в рамках одного об'єкту, що охороняється може використовуватися кілька типів охоронних пристроїв з об'єднаним або незалежним управлінням, засобами оповіщення, контролю. Власне у випадку саме нашого об’єкту так і відбуватиметься. Периметр - найважливіший фактор безпеки, тому вимоги до обладнання будуть зростати. Якісне обладнане і добре освітлена ділянка відрізняє вторгнення від дощу, снігу або вітру, не реагуючи на птахів і дрібних тварин. Для зменшення ймовірності помилок використовується логіка дисперсійного аналізу: монітор перевіряє показники прилеглих датчиків. Якщо такі індикатори присутні на прилеглих територіях, то вважається що це системне явище, тому в погану погоду немає ніяких труднощів.

Залежно від ситуації і активності може статися одна або кілька дій, що вказують на порушення безпеки:

- інформація консолі оператора;
- світлові і звукові сигнали в зонах;
- сповіщення на телефони, комп'ютери, монітори, монітори та інші пристрої;
- включення ламп по всій території або навколо неї для полегшення виявлення;
- відправка фотографії місцевості, де людина може бути знайдена;
- посилення контрольних заходів, фіксація дій злочинців;
- автоматичне закривання дверей і воріт, пускові системи, призначені для систем активної безпеки.

Щоб виключити наслідки перебоїв на коротких ділянках, додатковий захист обладнання або ж дублюючі пристрої встановлюється кожні 100-150 метрів, щоб обрізка однієї ділянки не впливала на роботу іншого обладнання.

1.5 Висновки за розділом

Перший розділ роботи присвячено аналізу об’єкту, визначення актуальності та постановка задачі проектування, наведена кореляція питань безпекових рішень та телекомунікаційних мережі і інфраструктурних рішень, також приділена увага особливостям впровадження систем периметральної охорони.

РОЗДІЛ 2. АНАЛІЗ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ, ЯКІ МОЖУТЬ БУТИ ВИКОРИСТАНІ ДЛЯ ВИРІШЕННЯ ПОСТАВЛЕНОЇ ЗАДАЧІ

2.1 Класифікація охоронних систем периметру

Розрізняють видів систем охорони периметру. Розглянемо кожну з них:

1. Ємнісна система безпеки периметру. Ємнісна система районної захисту складається з системи провідників з певною ємністю по відношенню до землі. При торканні або наближенні до огорожі їх потужність змінюється і спрацьовує сигнал тривоги.
2. Система вібрації для захисту периметра. Основною складовою такої системи охорони ділянки є спеціальний сенсорний кабель. Принцип дії заснований на трібоеффекте - виникненні електричного заряду при механічному впливі кабелю, і за типом електричного сигналу можна визначити тип удару. Перевага такої системи в тому, що її можна використовувати як на ґратчастих, так і на бетонних конструкціях. Також дана система може бути реалізована на базі отпичних сигналів і волоконної оптики.
3. Інфрачервона система охорони ділянки. Інфрачервоні системи можна розділити на два типи: активні і пасивні. Система активного периметра - це передавач і приймач, що випромінює кілька лінійних невидимих променів. Коли один або декілька з цих променів зникають, звучить сигнал тривоги. Відстань між передавачем і приймачем може становити від декількох метрів до сотень метрів, що дозволяє захистити великі площі правильної форми. Пасивні системи працюють за принципом виявлення теплового випромінювання від рухомого об'єкту в зоні виявлення. Залежно від лінзи сенсора зони можуть бути лінійними або мати тривимірні характеристики.

4. Система захисту від радіохвиль. Принцип роботи радіохвильових систем заснований на реєстрації збурень в електромагнітному полі, яке в це поле входить зловмисник. Тривимірна зона виявлення складається з «відкритою антени» - двох паралельних проводів (кабелів), до яких підключаються УКХ-генератор і приймач. Зона виявлення може бути як «Глазкової», так і «поверхневої», в будь-якому випадку надійно слідуючи по краю самої складної конфігурації.
5. Системи периметрового радіозахисту (провідний) використовуються для перекриття верхньої частини перил і дахів стаціонарних об'єктів, для захисту відкритих часових меж охорони, а також для посилення захисту на певних ділянках (ліс, прірва і т. Д.). Для захисту обгороджених територій, коли використання пасивних бар'єрів неможливо або небажано, він розробив радіохвильової систему, звану «вихідний хвилевід» (LVV), яка складається з двох паралельних кабелів, прокладених в землі по периметру. Зона виявлення досягає 3,5 м в ширину і 1,0 м у висоту. Система повністю замаскована і може бути виявлена тільки спеціальними пристроями.
6. Система радіопроменевого захисту периметру. Системи захисту від радіопроменів складаються з передавача і приймача, між якими створюється еліптичне електромагнітне поле. Якщо порушник потрапляє в зону дії цього поля, його амплітудно-тимчасові характеристики зміняться, що фактично реєструється трансівером. Ця система охорони периметра працює за принципом ефекту Доплера. Зона виявлення являє собою витягнутий еліпсоїд довжиною до 200 метрів і радіусом 5 метрів. Недоліком цих систем є помилкове спрацьовування через мінливих погодних умов.
7. Системи, чутливі до вібрації. Ці пристрої працюють на основі реєстрації механічної вібрації або деякої деформації огороджувальних конструкцій. В цьому випадку чутливим елементом виступає спеціальний сенсорний кабель. Він перетворює механічні коливання в

електричні сигнали. Бажано, щоб такий кабель кріпився до паркану. Сигнали виявляються аналізатором і генерують сигнал тривоги з використанням коаксіального або мікрофонного кабелю в якості чутливого елемента. Важливою особливістю їх є те, що вони точно повторюють профіль забору і не видно, сигналізація не спрацьовує належним чином через вібрації, створюваної проїжджаючими людьми або транспортними засобами.

8. Оптичні датчики з функцією сканування. Найсучаснішими вважаються оптичні аналоги. Це скануючі датчики, в яких в якості випромінювача використовується малопотужний лазер на напівпровідникових елементах. Ви можете розташувати датчик так, щоб його площина сканування була паралельна стіні. Так, ви з меншою ймовірністю отримаєте повідомлення про помилкові тривоги, так як сигнал тривоги буде згенеровано тільки в той момент, коли порушник наблизиться на неприпустиме відстань. Якщо площину сканування горизонтальна, датчик виявляє активність на відстані більше 30 м.
9. Бездротові датчики. Якщо прокладка кабелів неможлива або ускладнена з багатьох причин, використовуються спеціальні бездротові датчики. Вони живляться від незалежного джерела, а сигнал тривоги передається по радіоканалу. Сучасні модифікації економічні. У режимі очікування величина споживаного струму не перевищує декількох мікроампер.
10. Датчики одиночного положення. В якості альтернативи можна реалізувати деяку форми захисту [6].

Виходячи з наведеної класифікації, для умов об’єкту де буде розгортатись система захисту периметру можна реалізувати підходи засновані на використанні хвильових технологій. Таке рішення продиктовано саме територіальної розгалуженістю об’єкта та довжини огорожі. Таковою системою може виступити система, дія якої заснована на аналізі поведінки оптичного сигналу, що розповсюджується спеціальним сенсорним оптичним кабелем. Але

застосування тільки одного засобу охорони об’єкту не є доцільним, через те що в такому випадку неможливо буде ідентифікувати порушника периметру.

Ідея використання волокна як чутливий елемент витала в повітрі давно. Спочатку це були зонні системи на основі багатомодових волокон. Вони довели свою ефективність і розробили гарне програмне забезпечення за допомогою нейроаналіза. У нього є кілька недоліків. Кожен шматок волокна являє собою датчик. Це означає, що захищається контур розбивається на зони по 100 - 250 метрів, в які приварюється необхідну кількість смуг. Відповідно, місце опромінення може бути визначено з точністю до сотень метрів; волокна слід підготувати по колу. Чутливість цього методу також не дозволяє використовувати його при прокладці в землі.

Наступним кроком у розвитку технологій є рефлектометр, а точніше когерентний рефлектометр. Чутливий елемент являє собою класичний одномодовий оптичний кабель, що дозволяє знімати вібрації з кожного метра волокна до 10 кГц з високою чутливістю. Однією з особливостей систем є простий монтаж кабелю, але складність кінцевого обладнання. Отже, цей клас систем економічно ефективний при використанні на більш протяжних територіях, що перевищують 2 км.

Кабель можна прокладати одним кабелем по обом огорож, в тому числі легким, типу дротяної сітки, і в землю.

Для зменшення кількості помилкових спрацьовувань використовуються складні алгоритми, в тому числі елементи штучного інтелекту. Алгоритми з тематичними дослідженнями і можливістю підвищення кваліфікації використовуються в особливо складних умовах працевлаштування [7].

Джерелом випромінювання зазвичай є мініатюрні напівпровідникові лазери або світлодіоди. На виході кабелю випромінювання реєструється фотодетектором, який перетворює оптичний сигнал в електричний. Під час деформацій волокон змінюються умови внутрішнього відбиття, внаслідок чого фазові та просторові характеристики променя на виході кабелю змінюються, вони реєструються фотодетектором і обробляються аналізатором сигналів.

Оптичні волокна поділяються на багатомодові та одномодові. Діаметр серцевини багатомодових волокон зазвичай становить 50 ... 100 мкм. На такому волокні одночасно поширюється велика кількість типів хвиль (мод) з різними геометричними параметрами. Ці промені відчувають багатократні відбиття від інтерфейсу ядро-оболонка, що призводить до значного послаблення сигналу.

Діаметр серцевини одномодових волокон становить не більше 10 мкм. Лише один тип хвилі (мода) може поширюватися в такому волокні, і ослаблення світла тут набагато менше, ніж у багатомодових волокнах.

Оптичні системи безпеки використовують кілька методів для виявлення сигналів про вторгнення:

А. Метод реєстрації проміжних порушень

Напівпровідниковий лазер зазвичай генерує кілька десятків режимів (спектральних ліній), близьких до частот з певним розподілом енергії в спектрі випромінювання. Якщо багатомодовий оптичний кабель зазнає механічних навантажень, то на його виході спектр випромінювання зазнає змін, що дозволяють виявити деформації або вібрації кабелю.

В. Спосіб реєстрації спотової структури

На виході з багатомодового волокна спостерігається так звана «плямова структура», яка являє собою неправильну систему світлих і темних плям. Коли волокно деформується або вібрує, структура плям змінюється. Для виявлення деформацій кабелю тут використовуються чутливі до простору фотодетектори.

С. Метод інтерференції

Цей метод використовує принцип двопроменевої інтерферометрії. Лазерний промінь розділений на два і спрямований на два однакових одномодових оптичних волокна. На приймальному кінці два промені утворюють інтерференційну картину. Механічний вплив на чутливий кабель призводить до змін у схемі перешкод, що реєструються фотодетектором [8].

Основні характеристики оптичної системи захисту периметра:

- По периметру немає активного обладнання (немає електромагнітного випромінювання від датчика на периметрі), тому знайти оптичний кабель датчика складно або неможливо.
- Оптичний датчик повністю вибухо-і вогнестійкий.
- Можливість захисту складних і широких периметрів
- Нечутливість оптичного датчика до зовнішніх електромагнітних імпульсів, випромінювання і перешкод.
- Можливість використання в якості датчика стандартних типів оптичних кабелів зв'язку з міцної і надійної кевларовой оболонкою під зовнішньою ізоляцією.
- Можливість використання одного з вже встановлених контейнерів оптичного кабелю в якості датчика (інші контейнери використовуються для сигналів зв'язку в штатному режимі)
- Можливість інтеграції з високорівневими системами захисту периметра ієрархії (по протоколу MosBUS через з'єднання TCP / IP або через з'єднання сухого реле)
- Інтуїтивно зрозумілий графічний інтерфейс на робочому місці оператора системи безпеки
- Можливість диференціювати рівень доступу співробітників, що працюють з системою охорони периметра.
- Вести облік стану захищеної середовища з можливістю перегляду і застосування фільтрів на кшталт подій
- Можливість повідомити систему екстреної безпеки за допомогою SMS і / або електронної пошти
- З'єднайте кордону периметра з реальними географічними координатами за допомогою GPS
- Було вивчено набір нейроалгорітмов для виявлення інциденту / спроби порушення захисного периметра.
- Можливість включення віддаленого доступу до програмного забезпечення безпеки

- Вбудовані елементи для самостійної діагностики стану оптичного датчика
- Самодіагностика програмного забезпечення системи охорони периметра - в разі збою програмного забезпечення автоматичне відновлення роботи протягом 60 секунд.
- Захист доступу до програмної частини оптичної системи для захисту периметра за допомогою програмованого ключа.

Таким чином, можна сказати, що система захисту периметра Індустріального парку – Біла Церква буде реалізована на основі використання сенсорних оптичних кабельних систем.

2.2 Класифікація систем відеоспостереження

Для повноцінної реалзації захисту об’єкту, використання однієї системи периметриального контролю недостатньо. В разу виявлення місця порушення, виявити саме порушника не вдасться. Це пов’язано з неможливістю його ідентифікації. В такому випадку доцільно використовувати системи фіксації відеопорушень. Є два глобальних підходи – використання стаціонарних систем відеоспостереження, або ж використання мобільних комплексів аерофотозйомки. Другий підхід виглядає більш інноваційно, але при застосування дронів необхідно враховувати велику кількість чинників таких як погодні умови, затримка та низький рівень автономності (обмеженність у часі роботи). Виходячи з навкедених доводів, використання системи дронів не є раціональним тому більш правильним є застосування саме стаціонарних систем відеоспостереження.

Розглянемо типові системи відеоспостереження.

Аналогова система відеоспостереження

Залежно від типу використовуваного обладнання системи відеоспостереження поділяються на аналогові та цифрові. Аналогові системи відеоспостереження стали першопрохідцями на ринку відеоспостереження, але в чистому вигляді сьогодні рідко використовуються всюди. Скажімо, аналогові системи відеоспостереження можна простежити до минулої епохи в історії безпеки телевізійного спостереження, хоча шанувальників цієї рідкості все ще можна знайти.

Дійсно, основою аналогових систем були камери відеоспостереження - оптичні пристрої з ПЗС-матрицею, які генерують відеосигнал із потоку світла, який раніше проходив через лінзу та лінзу пристрою. У системі відеоспостереження відеоматеріали записувались на відеореєстратор та відображалися на моніторі, що визначало в першу чергу обмежені функції такої системи.

Щоб переглянути архів, не перериваючи запис, користувачеві потрібно встановити два відеореєстратори, а потім провести багато часу за стрічкою та скористатися спеціальним і дуже дорогим принтером під час друку потрібного кадру.

Іншими недоліками аналогової системи відеоспостереження є відсутність джерела для розширення своїх функцій, неможливість обслуговування більше одного аудіоканалу та необхідність постійного обслуговування - зміни касет, очищення та заміни заголовків відео на магнітофоні.

Істина полягає в тому, що системи відеоспостереження у вигляді вже встановлених камер спостереження та фахівців, навчених керувати ними, залишили велику спадщину, незважаючи на всі їх недоліки. У зв'язку з цим в наш час дуже поширені змішані системи (аналоговий сигнал - цифровий запис).

Цифровий відеореєстратор (DVR) постачається з жорстким диском, аналоговим входом для підключення коаксіального кабелю та аналогічним виходом для підключення монітора (відеореєстратора, який виконує функції мультиплексування та відеомагнітофона) або комп'ютерів з картою, що

використовується як відеозапис вбудований пристрій картки. спеціальне програмне забезпечення.

Треба сказати, що принципової різниці між побудовою систем відеоспостереження немає. Канали для передачі аналогових сигналів однакові, і їх кількість визначається вбудованою вбудованою кабельною системою, тобто системою кабельних елементів, що є засобом для передачі оптичних або електричних сигналів.

Є багато переваг перед системами відеоспостереження: більш якісна відеозапис, необхідність швидкого обміну джерелами пам’яті, можливість швидкого пошуку та відображення записаних подій. Крім того, завдяки наявності "інтелекту" у відеореєстраторі, напр. В. Датчик руху, аудіо- та відеозапис здійснюється лише під час руху об’єкта. Це значно спрощує процес відеоспостереження та економить простір. Жорсткий диск.

Звичайно, були деякі недоліки - найголовніше, попит на дорогі коаксіальні кабелі і, разом з цим, складність географічної структури розподіленої системи відеоспостереження, а також обмежена кількість відеореєстраторів, що ускладнює розширення зоровий комплекс. Крім того, перетворення сигналу з аналогового на цифровий і навпаки, яким би він не був, зменшує якісні характеристики зображення.

Незважаючи на вищезазначені недоліки, системи відеоспостереження успішно використовуються в невеликих приміщеннях, таких як офіси та житлові будинки.

Відеореєстратор - це пристрій для запису, обробки та зберігання інформації з камер спостереження. За допомогою стандартного пристрою ви можете відображати відео з камер (каналів) на моніторі, записувати їх, записувати відеодані на жорсткий диск, записувати звук і контролювати налаштування всіх системних пристроїв.

Відеореєстратори мають ряд функцій і можливість підтримувати певну кількість каналів - від 1 до 64, що робить різницю у вартості таких пристроїв.

Відеокамера

У той же час гібридні системи відеоспостереження (з використанням як аналогових, так і мережевих камер, підключених до відеосервера або гібридного реєстратора) в наші дні часто використовуються для забезпечення безпеки географічно розподілених, а головне, об'єктів. Вартість таких рішень вища порівняно зі змішаним розчином, але можливостей набагато більше.

Гібридні відеореєстратори

Такі системи відеоспостереження базуються на гібридних відеомагнітофонах, які дозволяють підключати як аналогові, так і мережеві камери, оскільки існують різні роз'єми і є інтерфейс для підключення до комп'ютерної мережі.

Гібридні відеореєстратори дозволяють користувачам бачити віддалено, крім використання екрану монітора, підключеного безпосередньо до записуючого пристрою. В останньому випадку спеціальне програмне забезпечення або стандартний веб-додаток, напр. В. Використовується Microsoft Internet Explorer. У цьому випадку є кілька пунктів візуального контролю, з кожного з яких можна отримати доступ до відеокамери системи відеоспостереження.

Крім того, гібридні відеореєстратори знімають обмеження щодо створення географічно розподілених систем відеоспостереження. Єдиним мінусом є те, що при значному збільшенні кількості відеокамер і розширенні функціональних можливостей часто доводиться замінювати дорогий пристрій. Крім того, розвиток відеореєстраторів має тенденцію відставати від розвитку комп'ютерних систем.

Гібридні системи спостереження з мережевими відеосерверами

У таких системах відеоспостереження мережевий відеосервер або відеокодер перетворює аналоговий сигнал з камери в цифровий і стискає відео для передачі через комп'ютерну мережу. Зазвичай перед відеокамерою встановлюється відеосервер. Пункт прийому - це комп'ютер для перегляду та запису зображень.

Системи відеоспостереження мають наступні переваги:

- Використовуйте звичайний комп’ютер для перегляду та запису відеоданих (замість дорогого відеомагнітофона з аналоговим входом);
- Можливість одночасного використання в системі аналогових і мережевих камер спостереження;
- можливість знаходити джерела зображень та записів на великі відстані, використовуючи комп’ютерну мережу як канал зв'язку;
- Хороша масштабованість системи, в цьому випадку кількість входів відеореєстратора (помножена на два) та можливість додавати більше камер за іншою не є необхідною.

До недоліків такої системи відеоспостереження належать вразливість до вірусів, помилки програмного забезпечення, невміле втручання операторів тощо.

Система моніторингу мережі

Системи мережевого спостереження побудовані на базі IP-відеокамер, які мають власну IP-адресу та програмне забезпечення, або іншими словами "інтелект". Все це дозволяє їм виступати як самостійні мережеві пристрої. Всі елементи системи відеоспостереження IP підключені як через локальну мережу Ethernet, так і безпосередньо, наприклад, через модем, мобільний телефон або бездротовий адаптер.

У цьому випадку він використовується як мережевий реєстратор відеозапису, який є стандартним комп'ютерним сервером із встановленим програмним забезпеченням для відеозапису.

Системи IP-відеоспостереження пропонують ряд переваг перед системами відеоспостереження та гібридного спостереження, наприклад Наприклад, запис даних на ваш жорсткий диск, пошук даних, які ви вимагали, у швидкому та плавному архіві, доступ до записів в Інтернеті тощо. Однак останнім часом системи відеоспостереження IP пройшли довгий шлях порівняно зі своїми попередниками, і для цього є об’єктивні причини:

- На ринку представлені різноманітні мережеві камери від Sony, AXIS, Arecontvision, Polyvision та багатьох інших відомих компаній - від простих коробчастих камер до купольних камер та Wi-Fi.
- Більш висока якість зображення зумовлена відсутністю додаткового перетворення цифрових сигналів в аналогові та аналогових в цифрові.
- Можливість передачі не лише відеоінформації, але й звуку, додаткових команд та живлення на камеру за допомогою кабелю.
- За допомогою мережевого рішення як складні географічно розподілені системи складаються з декількох тисяч камер, так і прості системи, що складаються з однієї або двох камер.
- Несинхронізація іловагії систем відеоспостереження на основі існуючої комп'ютерної мережі, а також за допомогою безім-вази основна технологія може бути аст, що знижує вартість насбро хеле кам мекунад.
- Технології та відеоспостереження та створення мереж роблять його простою інтеграційною платформою, яка відповідає потребам часу, а також ручними системами управління, системами управління, погодою тощо. Входить в одну систему.
- Різноманітність функцій IP-камери дозволяють приймати рішення про те, як увімкнути будильник, якість зображення, надіслати відео тощо. Покращує якість прийняття рішень у відео та Інтернеті.
- Можливість організувати зберігання та обробку відеозв'язку аірімутаму інформації, змінити захищену інфраструктуру в гаяірічммошті колатої, зв'язок, аварії, сервер пам'яті та офіс матері-хлопчика.
- Користувач комплексу захисту IP може виконувати візуальний та оперативний контроль управління системою на місцях, фоссілайні промені під час теми, теми, або PDA або мобільного телефону.

- Відеокамери пристроїв Bar'axi systemavii, які є технічно закритими рішеннями, базуються на чіткому загальноприйнятому припущенні, що використання обладнання від різних виробників, операцій, браузерів, комутаторів, серверів зменшує системні витрати та вдосконалений контроль стану системи відеоспостереження.

Хороша мережа доводить, що вони є альтернативою гарній гібридній системі.

І все ж, незважаючи на безліч переваг систем IP, існує низка факторів, які заважають розширенню світу покриття Інтернету у сфері відеоспостереження. По-перше, користувачі променя записують затримки відео-часу, які виникають під час сумісності з передачею даних та операцією через Інтернет. Роль полягає в управлінні музичними руками камер PTZ [9].

Основним варіантом з реалізації системи відеоспостереження є саме використання IP-рішенн, вони найбільш гнучкі та маштабовані. Виходячи з територіальної розгалуженності об’єкта то необхідно визначити тип підключення до мережі і спосіб розбудови телекомунікаційної інфраструктури з додатковими видами послуг.

2.3 Телекомунікаційна інфраструктура системи охорони периметра

Мультифункціональна телекомунікаційна мережа охорони периметру повинна також надавати додаткові послуги, такі як голосовий зв’язок і стати частиної загальної мережі об’єкту.

Зазвичай мережі будуються в відповідності до класичної трирівневої ієрархічної моделі – ядро, розподілу, доступ. Така ж сама модель буде реалізована і в мережі, що проектується. Для кожного з рівнів ієрархії необхідно провести огляд існуючих рішень з технології побудови фізичного та канального рівнів мережної моделі OSI.

В якості середовища розповсюдження сигналів для каналів зв’язку на сьогоднішній день використовуються як проводові так безпроводові канали. На рисунку 2.1 проілюстровані основні характеристики каналів зв’язку та їх основні характеристики.

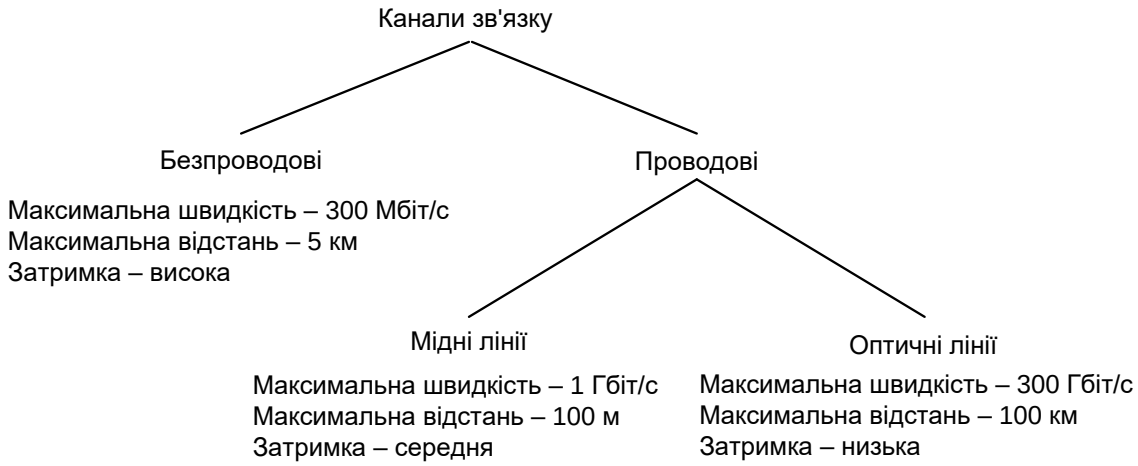


Рисунок 2.1 – Характеристика каналів зв’язку

Спираючись на основні характеристики середовищ розповсюдження сигналів, в таблиці 2.1 проведемо порівняльну характеристику типів каналів зв’язку з метою визначення оптимального.

Таблиця 2.1 – Порівняння типів фізичного середовища

	Мідь	Оптика	Радіоканал
Відстань	100 м	50 км	1,5 км
Швидкість на 1 канал	1 Гбіт/с	10 Гбіт/с	80 Мбіт/с
Завадо захищеність	середня	висока	низька
Надійність	середня	висока	низька
Строк сужби	20 років	50 років	10 років
Простота реалізації та розгортання	складна	складна	проста
Основні мережні технології	Ethernet	Ethernet, SDH	Wi-Fi, WiMax

Як виходить з проведеної порівняльної характеристики, оптимальним з точки зору показників пропускної здатності, дальності зв’язку та надійності

виявляються оптоволоконні технології, на другому місці йдуть мідні каналі, завершає рейтинг радіоканал.

Виходячи з трирівневої ієрархічної моделі, для побудови рівня ядра доцільно використовувати оптичні канали. Таке рішення пов'язано з необхідністю передачі великих об'ємів трафіку та надійним з'єднанням мережних компонентів ядра які окрім цього повинні бути захищені від впливу електромагнітних перешкод та наводок.

Рівень розподілу повинен об'єднувати точки, які підключені до мережі. В каналах рівня розподілу також повинен бути мінімізований вплив зовнішнього середовища на середовище передачі трафіку. Таким чином на цьому рівні також доцільно використовувати оптичні канали зв'язку.

Рівень доступу розташований на самій нижній сходинці ієрархічної моделі. Він призначений для підключення кінцевих користувачів. З огляду на невисокі вимоги з пропускної здатності, мінімального впливу на мережу зовнішніх чинників та на невеликі відстані доцільно використовувати в якості середовищі мідні кабелі. Також для підвищення якості сервісу можливе встановлення точок доступу безпосередньо в межах будинку для підключення до мережі сучасних мобільних пристроїв за бажанням власника.

Виходячи з того, що в якості базового середовища побудови мережі виступатиме оптичне волокно, слід зупинитися на основних концепціях розбудови мереж з використанням саме цієї кабельної продукції.

Розглянемо можливі варіанти організації мережі на кожному з рівнів ієрархічної моделі.

2.2.1 Технології побудови рівня ядра

Ключовими факторами при виборі технологій організації мережних сегментів є довжина кабельної ділянки, та пропускна здатність. Також важливим фактором для побудови мережі виступають витрати на її організацію.

Для побудови мережі на рівні ядра можна використати одну з технологій з сімейства Gigabit Ethernet. Існують три різних фізичних рівня стандартів для Gigabit Ethernet, які використовують оптоволоконий (1000Base-X) кабель, кручену пару (1000Base-T), або збалансований мідний кабель (1000Base-CX). Виходячи з обраної концепції, в таблиці 2.2 наведені основні характеристики стандартів, що використовують оптичні канали.

Таблиця 2.2 – Основні характеристики логічних інтрефейсів Gigabit Ethernet

Стандарт	Тип середовища	Відстань, км
1000BASE-SX	Багатомодове волокно	0,55
1000BASE-LX	Одномодове волокно	5
1000BASE-SX	Багатомодове волокно використовується довжина хвилі 850 нм	0,55
1000BASE-LH	Одномодове або Багатомодове волокно використовується довжина хвилі 1310 nm	10
1000BASE-ZX	Одномодове волокно на довжині хвилі 1550 nm	70
1000BASE-LX10	Одномодове волокно використовується довжина хвилі 1310 nm	10
1000BASE-BX10	Одномодове волокно, по single-strand fiber: 1490 nm прямий канал 1310 nm зворотний канал	10

Виходячи з наведених характеристик стандартів, для побудови мережі на рівні ядра доцільно використовувати технологію 1000 Base-SX, яка використовує для зв’язку оптичне багатомодове волокно. Вибір саме цієї технології пов’язаний з рівнем витрат на кабельну інфраструктуру, оптимальною швидкістю та дальністю зв’язку.

2.2.2 Технології побудови рівня розподілу

При будівництві мереж на базі волоконно оптичних технологій використовуються як пасивні оптичні мережі (Passive Optical Network - PON), так і активні оптичні мережі (Active Optical Network - AON). Обидва принципових підходи цілком вписуються в сучасну стратегію розвитку мережі доступу, яку

прийнято називати "волокно в будинок" або FTTx, де під"x" розуміється кінцева точка надання послуги з волокна. Концепція FTTx наведена на рисунку 2.2.

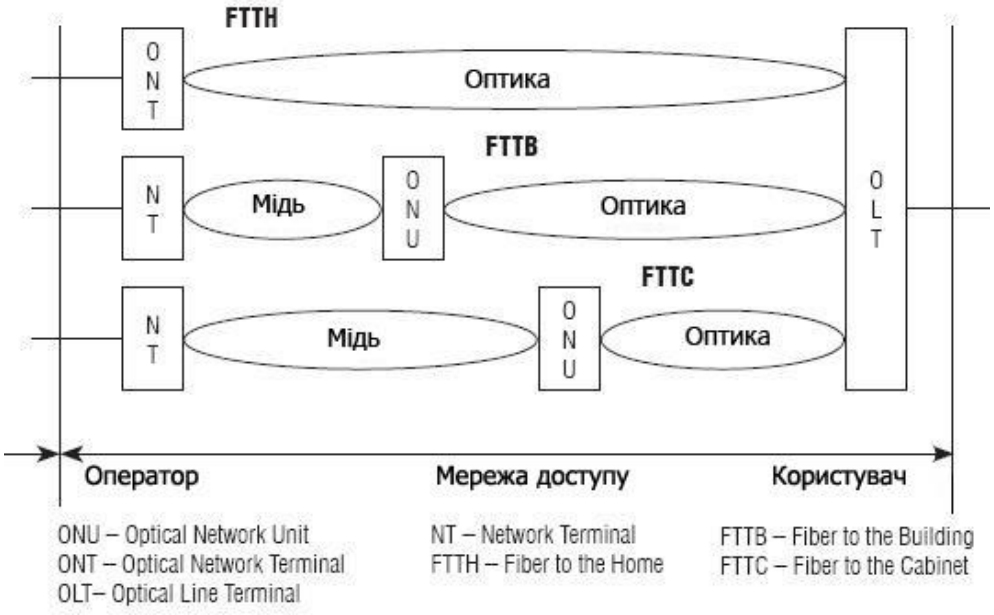


Рисунок 2.2 – Архітектура FTTx

Згідно з рисунком 2.2 та відповідно до Рекомендації ITU-T G.984.1. оптична лінія закінчується в абонента оптичним лінійним терміналом (OLT), розташованим, як правило, у приміщенні оператора, у той час як оптичні мережні пристрої (ONU) і мережні термінали (ONT) розташовуються поблизу точок присутності користувачів.

Слід зазначити, що застосування оптичного волокна для побудови мережі викликає необхідність використання концепції FTTx та СКС.

Концепції FTTx передбачає використання оптичного волокна при побудові як транспортних так і мереж доступу. Варіанти реалізації концепції FTTx поділяються на PON (Passive optical network) та AE (Active Ethernet). Концепція PON вимагає використання окремих жил оптичного волокна для кожного клієнта,концепція AE не вимагає такої необхідності. Розподіл середовища при використанні технології AE виконується як і в класичній мережі Ethernet за способом CSMA/CD.

Виходячи з використання оптичного волокна лише на ділянках мережі ядра та розподілу та кільцевих топологій, буде застосована концепція розбудови мережі – АЕ. Обрана концепція АЕ дозволяє використання повного спектру технологій FTTx, до якого відносяться наступні:

– FTTB (Fiber To The Building) - оптична система передачі до будинку;
– FTTN/FTTC (Fiber To The Node) - оптична система передачі до вузла;
– FTTO (Fiber To The Office) - оптична система передачі до офісу;
– FTTH (Fiber To The Home) - оптична система передачі до квартири;

Узагальнено FTTx можна проілюструвати на рисунку 2.3.

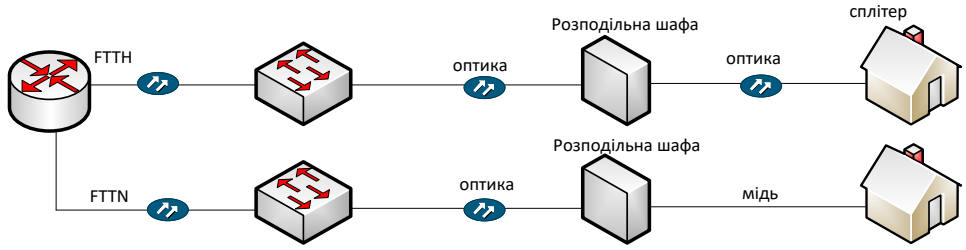


Рисунок 2.3 - Варіанти побудови мереж FTTx

Для реалізації мережі що проектується обрана концепція (FTTB), яку пропонується використовувати з AON або PON оптичною мережею. Вибір саме концепції FTTB зумовлений вимогами до швидкостей передачі в мережі (зумовлена великою кількістю кінцевих абонентських пристроїв). Концепція FTTB дозволяє довести оптичний кабель індивідуально до кожного будинку, а це гарантує стабільність з'єднання з мережею, високу пропускну здатність та незалежність від інших вузлів мережі.

PON, будучи операторським рішенням, передбачає на самому початковому етапі доведення до споживача всього комплексу послуг Triple Play - телебачення, Інтернету й телефонії. Технологія PON, має більші переваги над AON, тому саме вона буде використана при побудові мережі. До основних переваг PON слід віднести використання пасивних солітерів, що, в свою чергу, гарантує

роботоспроможність мережі в критичних ситуаціях незалежно від мережі електропостачання.

PON використовує деревоподібну архітектуру розведення волокна із застосуванням оптичних сплітерів, це рішення вимагає спеціального устаткування як на операторській стороні (OLT), так і на стороні користувача (ONU). Реалізація з'єднання «точка-многоточка», а саме так побудована PON, вимагає певних зусиль, щоб коректно розділити інтервали активності кожного термінала. Це нагадує роботу комп'ютерів у локальних мережах із застосуванням концентраторів, коли доводилося боротися з колізіями (одночасним заняттям каналу різними абонентами). В PON це завдання вирішене більш коректно – тут кожному абонентові виділяється свій інтервал часу, протягом якого він може формувати запити до OLT.

В таблиці 2.3 проведемо порівняння основних стандартів PON.

Таблиця 2.3 – Порівняння PON

Характеристики	APON (BPON)	EPON	GPON
Стандарт	TU-T G.981.x	IEEE 802.3ah	ITU-T G.984.x
Швидкість передачі прямий/зворотній потік, Мбіт/с	155/155 622/155 622/622	1000/1000	1244/155,622,1244 2488/622,1244, 2488
Базовий протокол	ATM	Ethernet	SDH
Максимальна кількість абонентський пристроїв на волокно	32	16	64(128)
Додатки	будь які	IP	будь які
Корекція помилок FEC	так	ні	так
Довжина хвиль прямого/зворотнього потоку, нм	1550/1310 (1480/1310)	1550/1310 (1310/1310)	1550/1310 (1480/1310)
IP-фрагментація	так	ні	так
Максимальна довжина, км	20	20	60
Загасання		26 дБ	22 дБ
Динамічний розподіл смуги	так	так	так
Захист даних	шифрування відкритими ключами	ні	шифрування відкритими ключами
Резервування	так	ні	так

Найбільш оптимальним рішенням на основі PON є EPON/GEPON або GPON. При виборі з двох стандартів слід звернути увагу на ключову відмінність, яку мають обрані стандарти, а саме, технологія GPON в якості базового стандарту використовує SDH, а технологія EPON/GEPON – Ethernet. Як відомо технологія SDH має гарантовану доставку та гарантовану смугу пропускання на відміну технології Ethernet, а це свідчить про більш високу організацію політики QoS. Виходячи з того, що більшу частину трафіку в мережі будуть представляти мультимедійні послуги, то краще використовувати стандарт, що заснований на технології SDH – GPON.

Для побудови мережі розподілу буде використана технологія GPON. До її переваг в порівнянні з іншими слід віднести:

- відсутність проміжних активних вузлів;
- економія оптичних прийомо-передавачів у центральному вузлі;
- економія волокон;
- легкість підключення нових абонентів і зручність обслуговування (підключення, відключення або вихід з ладу одного або декількох абонентських вузлів ніяк не позначається на роботі інших).

Як уже було відзначено вище, GPON є найбільш перспективною технологією сімейства пасивних оптичних мереж. GPON забезпечує істотну економію оптичних волокон за рахунок деревоподібної архітектури мережі. Крім того, використання технології забезпечує високу надійність, завдяки пасивним елементам розгалужень. Загалом , архітектуру мережі доступу GPON (Gigabit PON) можна розглядати як органічне продовження технології APON.

Підтримка сучасних технологій хвильового мультиплексування дозволяє значно збільшувати загальну пропускну здатність мережі без модернізації кабельної інфраструктури. При цьому деревоподібна структура мережі «точка-многоточка» дає можливість гнучкого керування смугою пропускання для клієнтських сервісів.

При досить високій швидкості передачі в обох напрямках GPON забезпечує прозорий транспорт для будь-яких сервісів (ATM, SDH, TDM,

Ethernet). За рахунок повної ізоляції кожного сервісу й підтримки убудованих засобів шифрування інформації досягається високий рівень безпеки мережі.

Таким чином для побудови мережі розподілу буде використана технологія GPON з концепцією організації фізичного середовища FTTB.

2.2.3 Технології організації рівня доступу

Як було визначено раніше, на рівні доступу використаний мідний кабель. Сьогодні Ethernet - неофіційний світовий стандарт адміністративних і обчислювальних мереж. Технологія Ethernet є основою специфікації IEEE 802.3. В таблиці 2.4 наведена узагальнена характеристика стандартів даного сімейства, що знаходять найчастіше використання.

Таблиця 2.4 – Реалізації технологій Ethernet

Реалізація	Fast Ethernet	Gigabit Ethernet	10 Gigabit Ethernet
Швидкість передачі,	100 Мб/с	1000 Мб/с	10 Гб/с
Середовище передачі	кручена пара, кабель оптичний	кручена пара, кабель оптичний	кручена пара, кабель оптичний
Варіанти реалізації	100BASE-TX 100BASE-SX 100BASE-FX	1000Base-X, 1000Base- LX 1000Base-T	10GBASE-T 10GBASE-LX4 10GBASE-LR

Найхарактернішою рисою Ethernet є метод доступу до середовища передачі – CSMA/CD – множинний доступ з виявленням колізій. Перед початком передачі даних мережевий адаптер Ethernet "прослуховує" мережу, аби упевнитися, що ніхто більше її не використовує. Якщо середовище передачі в даний момент кимось використовується, адаптер затримує передачу, інакше починає передавати. У тому випадку, коли два адаптери, заздалегідь прослухавши мережевий трафік і виявивши "тишу", починають передачу одночасно, відбувається колізія. При виявленні адаптером колізії обидві передачі уриваються, і адаптери повторюють передачу через деякий випадковий час

(природно, заздалегідь знову прослухавши канал на предмет зайнятості). Для прийому інформації адаптер повинен приймати всі пакети в мережі, аби визначити, чи не він є адресатом.

Основний недолік мереж Ethernet обумовлений методом доступу до середовища передачі: за наявності в мережі великої кількості станцій зростає кількість колізій, а пропускна спроможність мережі падає. У екстремальних випадках швидкість передачі в мережі може впасти до нуля. Але навіть в мережі, де середнє навантаження не перевищує максимально допустиму (рекомендується 30-40% від загальної смуги пропускання), швидкість передачі складає 70-80% від номінальної. В деякій мірі цей недолік може бути усунений використанням комутаторів (switch) замість концентраторів (hub). При цьому трафік між портами, підключеними до передавального і приймаючого мережевих адаптерів, ізолюється від інших портів і адаптерів.

Вельми істотною перевагою різних варіантів Ethernet є зворотна сумісність, яка дозволяє використовувати їх спільно в одній мережі, у ряді випадків навіть не змінюючи існуючу кабельну систему.

Головною перевагою мереж Ethernet, завдяки якій вони стали такими популярними, є їх економічність. В мережах Ethernet реалізовані достатньо прості алгоритми доступу до середовища, адресації і передачі даних. Простота логіки роботи мережі веде до спрощення і, відповідно, здешевлення мережевих адаптерів і їх драйверів. По тій же причині адаптери мережі Ethernet володіють високою надійністю. І, нарешті, ще однією визначною властивістю мереж Ethernet є легкість підключення нових вузлів.

Виходячи з наведених переваг, безапеляційно в мережі буде використана технологія Fast Ethernet 1000 Base-FX зі швидкістю 1000 Мбіт/с з використанням оптичного кабелю. Максимальна довжина кабельної ділянки для підключення пристроїв згідно з стандартом технології становить кілька сотень метрів, що цілком достатньо для організації підключення кінцевих користувачів до пристрою рівня розподілу.

2.2.4 Вибір способу побудови мережі IP-телефонії

Телефонна мережа на об’єкті проектування повинна функціонувати поверх мережі передачі даних, IP-мережі. При побудові таких мереж використовують протоколи IP-телефонії SIP та H.323. Для якісного функціонування послуги, необхідно забезпечення мінімального рівня затримки та завантаженості каналу зв’язку. Виходячи з того, що ми маємо два різних протоколи, необхідно провести їх порівняльну характеристику з точки зору наведених критеріїв QoS, але спочатку дамо визначення та стислий опис протоколів.

Протокол IP-телефонії H.323 більш підходить для використання при відмові від класичної телефонної мережі і переході до мереж IP-телефонії. Даний протокол був розроблений спеціалістами в галузі телефонії, заголовки пакетів цього протоколу містять велику кількість службової інформації, за допомогою якої можна визначити стан мережі, система сигналізації та керуючих повідомлень також насичена великою кількістю інформації і в деякому сенсі цей протокол є проекцією телефонної мережі на IP. Даний протокол підтримує тільки обмін голосовими даними, передача відео та організація відео конференцій навіть в останній редакції цього протоколу неможлива. Одним з немаловажним чинників є те, що новіші версії протоколу в більшості випадків не підтримують більш старі версії. Даний факт є вкрай незручним як для кінцевих користувачів так і для виробників телекомунікаційного устаткування. З цього приводу є великі сумніви з точки зору можливості введення нового більш ефективного термінального устаткування в існуючі мережі IP-телефонії.

Протокол IP-телефонії SIP більш орієнтований на використання в IP-мережах. Його розробниками є люди, що працюють в IT-галузі. Якщо розшифрувати абревіатуру яка представляє собою назву протоколу то вона звучить наступним чином – протокол ініціалізації сесій. Даний протокол дозволяє проводити обмін як аудіо інформацією (телефонний зв’язок) так відео (організація відеоконференцій). Список кодеків, які підтримує даний протокол

співпадає з списком H.323. Сучасна версія протоколу має повну сумісність з редакціям протоколів SIP що були визначені раніше.

В таблиці 2.5 проведемо порівняння протоколів за основними характеристиками.

Таблиця 2.5 – Порівняння протоколів

	SIP	H.323
додаткові послуги	однаковий набір	
персональна мобільність користувачів	високий рівень	посередній рівень
підтримка попередніх версій	в повному обсязі	частково
масштабованість мережі	так	
час встановлення з'єднання	одна транзакція	декілька транзакцій
складність протоколу	низька, мала кількість запитів, використовуються текстові повідомлення	висока, велика кількість запитів, двійковий формат повідомленнь

Якщо порівнювати ці два протоколи з точки зору необхідної сигнальної інформації при встановлені з'єднання, то протокол SIP використовує лише три повідомлення, а в свою чергу протокол H.323 використовує сім. Після встановлення з'єднання обидва протоколи використовують RTP та UDP для обміну голосовим трафіком. Після проведення розмови, для завершення з'єднання в SIP використовується 2 повідомлення, а H.323 п'ять. Як виходить з кількості службових повідомлень протокол SIP менш завантажує мережу ніж протокол H.323.

Виходячи з проведеного порівняння, в мережі буде використовуватись протокол SIP, який більш гнучкий, простий в використанні, надає можливість великої мобільності та сумісності устаткування та має біль широкий вибір абонентський терміналів.

2.2.5 Огляд базових протоколів функціонування мережі

В цілому мережа що проектується працює та управляється великою кількістю протоколів та технологій. Ключовими для функціонування мережі є протоколи Ethernet, TCP/IP, SDH.

Почнемо розгляд роботи мережі з базового протоколу TCP/IP. TCP/IP - це абревіатура терміну Transmission Control Protocol / Internet Protocol (Протокол керування передачею /міжмережевий протокол). Фактично TCP/IP не один протокол, а декілька. Саме тому його часто називають набором, або комплектом протоколів, серед яких TCP і IP — два основні. Фактично TCP/IP представляє цей базовий набір протоколів, відповідальний за розбивання вихідного повідомлення на пакети (TCP), доставку пакетів на вузол адресата (IP) і збирання (відновлення) вихідного повідомлення з пакетів (TCP).

Стек протоколів TCP/IP ділиться на 4 рівні: прикладний, транспортний, міжмережевий та рівень доступу до середовища передачі. Терміни, що використовуються для позначення блоку переданих даних, різні при використанні різних протоколів транспортного рівня: TCP і UDP. На прикладному рівні це потік (TCP) і повідомлення (UDP); на транспортному – сегмент і пакет.

Як і в моделі OSI, дані верхніх рівнів інкапсулюються в блоки даних нижніх рівнів, наприклад, сегмент (TCP) або пакет (UDP) зі своїми даними і службовими заголовками інкапсулюється всередині поля «Дані» дейтаграмм.

Протоколи прикладного рівня TCP/IP визначають процедури організації взаємодії прикладних процесів (програм) різних мережевих комп'ютерів і форми подання інформації за такої взаємодії. За ознаками взаємодії прикладних процесів виділяють два типи прикладного програмного забезпечення: програма-клієнт та програма-сервер. Протоколи прикладного рівня зорієнтовано на конкретні прикладні завдання. В таблиці 2.3 наведені протоколи прикладного рівня та їх призначення, що використані в мережі.

Таблиця 2.3 – Протоколи прикладного рівня та їх призначення

Протокол	Призначення
SMTP	протокол передачі електронної пошти
POP3	протокол прийому електронної пошти
FTP	протокол файлового обміну
HTTP	гіпертекстовий протокол
SIP	сигнальний протокол IP-телефонії
RTP	протокол передачі медіа трафіку в режимі реального часу
XML	протокл розмітки

Протоколи транспортного рівня TCP/IP надають транспортні послуги прикладним процесам. Основними протоколами транспортного рівня TCP/IP є протокол керування передачею TCP і протокол користувальницьких дейтаграм UDP. Транспортні послуги цих протоколів суттєво відрізняються. Протокол UDP доставляє дейтаграми без установлення з'єднання. При цьому він не гарантує їхнього доставляння. Протокол TCP забезпечує надійне доставляння байтових потоків (сегментів) із попереднім встановленням транспортного дуплексного з'єднання (віртуального каналу) між модулями TCP мережних комп'ютерів. Для розв'язання транспортних завдань протоколи TCP та UDP при передачі даних формують і додають до даних свої заголовки обсягом 20 байт та 8 байт відповідно.

Кожен прикладний процес взаємодіє з модулем транспортного рівня TCP або UDP через окремий порт, що дозволяє при взаємодії систем однозначно ідентифікувати прикладні процеси. Ці порти нумеруються починаючи з нуля. При передачі запиту прикладної програми клієнта до прикладної програми сервера транспортний модуль, формуючи датаграму чи сегмент, вказує номери портів програмних модулів прикладних протоколів сервера й клієнта. З цією метою в заголовку пакета протоколу транспортного рівня виділено два поля — «порт одержувача» і «порт відправника», обсягом по 2 байти. Номери портів TCP та UDP до прикладних протоколів сервера стандартизовані IETF. Для цього надано номери в діапазоні від 1 до 1023. Наприклад, програмний модуль TCP сервера зазвичай взаємодіє з модулем протоколу HTTP через порт з номером 80.

Взаємодія модуля TCP чи UDP клієнта з будь-яким модулем прикладного протоколу відбувається через порт, якому надається вільний номер більший за 1023.

Протоколи мережного рівня TCP/IP забезпечують взаємодію мереж різної архітектури. Основним протоколом мережного рівня технології TCP/IP є міжмережний протокол IP та його допоміжні протоколи: адресний протокол ARP; реверсний адресний протокол RARP (Reverse ARP); протокол діагностичних повідомлень ICMP (Internet Control Message Protocol), який надсилає повідомлення вузлам мережі про помилки на маршруті, які виникають при передачі пакетів тощо.

Головне завдання міжмережного протоколу IP — це маршрутизація пакетів даних між різнотипними комп'ютерними мережами. Для розв'язання цього завдання протокол IP підтримує IP-адресацію мереж та вузлів, використовує таблицю маршрутизації пакетів, виконує, за необхідності, фрагментацію та дефрагментацію цих пакетів.

Функціонування мережного рівня також забезпечує низка протоколів динамічної маршрутизації RIP, OSPF, які динамічно формують маршрути таблиці маршрутизації.

Рівень доступу до середовища передачі виконує функції перетворення IP-адреси в фізичні адреси мережі (MAC-адреси) та інкапсуляції IP-дейтаграм в кадри для передачі по фізичному каналу і передачі кадрів. На цьому рівні працює протокол ARP, який здійснює відображення адреси IP-> MAC.

На канальному рівні в мережі доступу та ядра використаний протокол Ethernet, який в свою чергу використовує протокол CSMA/CD (множинний доступ з контролем несучої та виявленням колізій). Цей протокол дозволяє в кожний момент часу лише один сеанс передачі в логічному сегменті мережі. При появі двох і більше сеансів передачі одночасно виникає колізія, яка фіксується станцією, що ініціює передачу. Станція аварійно зупиняє процес і очікує закінчення поточного сеансу передачі, а потім знову намагається повторити передачу.

2.4 Висновки за розділом

У другому розділі магістерскьої роботи проведено аналіз і класифікація систем охорони об’єктів і їх периметру. Обрані основні технології для реалізації пермитральної безпеки об’єкту – Індустріального парку Біла Церква.

РОЗДІЛ 3. РОЗРОБКА МУЛЬТИФУНКЦІОНАЛЬНОЇ МЕРЕЖІ ДЛЯ СИСТЕМИ БЕЗПЕКИ ПЕРИМЕТРА

3.1 Опис технологичного рішення системи охорони периметру

Розглянемо комплексні системи охорони периметра для стратегічно важливих об'єктів України з метою захисту від кримінальних, диверсійних і терористичних посягань та охорони матеріальних цінностей від розкрадання і вандалізму на базі високотехнологічного обладнання вібраційного і акустичного контролю компанії NBG-Systems (Австрія).

Завдяки унікальним технічним параметрам цих систем можуть бути вирішені різні завдання щодо захисту периметра об'єкта. Зокрема, система FiberGuard має надширокий частотний діапазон (від 3 Гц до 500 кГц) незалежно від довжини оптичного сенсорного кабелю, що дозволяє виявляти проникнення на об'єкт з високою точністю локалізації на ранній стадії і завчасно попереджати про це службу безпеки підприємства. На наш погляд, використання систем на базі волоконно-оптичного кабелю є найбільш виправданим рішенням для периметральної охорони стратегічно важливих об'єктів.

Для створення такої системи важливе значення має використання технології волоконно-оптичного зондування - сенсорного кабелю з двома технічними рівнями захисту: перший рівень для попередження наближення об'єкта з можливістю вторгнення; другий - безпосереднє вторгнення шляхом перелазу, підкопу або руйнування інженерних конструкцій.

В якості основного обладнання для дворівневої системи захисту використовуються розробки компанії NBG-Systems на базі сенсорного оптичного кабелю, виробленого за технологією FIMT (Fiber-In-Metal-Tube) і DVS (Distributed Vibration Sensing).

При опрацюванні технічного рішення для охорони периметра електростанції було вибрано декілька систем, виробництва компанії NBG-Systems, а саме:

1. Для охорони периметра за допомогою оптичного сенсорного кабелю, що закріплюється на паркані і закопували в грунті, застосовується система FiberGuard. Система являє собою обладнання для приймання та обробки впливів, що надаються на паркан.

Система складається з наступних основних елементів:

- Опитувальний модуль системи охорони периметра FiberGuard Monitoring System. Даний модуль призначений для обробки всіх сигналів, що надходять від оптоволоконного сенсорного кабелю. Опитувальний модуль кріпиться в стандартний 19 "шафа або 19" стійку. Залежно від модифікації модуль може здійснювати обробки сигналів від сенсорного оптичного кабелю довжиною 50 км або 20 км. Модуль може підключати до себе тільки один волоконно-оптичний сенсорний кабель.

- Волоконно - оптичний сенсорний кабель. Являє собою ВОК з 10 одномодовими волокнами. У даній системі ВОК не містить в своєму складі FIMT (металева трубка, в яку поміщено волокно), що в свою чергу суттєво знижує вимоги до ВОК при виборі виробника кабелю. Даний кабель може як кріпитися до паркану, так і бути закопаний в землю. Не потрібно харчування на всьому протязі кабелю.

- Початковий модуль FiberGuard Monitoring System Passive Start Termination для сенсорного кабелю. Служить для з'єднання підводить ВОК з сенсорним. Початковий модуль служить для поділу світлового потоку на кілька променів. Повністю пасивне пристрій.

- Кінцевий модуль FiberGuard Monitoring System Passive End Termination для сенсорного кабелю. Служить для установки в кінці сенсорного кабелю. Об'єднує кілька променів в один. Повністю пасивне пристрій.

- Ізолюючий модуль FiberGuard Monitoring System Zone Isolation Unit (пара), для сенсорного кабелю. Ізолюючі модулі застосовуються тільки парою. Встановлюється в сенсорний кабель і служить для виділення фрагмента сенсорного кабелю, який в даному фрагменті не реагує на зовнішні впливи (перестає бути сенсорним). Такі фрагменти виділяють при проходженні кабелю під дорогами, біля будівлі, під воротами, хвіртками та ін. Зонами, в яких не треба вимір. Повністю пасивне пристрій.

- Сервер FiberGuard Titan Commander ™. Центральний сервер системи. Являє собою апаратну платформу з інстальованим на неї спеціалізованим ПО. Служить для обробки, зберігання і виведення надходить масиву даних, прийнятих і сформованих опитувальними модулями системи. Виступає сполучною ланкою при об'єднанні кількох систем в єдину систему.

2. Для охорони і контролю доступу будівель і приміщень будуть застосовані:

• Система охоронної сигналізації Satel Integra з комплексом охоронних датчиків, сповіщувачів, клавіатур суміщених зі зчитувачами і індивідуальних ідентифікаторів;

• Система контролю доступу Keyprocessor в складі з мережевими і дверними контролерами, зчитувачами, датчиками, індивідуальними ідентифікаторами, і програмно-апаратним комплексом для адміністрування системи;

• Система програмно-апаратної інтеграції VDG, для інтеграції вищезазначених систем з системою ip-відеоспостереження і надання аналітичних функцій оператору систем.

3. Для відображення інформації від систем охорони периметра і зон служить Диспетчерський пульт системи охорони периметра. Даний пульт дозволяє оператору моніторити роботу системи, а також сигналізує про порушення периметра в конкретному місці або в певній зоні.

Програмне забезпечення диспетчерського пульта надає інтуїтивно-зрозуміле схематичне представлення структури рубежів охорони периметра підприємства у вигляді карт. Набір карт об'єкта містить його укрупнення і докладні багатошарові зображення, якість і ступінь деталізації яких відповідають технічним вимогам до системи.

Контрольовані системою охорони периметра події (тривоги, зміна стану обладнання і т.п.) оперативно відображаються у відповідних позиціях карти за допомогою умовних позначень. Якщо конкретну подію може бути асоційоване з різними верствами карти, вони всі будуть показані системою для оцінки ситуації з боку персоналу.

Карта об'єкта в системі охорони периметра реалізована не як статичний об'єкт, а у вигляді інтерактивного интерфейсного елемента - так, персонал може виробляти постановку або зняття з охорони окремих охоронних зон об'єкта безпосередньо взаємодіючи з графічними елементами на карті.

Всі однотипні об'єкти представлені у вигляді списків, всі команди управління або конфігурації об'єднані в меню. На малюнку зображений загальний вид пульта управління системи охорони периметра з органами управління та індикації.

До складу диспетчерського комплексу так само входить система оперативного зв'язку та оповіщення яка буде побудована на основі Інтерком-системи компанії Commend (Австрія), з більш ніж 40 річним досвідом в сфері виробництва систем зв'язку.

На автомобільних КПП, пішохідних хвіртках і входах в будівлі для переговорів з диспетчером передбачено використання антивандального терміналу (ступінь вандалозащіти IK09) з однією клавішею прямого виклику, вбудованої кольоровою відеокамерою з підсвічуванням, обігрівачем і механічним регулюванням на 30 ° по вертикалі / горизонталі.

У приміщеннях диспетчера і персоналу служби охорони пропонується використовувати термінал з мікрофоном типу «гусяча шия» і пульта управління

заснованому на програмному рішенні на базі ПК для відображення графічного меню і IP-відеопотоків.

Система оперативного зв'язку та оповіщення надасть наступні переваги:

• Забезпечення доступу транспортним засобам і пішоходам на об'єкт і до окремих областей. Виклики, які не можуть бути прийняті відразу, автоматично переадресовуються на інші пристрої (стаціонарні, мобільні);

• Модулі для інтеграції в ворота зі шлагбаумами в пунктах входу і виходу;

• Ідеальна розбірливість мови навіть в разі гучного шуму дорожнього руху;

• IP-гучномовці виготовлені для мережевого підключення;

• Голосові оголошення на певних поверхах, територіях або в усіх приміщеннях будівлі, території підприємства для передачі потрібної інформації або для пошуку співробітників;

• Відтворення попередньо записаних голосових повідомлень для передачі інформації, оповіщення та евакуації;

• Відтворення фонової музики або радіо;

• Інтелектуальний контроль гучності (IVC) автоматично регулює рівень гучності відповідно до акустичних умовами навколишнього середовища, щоб інформація завжди передавалася голосно і чітко;

• Системи пульта управління Commend забезпечують безперервний огляд всіх компонентів системи і дозволяють миттєво реагувати на надзвичайну ситуацію. Завдяки зручному графічному інтерфейсу, дуже просто керувати навіть складними інтерком мережами або відео і функціями.

Запропонована система має наступні переваги в порівнянні з традиційними системами охорони периметра:

- «невидима», не визначається візуально і засобами електромагнітного зондування за рахунок прихованого розміщення і властивостей ВОЛЗ (волоконно-оптична лінія зв'язку);

- має імунітет до електромагнітних завад і засобів електромагнітного придушення;

- має можливість дистанційного конфігурування (управління) і моніторингу системи з центру в режимі реального часу 24/7;

- має можливість додаткового резервування каналів передачі інформації за допомогою електронної пошти, SMS, Інтернет і т.д .;

- має більш низьку вартість володіння, обслуговування та управління в порівнянні з традиційними системами охорони периметра, які сьогодні встановлюється на об'єктах обслуговування Вашого підприємства через відсутність активних компонентів в польовий частини і стійкості ВОЛЗ до впливу корозії, хімічних речовин, води, погоди, блискавок . Термін служби - більше 20 років;

- має широкий діапазон контрольованих ділянок;

- має повністю пасивну польову частину, не вимагає електроживлення і вибухобезпечна;

- має наземне і підземне розташування чутливого кабелю ВОЛЗ;

- має можливість моніторингу як втручання третіх осіб, так і сейсмічної активності;

- має вдосконалене програмне забезпечення, яке працює в автоматичному режимі;

- має імунітет до несприятливих кліматичних явищ, таким, як вітер, дощ, сніг і раптові зміни температури, а також до перешкод прилеглих автодоріг і залізничних колій;

- самонавчального програмне забезпечення системи в стартовий період часу накопичує інформацію і створює інформаційні шаблони щодо різних подій, що відбуваються уздовж периметра стратегічних об'єктів, мінімізуючи таким чином ризик помилкового спрацьовування системи.

3.2 Вибір обладнання системи відеоспостереження та телефонії

Вибір активного устаткування базується на аналізі вимог отриманих в процесі виконання дипломної роботи, та на порівняльному аналізі продуктів компаній виробників телекомунікаційного устаткування. Згідно з розробленою структурною схемою в мережі повинні бути присутні наступні активні телекомунікаційні пристрої:

- маршрутизатор;
- комутатор;
- IP-АТС та телефонні апарати;
- компоненти системи відеоспостереження;

Перейдемо до вибору кожного з компонентів.

3.2.1 Вибір маршрутизаторів

Маршрутизатор є ключовим пристроєм при організації ядра мережі. Ядро мережі побудовано на базі двох прикордонного прикордонних маршрутизаторів, внутрішнього та зовнішнього. Наведемо вимоги до маршрутизаторів згідно з проведеними розрахунками:

- функція автоматичного розподілу адресного простору за протоколом DHCP;
- підтримка фільтрації пакетів та використання списків доступу ACL;
- можливість організації захисної зони DMZ;
- підтримка технології FireWall, трансляція адрес NAT;
- пропускна здатність не менш ніж 550 Мбіт/с;
- підтримка політики QoS;
- організація мережі за технологією 1000 Base-LX;
- можливість створення приватних тунелів VPN;
- підтримка технології віртуальних мереж VLAN;

– підтримка статичної маршрутизації та протоколів динамічної маршрутизації;
– підтримка голосових додатків на базі протоколів SIP та H.323.

Згідно з розробленою структурною схемою, кількість пристроїв становить одну одиницю, він повинен бути обладнаний оптичними інтерфейсами SC з підтримкою технології GE. В таблиці 3.1 проведемо порівняння маршрутизаторів.

Таблиця 3.1 – Порівняння маршрутизаторів

	Cisco 2951	D-Link DI-2630	Ericsson SE100
Специфікація портів	3 FE FX, 3 GE LX	2 FE TX	FE, GE
Пропускна здатність	8 Гбіт/с	N/A	12 Гбіт/с
Підтримка VoIP	SIP, H.323	SIP	SIP, H.323
Резервування блоків живлення	так	ні	так
Взаємодія з WLAN	так	так	так
Слоти розширення	3 GE	2 WAN 2 LAN	8
Маршрутизація OSPF	так	ні	так
Підтримка QoS	так	так	так
Функції VPN	так	ні	так
NAT, ACL	так	так	так

З точки зору продуктивності, оптимальним варіантом є використання продукції Ericsson, з точки зору співвідношення ціна/якість/відповідність вимогам, оптимальним варіантом є модель Cisco 2951. Продукція компанії D-Link не відповідає поставленим вимогам. Обрана модель для реалізації мережі – Cisco 2951. Маршрутизатор призначений для організацій, діяльність яких заснована на передових технологіях, маршрутизатори Cisco серії 2900 з інтегрованими мережними сервісами (ISR) забезпечують захищене високошвидкісне підключення робочих місць до мультисервісної мережі, підтримку мультимедійних даних і відмінні експлуатаційні характеристики.

Маршрутизатори Cisco ISR серії 2900 забезпечують:

– безперервне підключення до мережі: високий рівень доступності й тривалий час безвідмовної роботи за рахунок застосування ПЗ Cisco IOS, апаратного резервування й засобів аварійного перемикання;

- універсальний набір сервісів: модульна підтримка найширшого набору мережних і захисних сервісів Cisco, а також віртуальних сервісів;
- колективна робота з високим рівнем безпеки: архітектура, підготовлена до передачі відео, підтримує мультимедійні можливості уніфікованих комунікацій;
- вбудовані засоби мережної безпеки;
- гнучка підтримка мереж VPN: надання мобільному персоналу й вилученим співробітникам безпечного доступу до ресурсів компанії по захищеному з'єднанню.

3.2.2 Вибір комутаторів

Комутатори в мережі повинні бути двох типів – комутатор оптичні (для включення серверного устаткування та орендаторів) та мідні для організації мережі офісу. Наведемо вимоги до оптичних комутаторів згідно обраним рішенням:

- комутатор повинен працювати на 3 рівні моделі OSI;
- комутатор повинен підтримувати VLAN;
- можливість керування трафіком з використанням політики QoS;
- підтримка організації мережі зі швидкістю в 1000 Мбіт/с за технологією Base-LX;
- пропускна здатність не менш 500 Мбіт/с;
- загальна кількість портів 200.

До мідних згідно розрахункам висуваються наступні вимоги:

- комутатори повинні працювати на 3 рівні моделі відкритих систем – OSI;
- комутатори повинні підтримувати технологію віртуальних під мереж VLAN;
- можливість керування трафіком з використанням політики QoS;

- підтримка організації мережі зі швидкістю в 100 Мбіт/с за технологією Fast Ethernet 100 Base-TX та 1000 Мбіт/с за технологією Base-LX;
- підтримка технології PoE для мідних інтерфейсів;
- пропускна здатність не менш 20 Мбіт/с;
- керування портами.

В таблиці 3.2 проведемо порівняння мідних комутаторів рівня.

Таблиця 3.2 – Порівняння комутаторів розподілу/доступу

	Juniper EX3200-48	Alcatel OmniStack LS 6248	Huawei S3352P-EI-48S	НАТЕКС NX-3428	Cisco Catalyst WS-2960S-48TD-L
Пропускна здатність	136 Гбіт/с	17,6 Гбіт/с	17,6 Гбіт/с	36 Гбіт/с	40 Гбіт/с
Рівень OSI	3	2	2	2	3
Стаціонарні порти	48xRJ-45 10/100/ 1000 Мбіт/с 2xSC 1000 Мбіт/с	48xRJ-45 10/100 Мбіт/с 2xSC 1000 Мбіт/с	48xRJ-45 10/100 Мбіт/с 4xSC 1000 Мбіт/с	48xRJ-45 10/100 Мбіт/с 2xSC 1000 Мбіт/с	48xRJ-45 10/100/ 1000 Мбіт/с 4xSC 1000 Мбіт/с
Наявність слотів	1	1	1	1	1
Підтримка PoE	так	ні	ні	ні	так
Резервування	так	ні	ні	так	так
Вартість	7000 $	600 $	750 $	1100 $	3200 $

Встановленим вимогам в більшій чи меншій мірі відповідають два продукти – Juniper EX3200-48 та Cisco Catalyst WS-2960S-48TD-L. Вибір комутатора базується в першу чергу на граничній пропускній здатності та швидкості комутації,а також наявності необхідної кількості фізичних інтерфейсів. Серед представлених моделей лідером є пристрій Cisco Catalyst WS-2960S-48TD-L . Комутатор Layer 3, 48 портів 10/100/1000 Base-T (48 з підтримкою PoE), 4 порти 1000Base-LX, слот для установки модулів розширення. Даний комутатор підтримує L2/L 3-комутацію на швидкості інтерфейсів, VLAN, RVI, QoS, Power over Ethernet, динамічну маршрутизацію, кластеризацію Virtual Chassis, 802.1X, port- security, PVLAN, Q-In- Q.

Основні особливості:

- розмір таблиці MAC- Адрес: 24000;

- кількість VLAN: 4096;
- протоколи маршрутизації: RI v1/v2, OSPF, BGP, IS- IS;
- кількість активних unicast- маршрутів: 12 000;
- функція BFD;
- функція віртуальних маршрутизаторів (VRF);
- функція Dynamic ARP Inspection;
- функція IP Source Guard;
- функція Virtual Chassis;
- функція Cable Diagnostic.

Для організації оптичного сегменту можливі три варіанти,а саме:

- використання повністю оптичних комутаторів;
- використання комутаторів зSFP-модулями;
- використання мідних комутаторів з меді конвертерним шасі.

В таблиці 3.3 проведемо порівняння трьох підходів.

Виходячи з проведеного порівняння для побудови мережі доцільно використовувати варіант з модулями SFP.

Таке рішення в першу чергу пов’язано з можливістю довільної конфігурації пристрою як за типом портів (оптичні/мідні)так і за наявністю високих показників надійності і відносно невеликої вартості.

Таблиця 3.3 – Порівняння варіантів побудови оптичної підсистеми

	Оптичний комутатор	Комутатор SFP	Мідний комутатор з медіаконверторами
Надійність	висока	середня	низька
Модульність	обмежена	висока	низька
Можливість вільного набору мідних та оптиних портів	ні	так	так
Вартість	висока	середня	висока
Кількість компнентів	1	2	2
Тип фізичного оптичного рознімання	однаковий для всіх портів	довільний	довільний

В якості базової моделі для побудови оптичного сегменту мережі буде використаний комутатор Cisco Catalyst 4500X з універсальними модулями SFP.Кількість місць для установки модулів в одному пристрої – 32, швидкість в кожному порту в залежності від обраного типу модуля становить від 100 Мбіт/с до 10Гбіт/с. Немаловажним чинником є той фактор, що пристрої можна об’єднувати в один мережний логічний сегмент, тобто вони є такими, що стикуються.

3.2.3 Вибір IP-АТС та телефонних апаратів

В якості кінцевого устаткування телефонної мережі виступають телефонні апарати. Згідно з технічним завданням до телефонних апаратів висуваються наступні вимоги:

- фізичний інтерфейс RJ-45 100 BaseTX;
- підтримка PoE;
- протокол IP- телефонії SIP.

Глобально їх можна розбити на 2 класи – телефонні апарати для встановлення на орендуємих площах (звичайні) та офісі (продвинуті з додатковими функціями). Виходячи з обраного комутаційного устаткування, а саме маршрутизатора Cisco 2951, який має програмне забезпечення для реалізації на своїй базі IP- АТС – Cisco Call Manager, вибір бренду очевидний– це буде компанія Cisco. До таблиці 3.4 наведена порівняльна характеристика звичайних телефонних апаратів.

Таблиця 3.4 – Порівняльна характеристика звичайних телефонних апаратів

	Cisco SPA504G	Cisco Unified IP 521G	Cisco SPA502G	Cisco Unified SIP CP-3911
Фізичний інтерфейс	2 порти 10/100BASE-T - роз'єм RJ-45	2 порти 10/100BASE-T - роз'єм RJ-45	1 порт 10/100BASE-T - роз'єм RJ-45	1 порт 10/100BASE-T - роз'єм RJ-45

Наявність вбудованого комутатора	так	так	ні	ні
Протоколи IP-телефонії	SIP, SIP2	SIP, SIP2	SIP, SIP2	SIP, SIP2
Підтримка CCM	так	так	так	так
Підтримка PoE	так	так	Так	так
Зовнішній адаптер живлення	так	ні	Так	ні
Підтримка DHCP	так	так	так	так
Вартість, грн.	1280	1216	1025	615

Виходячи з економічних та функціональних показників, обираємо модель Cisco Unified SIP CP-3911. Cisco Unified SIP VoIP **CP-3911** є економічно ефективним апаратом початкового рівня. Це однорядний телефон з напівдуплексним спікерфоном і вбудованим мікрофоном. Cisco Unified SIP-телефон 3911 забезпечує конференц-зв’язок, утримання, можливість обрати одну з двох ліній, відключення звуку, гучний зв'язок, голосову пошту та функції доступу. Крім цього телефон обладнаний 2-рядковим 24-символьним дисплей. Цей дисплей забезпечує підтримку додаткових можливостей, таких як визначення номера абонента, історія дзвінків, а також можливість налаштування телефону. Ключовим також є те, що телефон підтримує IEEE 802.3af Power Over Ethernet (PoE), або живлення від блоку живлення (в комплект не входить).

Для телефонів другого класу необхідно використання більш продвинутих моделей, які матимуть у своєму арсеналі більш інформативний дисплей та розширені додаткові функції. До такої моделі можні віднести Cisco 7945G. IP-телефон **Cisco 7945G** підтримує PoE і адаптер живлення від мережі змінного струму, який не входить в комплект поставки. Нижче наведена стисла технічна специфікація:

- **протоколи** – SIP, SCCP;
- **електроживлення –** IEEE 802.3af PoE (Class 3), або мережа змінного струму 220 В (використовується зовнішній блок живлення);

- графічний дисплей – сенсорний 16 біт (кольоровий) 320 х 240 пікс. (Діагон.12, 5 см);
- налаштування IP- адрес – ручне або DHCP;
- кількість телефонних ліній (макс.): 2; гучний зв'язок;
- підтримка XML-додатків;
- QoS.

3.3.4 Вибір відеокамер та серверного устаткування

Для побудови системи відеоспостереження необхідно обрати IP-відеокамери та відеосервер. Узагальнені вимоги до IP-відеокамер наступні:

- підтримка протоколу H.264;
- підтримка технології PoE;
- фізичний інтерфейс RJ-45;
- підтримка протоколу 100 Base-TX.

В відповідності до характеристик було проведено порівняння. В таблиці 3.5 зведено основні моделі та їх характеристики.

Таблиця 3.5 – Порівняння відеокамер

Модель	DN-H09-MPC-WS	FI8904W	M601W	FI8905W
Тип камери	Вулична, 2 Мпікс	Вулична, 2 Мпікс	Поворотна IP Камера	Вулична, 2 Мпікс
Лінза	6-12 мм	6-8 мм	4-9 мм	8-12мм
ІК-пушка	так	ні	так	так
Метод компресії	H.264/MJPEG	MJPEG	H.264/MJPEG	H.264/MJPEG
Аудіо	так	ні	так	ні
Мережний інтерфейс	10/100 Base-T PoE	10/100 Base-T	802.11 b/g, 10/100 Base-T	802.11 b/g 10/100 Base-T PoE
Вартість, грн	2570	1300	3210	1740

Виходячи з проведеного порівняння оптимальним буде побудови мережі відеоспостереження на IP камерах **Foscam FI8905W.**

Наступним етапом є вибір відеосервера. Дешевим варіантом є програмний сервер на базі ПК. В апаратному варіанті реалізації великим недоліком є його вартість, що насамперед пов'язано з вартістю комплектуючих. В порівнянні з програмною реалізацією, різниця в вартості може досягати в декілька разів.

Програма для перегляду IP-камер дозволяє навіть при високому ступені стиску, а виходить, економії трафіка, одержувати незмінного гарну якість відеоконтенту, переданого з камер.

Повні версії програмного забезпечення пропонують функцію планувальника, завдяки чому можна починати запис відео в призначений момент часу. Програма відеоспостереження IP-камер захоплює контент не тільки з камер, але й з будь-яких пристроїв, що підключають за допомогою USB. Розширюють функціонал ПЗ можливості настроювання інтерфейсу, пошуку, кодувальника відео й зміна імені папки.

З безкоштовного ПЗ, прогресивним є Blue Iris - програмне забезпечення для IP Камер професійного класу, що використовує найсучасніші відео - програмні технології. Уміє працювати з форматами MPEG, H.264, RTSP. Підтримує підключення до 256 камер (веб-камери, відеокамери, мережні IP-камери). Веде запис відео за рухом, розкладом або постійно. Можливе накладення тексту або графіки. Має убудований веб-сервер для перегляду камер й архіву записів через Інтернет. Присутні повідомлення через електронну пошту, завантаження фотографій на FTP сервер.

Особливості:

- версія програми 2.49.10;
- підтримка 256 камер;
- фільтр роликів камерою;
- підтримка IP-камер FOSCAM, CCDCAM й інших;
- запуск як служба Win32 (не потрібно логин);
- автозбереження вікна при виявленні руху.

Самим вагомим чинником є те, що програма розповсюджується як shareware ПЗ.

В якості серверного устаткування виступає комп’ютер, який має наступну конфігурацію (таблиця 3.6):

Таблиця 3.6 – Конфігурація серверного устаткування

Найменування	Призначення
Phenom x3 8650 Socket AM2+; BOX; Revision B3 !!!; Triple-Core; 2300Mhz; 3x512KB L2 Cache; 2048KB L3 Cache; 95W; DDRII	процесор
Rack Mounted, 5 U, 500W FSP ATX- 5.25"x4, 3.5"x1e+5i; w/USB; ATX	корпус з БЖ
Модуль памяти DDR2 SDRAM 2048Mb; PC-6400; 800 MHz; Kingston	модуль пам'яті
Жесткий диск 500 Gb Western Digital; Caviar Blue (WD5000AAKS); 7200 rpm; 16Mb cache; SATA II 3 Gb/s	накопичувач
ASUS M3N78 PRO; Socket AM2/AM2+; GeForce 8300; Video; 4DDRII; HT 3.0; 1xP-Ex16(V2.0); 2xP-Ex1; 3xP; Sound 8-ch; GigabitLan; 6xSATAII; 1xATA133; (RAID 0, 1, 0+1, 5, JBOD); SATA5-6; ATX	материнська плата

3.3 Висновки

В третьому розділі виконаний апаратний синтез мережі, визначені основні види обладнання для розбудови мережі.

РОЗДІЛ 4. IP-ПРОЕКТУВАННЯ СЕГМЕНТУ МЕРЕЖІ. ПОЛІТИКА ЗАХИСТУ ВІД ЗОВНІШНІХ ЧИННИКІВ

4.1 Ключові вимоги та вихідні дані

Телекомунікаційна мережа, що була розроблена, надає орендаторам доступ до мережі Інтернет та телефонний зв’язок, надає вільний доступ до мережі Інтернет відвідувачам, та послуги відеоспостереження. Одною з ключових вимог до мережі є те, що вона повинна бути прозорою для зовнішніх підключень, та одночасно захищеною від небажаних вторгнень.

В мережі представлені наступні інформаційні сервіси:

- доступ до мережі Інтернет;
- доступ до серверу БД;
- доступ до файлового сервера;
- ведення відеоспостереження;
- локальна телефонія;
- телефонний зв'язок з місцевою мережею.

В якості користувачів та кінцевого термінального устаткування для користування інформаційними послугами виступають наступні:

- робочі станції співробітників;
- абонентські пристрої відвідувачів;
- орендні площі;
- телефонні апарати;
- компоненти відеоспостереження.

Всі користувачі мережі умовно розділені на чотири категорії:

- адміністрація;
- орендатори;
- відвідувачі;
- спостереження.

Виходячи з типів устаткування та груп користувачів, для реалізації мережі необхідна наявність наступних класів обслуговування:

- телефонні апарати - TA;
- персональні комп’ютери, сервери та мережні пристрої адміністрації - ADMIN;
- бездротові Wi-Fi пристрої персоналу обслуговуючого персоналу - PERSONAL;
- локальний web-сервер з Інтернет сторінкою – WEB;
- персональні комп’ютери, сервери та мережні пристрої орендаторів - ORENDA;
- термінальні пристрої відвідувачів - FREE;
- камери спостереження - VS.

Виходячи з проведеного опису та розробленої інформаційної моделі уточнимо вимоги до надання доступу до тих чи інших ресурсів (таблиця 4.1)

Таблиця 4.1 – Доступ до ресурсів мережі для класів обслуговування

Клас обслуговування	Мережний ресурс				
	Інтернет	База даних	Файл-сервер	Сервер спостереження	Телефонія
TA	-	-	-	-	+
ADMIN	+	+	+	-	-
PERSONAL	-	+	-	-	-
WEB	+	-	-	-	-
ORENDA	+	-	-	-	-
FREE	+	-	-	-	-
VS	-	-	-	+	-

4.2 Розподіл адресного простору

В додатку Б на рисунках Б.2-Б.4 наведені основні схеми мережі. На базі цих схем необхідно розробити імітаційну модель мережі, план розподілу адресного простору та план логічної структуризації мережі.

Для логічної структуризації мережі можна використовувати декілька підходів, вони базуються на використані унікального адресного простору для кожної з груп устаткування, відокремленні груп устаткування в різні логічні сегменти засобами VLAN, накладенні списків обмеження доступу ACL при підключенні груп устаткування через комутатори до відокремлених віртуальних підмереж. Виходячи з функціональної схеми мережі, найбільш простим варіантом з реалізації буде саме використання віртуальних підмереж 802.1q.

Для побудови мережі буде створено декілька віртуальних підмереж, в кожній з яких буде використаний окремий адресний простір. Ключовим елементом, який буде займатися питаннями обмеження доступу виступає маршрутизатор, також на ньому буде організована служба автоматичного розподілу адресного простору DHCP.

В таблиці 4.2 наведемо перелік віртуальних підмереж, кількість устаткування в них, та необхідний адресний простір.

Таблиця 4.2 – Розподіл адресного просторі між VLAN

VLAN №	Назва VLAN	Кількість пристроїв	Мережа	Маска
101	TA	199	192.168.1.0	24
102	PERSONAL	50	192.168.2.0	26
103	ADMIN	20	192.168.2.64	26
104	VS	83	192.168.2.128	25
105	FREE	4200	10.10.0.0	19
1001	ORENDA_1	250	10.0.1.0	24
1002	ORENDA_2	250	10.0.2.0	24
1xxx	ORENDA_xxx	250	10.0.xxx.0	24
1178	ORENDA_178	250	10.0.178.0	24
1179	ORENDA_179	250	10.0.179.0	24

На рисунку 4.1 наведемо схему розподілу адресного простору між віртуальними під мережами та серверним устаткуванням.

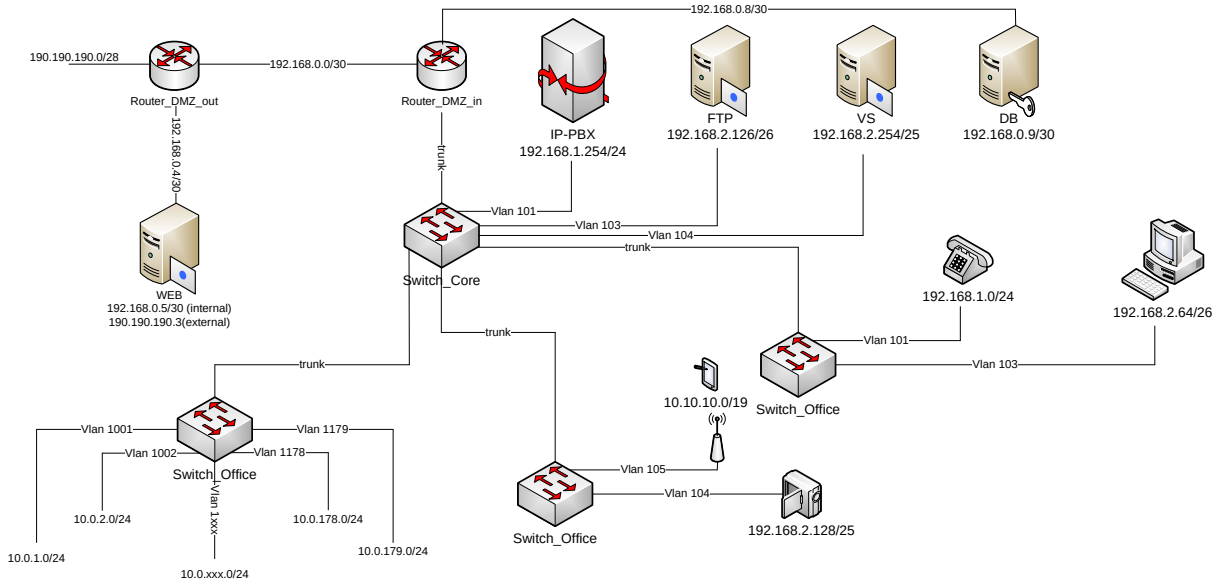


Рисунок 4.1 – Схема розподілу IP-адрес

4.2 Розробка та налаштування моделі

В якості середовища роботи IP-мережі, що проектується використаємо емулятор Cisco Packet Tracer 6.0. На рисунку 4.2 наведена схема моделі, що використовується для перевірки роботи мережі.

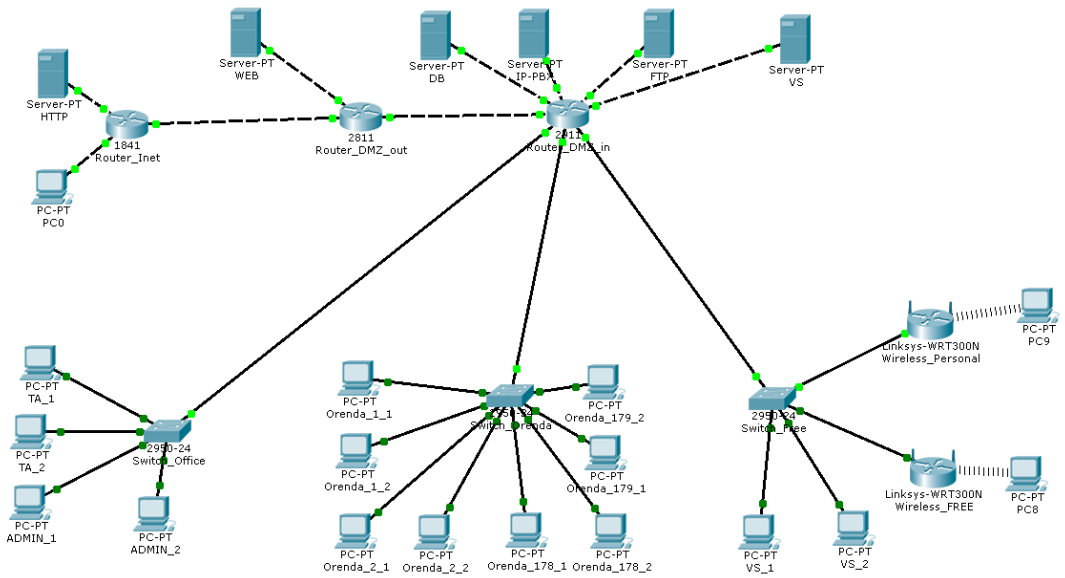


Рисунок 4.2 – Схема моделі

Проведемо налаштування Router_Inet

```
Router>enable
Router#configure terminal
Router_Inet(config)#interface FastEthernet0/0
Router_Inet(config-if)#ip address 130.15.17.1 255.255.0.0
Router_Inet(config-if)#no shutdown
Router_Inet(config)#interface Ethernet0/1/0
Router_Inet(config-if)#ip address 76.87.55.1 255.0.0.0
Router_Inet(config-if)#no shutdown
Router_Inet(config)#interface FastEthernet0/1
Router_Inet(config-if)#no shutdown
Router_Inet(config-if)#ip address 190.190.190.2 255.255.255.240
```

Проведемо первинне налаштування Router_DMZ_out:

```
Router(config)#hostname Router_DMZ_out
Router_DMZ_out(config)#interface FastEthernet0/0
Router_DMZ_out(config-if)#no shutdown
Router_DMZ_out(config-if)#ip address 190.190.190.1 255.255.255.240
Router_DMZ_out(config)#interface FastEthernet0/1
Router_DMZ_out(config-if)#no shutdown
Router_DMZ_out(config-if)#ip address 192.168.0.1 255.255.255.252
Router_DMZ_out(config)#interface Ethernet0/2/0
Router_DMZ_out(config-if)#ip address 192.168.0.6 255.255.255.252
Router_DMZ_out(config-if)#no shutdown
```

Проведемо первинне налаштування маршрутизатора Router_DMZ_in:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router_DMZ_in
Router_DMZ_in(config)#interface GigabitEthernet0/0
```

```
Router_DMZ_in(config-if)#no shutdown
Router_DMZ_in(config-if)#ip address 192.168.0.2 255.255.255.252
Router_DMZ_in(config)#interface GigabitEthernet0/1
Router_DMZ_in(config-if)#no shutdown
Router_DMZ_in(config-if)#ip address 192.168.0.10 255.255.255.252
Router_DMZ_in(config)#exit
Router_DMZ_in#vlan database
Router_DMZ_in(vlan)#vlan 101 name TA
Router_DMZ_in(vlan)#vlan 102 name PERSONAL
Router_DMZ_in(vlan)#vlan 103 name ADMIN
Router_DMZ_in(vlan)#vlan 104 name VS
Router_DMZ_in(vlan)#vlan 105 name FREE
Router_DMZ_in(vlan)#vlan 201 name ORENDA_1
Router_DMZ_in(vlan)#vlan 202 name ORENDA_2
Router_DMZ_in(vlan)#vlan 378 name ORENDA_178
Router_DMZ_in(vlan)#vlan 379 name ORENDA_179
Router_DMZ_in(vlan)#exit
Router_DMZ_in#configure terminal
Router_DMZ_in(config)#interface FastEthernet0/0/0
Router_DMZ_in(config-if)#switchport access vlan 101
Router_DMZ_in(config-if)#no shutdown
Router_DMZ_in(config)#interface FastEthernet0/0/1
Router_DMZ_in(config-if)#no shutdown
Router_DMZ_in(config-if)#switchport access vlan 103
Router_DMZ_in(config)#interface FastEthernet0/0/2
Router_DMZ_in(config-if)#no shutdown
Router_DMZ_in(config-if)#switchport access vlan 104
Router_DMZ_in(config)#interface FastEthernet0/1/0
Router_DMZ_in(config-if)#no shutdown
Router_DMZ_in(config-if)#switchport mode trunk
Router_DMZ_in(config)#interface FastEthernet0/1/1
Router_DMZ_in(config-if)#no shutdown
Router_DMZ_in(config-if)#switchport mode trunk
Router_DMZ_in(config)#interface FastEthernet0/1/2
Router_DMZ_in(config-if)#no shutdown
Router_DMZ_in(config-if)#switchport mode trunk
```

Проведемо налаштування комутатора Switch_Office:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Switch_Office
Switch_Office(config)#vlan 101
Switch_Office(config-vlan)#name TA
Switch_Office(config-vlan)#exit
Switch_Office(config)#vlan 103
Switch_Office(config-vlan)#name ADMIN
Switch_Office(config-vlan)#exit
Switch_Office(config)#interface FastEthernet0/1
Switch_Office(config-if)#switchport mode trunk
Switch_Office(config)#interface FastEthernet0/2
Switch_Office(config-if)#switchport access vlan 101
Switch_Office(config)#interface FastEthernet0/3
Switch_Office(config-if)#switchport access vlan 101
Switch_Office(config)#interface FastEthernet0/4
Switch_Office(config-if)#switchport access vlan 103
Switch_Office(config)#interface FastEthernet0/5
Switch_Office(config-if)#switchport access vlan 103
```

Проведемо налаштування комутатора Switch_Orenda:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Switch_Orenda
Switch_Orenda(config)#vlan 201
Switch_Orenda(config-vlan)#name ORENDA_1
Switch_Orenda(config-vlan)#exit
Switch_Orenda(config)#vlan 202
Switch_Orenda(config-vlan)#name ORENDA_2
Switch_Orenda(config-vlan)#exit
Switch_Orenda(config)#vlan 378
Switch_Orenda(config-vlan)#name ORENDA_178
Switch_Orenda(config-vlan)#exit
```

```
Switch_Orenda(config)#vlan 379
Switch_Orenda(config-vlan)#name ORENDA_179
Switch_Orenda(config-vlan)#exit
Switch_Orenda(config)#interface FastEthernet0/1
Switch_Orenda(config-if)#switchport mode trunk
Switch_Orenda(config)#interface FastEthernet0/2
Switch_Orenda(config-if)#switchport access vlan 201
Switch_Orenda(config)#interface FastEthernet0/3
Switch_Orenda(config-if)#switchport access vlan 201
Switch_Orenda(config)#interface FastEthernet0/4
Switch_Orenda(config-if)#switchport access vlan 202
Switch_Orenda(config)#interface FastEthernet0/5
Switch_Orenda(config-if)#switchport access vlan 202
Switch_Orenda(config)#interface FastEthernet0/6
Switch_Orenda(config-if)#switchport access vlan 378
Switch_Orenda(config)#interface FastEthernet0/7
Switch_Orenda(config-if)#switchport access vlan 378
Switch_Orenda(config)#interface FastEthernet0/8
Switch_Orenda(config-if)#switchport access vlan 379
Switch_Orenda(config)#interface FastEthernet0/9
Switch_Orenda(config-if)#switchport access vlan 379
```

Проведемо налаштування комутатора Switch_Free:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Switch_Free
Switch_Free(config)#vlan 102
Switch_Free(config-vlan)#name PERSONAL
Switch_Free(config-vlan)#exit
Switch_Free(config)#vlan 104
Switch_Free(config-vlan)#name VS
Switch_Free(config-vlan)#exit
Switch_Free(config)#vlan 105
Switch_Free(config-vlan)#name FREEE
Switch_Free(config-vlan)#exit
```

```
Switch_Free(config)#interface FastEthernet0/1
Switch_Free(config-if)#switchport mode trunk
Switch_Free(config)#interface FastEthernet0/2
Switch_Free(config-if)#switchport access vlan 105
Switch_Free(config)#interface FastEthernet0/3
Switch_Free(config-if)#switchport access vlan 102
Switch_Free(config)#interface FastEthernet0/4
Switch_Free(config-if)#switchport access vlan 104
Switch_Free(config)#interface FastEthernet0/5
Switch_Free(config-if)#switchport access vlan 104
```

Перейдемо до налаштування точок бездротового доступу. На точці доступу необхідно налаштувати наступні параметри – обрати частотний канал, режим роботи точки доступу, SSID та вимкнути внутрішній DHCP сервер. Налаштуємо точку доступу Wireless Router1.

Налаштовуємо частотний канал, режим роботи точки та SSID (рисунок 4.3).

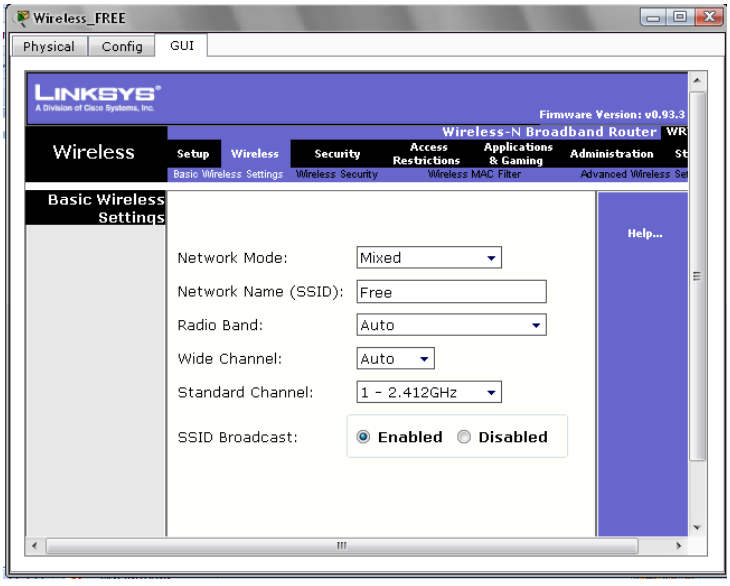


Рисунок 4.3 – Налаштування радіо інтерфейсу

Далі необхідно вимкнути внутрішній сервер DHCP (рисунок 4.4).

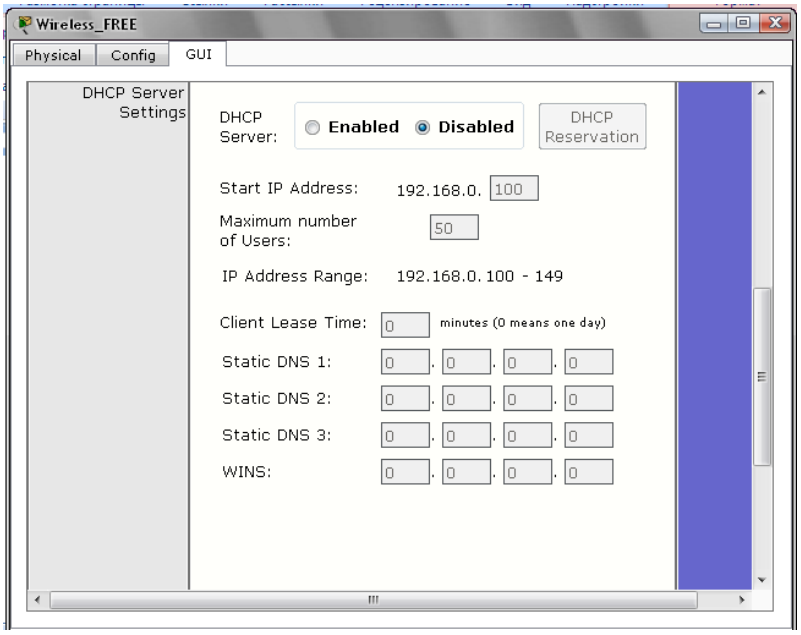


Рисунок 4.4 – Відключення внутрішньої служби DHCP на точці доступу

Аналогічні налаштування проведемо на точці доступу Wireless_Personal, відмінність полягатиме в частотному каналі (буде використаний каналі №5), SSID (Personal).

Налаштовуємо частотний канал, режим роботи точки та SSID (рисунок 4.5).

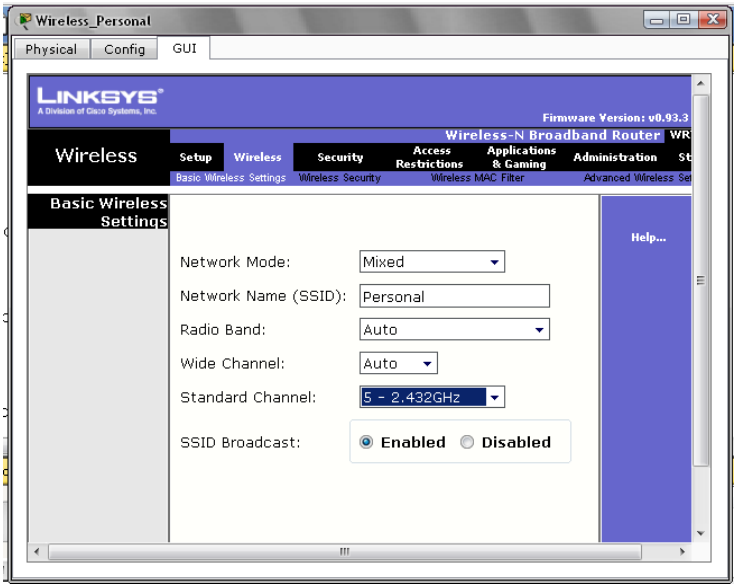


Рисунок 4.5 – Налаштування радіо інтерфейсу

Далі необхідно вимкнути внутрішній сервер DHCP (рисунок 4.6).

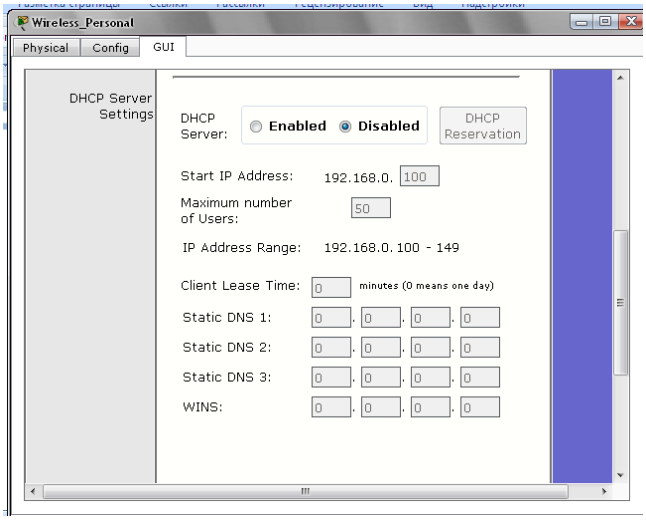


Рисунок 4.6 – Відключення внутрішньої служби DHCP на точці доступу

Налаштуємо пароль (рисунок 4.7)

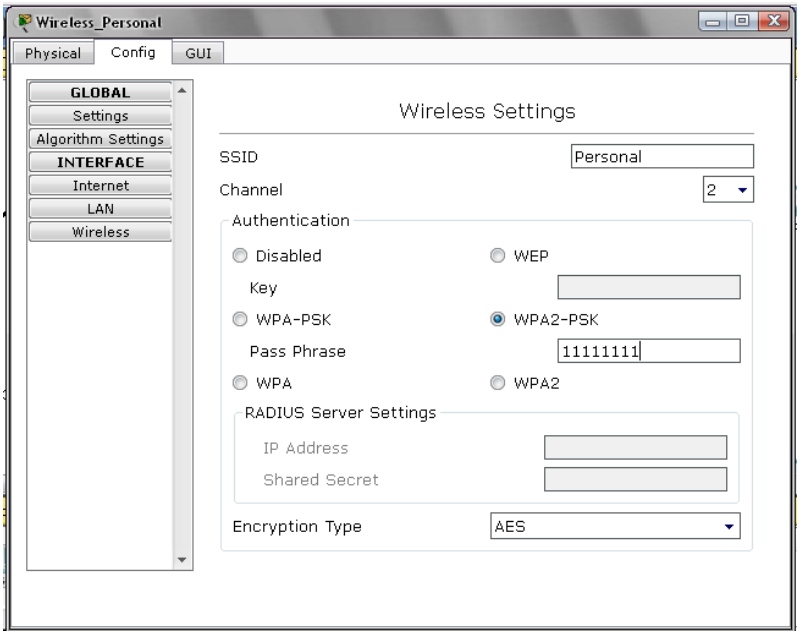


Рисунок 4.7 – Налаштування паролю

На маршрутизаторі Router_DMZ_in проведемо налаштування служб DHCP та інтерфейсів віртуальних підмереж:

```
Router_DMZ_in(config)#ip dhcp pool TA
Router_DMZ_in(dhcp-config)#network 192.168.1.0 255.255.255.0
```

```
Router_DMZ_in(dhcp-config)#default-router 192.168.1.1
Router_DMZ_in(dhcp-config)#ip dhcp pool PERSONAL
Router_DMZ_in(dhcp-config)#network 192.168.2.0 255.255.255.192
Router_DMZ_in(dhcp-config)#default-router 192.168.2.1
Router_DMZ_in(dhcp-config)#ip dhcp pool ADMIN
Router_DMZ_in(dhcp-config)#network 192.168.2.64 255.255.255.192
Router_DMZ_in(dhcp-config)#default-router 192.168.2.65
Router_DMZ_in(dhcp-config)#ip dhcp pool VS
Router_DMZ_in(dhcp-config)#network 192.168.2.128 255.255.255.128
Router_DMZ_in(dhcp-config)#default-router 192.168.2.129
Router_DMZ_in(dhcp-config)#ip dhcp pool FREE
Router_DMZ_in(dhcp-config)#network 10.10.0.0 255.255.224.0
Router_DMZ_in(dhcp-config)#default-router 10.10.0.1
Router_DMZ_in(dhcp-config)#ip dhcp pool ORENDA_1
Router_DMZ_in(dhcp-config)#network 10.0.1.0 255.255.255.0
Router_DMZ_in(dhcp-config)#default-router 10.0.1.1
Router_DMZ_in(dhcp-config)#ip dhcp pool ORENDA_2
Router_DMZ_in(dhcp-config)#network 10.0.2.0 255.255.255.0
Router_DMZ_in(dhcp-config)#default-router 10.0.2.1
Router_DMZ_in(dhcp-config)#ip dhcp pool ORENDA_178
Router_DMZ_in(dhcp-config)#network 10.0.178.0 255.255.255.0
Router_DMZ_in(dhcp-config)#default-router 10.0.178.1
Router_DMZ_in(dhcp-config)#ip dhcp pool ORENDA_179
Router_DMZ_in(dhcp-config)#network 10.0.179.0 255.255.255.0
Router_DMZ_in(dhcp-config)#default-router 10.0.179.1
Router_DMZ_in(dhcp-config)#ex
Router_DMZ_in(config)#int vlan 101
Router_DMZ_in(config-if)#ip address 192.168.1.1 255.255.255.0
Router_DMZ_in(config-if)#int vlan 102
Router_DMZ_in(config-if)#ip address 192.168.2.1 255.255.255.192
Router_DMZ_in(config-if)#int vlan 103
Router_DMZ_in(config-if)#ip address 192.168.2.65 255.255.255.192
Router_DMZ_in(config-if)#int vlan 104
Router_DMZ_in(config-if)#ip address 192.168.2.129 255.255.255.128
Router_DMZ_in(config-if)#int vlan 105
Router_DMZ_in(config-if)#ip address 10.10.0.1 255.255.224.0
```

```
Router_DMZ_in(config-if)#int vlan 201
Router_DMZ_in(config-if)#ip address 10.0.1.1 255.255.255.0
Router_DMZ_in(config-if)#int vlan 202
Router_DMZ_in(config-if)#ip address 10.0.2.1 255.255.255.0
Router_DMZ_in(config-if)#int vlan 378
Router_DMZ_in(config-if)#ip address 10.0.178.1 255.255.255.0
Router_DMZ_in(config-if)#int vlan 379
Router_DMZ_in(config-if)#ip address 10.0.179.1 255.255.255.0
```

На маршрутизаторі Router_DMZ_in створимо список доступу до серверу БД для груп ADMIN, PERSONAL:

```
Router_DMZ_in(config)#ip access-list standard DB
Router_DMZ_in(config-std-nacl)#permit 192.168.2.0 0.0.0.127
Router_DMZ_in(config-std-nacl)#ex
Router_DMZ_in(config)#int gigabitEthernet 0/1
Router_DMZ_in(config-if)#ip access-group DB out
```

Для організації можливості виходу до мережі Інтернет необхідно накласти список доступу на інтерфейс gigabitEthernet 0/1маршрутизатора Router_DMZ_in для груп FREE, ADMIN та ORENDA_xxx:

```
Router_DMZ_in(config)#ip access-list standard inet
Router_DMZ_in(config-std-nacl)#permit 192.168.2.64 0.0.0.63
Router_DMZ_in(config-std-nacl)#permit 10.10.0.0 0.0.31.255
Router_DMZ_in(config-std-nacl)#permit 10.0.1.0 0.0.0.255
Router_DMZ_in(config-std-nacl)#permit 10.0.2.0 0.0.0.255
Router_DMZ_in(config-std-nacl)#permit 10.0.178.0 0.0.0.255
Router_DMZ_in(config-std-nacl)#permit 10.0.179.0 0.0.0.255
Router_DMZ_in(config-std-nacl)#ex
Router_DMZ_in(config)#int gigabitEthernet 0/0
Router_DMZ_in(config-if)#ip access-group inet out
```

Заключний етап налаштування – маршрутизатор Router_DMZ_out. На данному пристрої необхідно налаштувати NAT та списки доступу ACL до мережі інтернет:

```
Router_DMZ_out(config)#int fa 0/0
Router_DMZ_out(config-if)#ip nat outside
Router_DMZ_out(config-if)#int fa 0/1
Router_DMZ_out(config-if)#ip nat inside
Router_DMZ_out(config-if)#int eth 0/2/0
Router_DMZ_out(config-if)#ip nat inside
Router_DMZ_out(config-if)#ex
Router_DMZ_out(config)#access-list 1 permit 192.168.2.64 0.0.0.63
Router_DMZ_out(config)#access-list 1 permit 10.10.0.0 0.0.31.255
Router_DMZ_out(config)#access-list 1 permit 10.0.1.0 0.0.0.255
Router_DMZ_out(config)#access-list 1 permit 10.0.2.0 0.0.0.255
Router_DMZ_out(config)#access-list 1 permit 10.0.178.0 0.0.0.255
Router_DMZ_out(config)#access-list 1 permit 10.0.179.0 0.0.0.255
Router_DMZ_out(config)#ip nat inside source list 1 int fa 0/0
overload
```

Налаштуємо можливість доступу до web-серверу з мережі Інтернет:

```
Router_DMZ_out(config)#ip nat inside source static 192.168.0.5
190.190.190.5
```

Налаштуємо маршрутизацію на всіх маршрутизаторах:

```
Router_DMZ_out(config)#router rip
Router_DMZ_out(config-router)#no network 192.168.0.0
Router_DMZ_out(config-router)#network 192.168.0.0
Router_DMZ_out(config-router)#network 190.190.0.0
Router_DMZ_out(config-router)#default-information originate
Router_DMZ_out(config-router)#

Router_DMZ_in(config)#router rip
Router_DMZ_in(config-router)#network 10.0.0.0
Router_DMZ_in(config-router)#network 192.168.0.0
```

```
Router_DMZ_in(config-router)#default-information originate

Router_Inet(config)#router rip
Router_Inet(config-router)#network 76.0.0.0
Router_Inet(config-router)#network 130.15.0.0
Router_Inet(config-router)#network 190.190.0.0
Router_Inet(config-router)#default-information originate
Router_Inet(config-router)#
```

Виходячи з проведених налаштувань мережа є працездатною та захищеною.

4.3 Висновки

В четвертій главі дипломної роботи було проведено імітаційне моделювання роботи IP-мережі. Був розроблений план та схема розподілу IP-адресного простору для мережі. Для сегментації активних пристроїв мережі використовується технологія віртуальних мереж – VLAN, кількість таких мереж відповідає інформаційній моделі. Була розроблена імітаційна модель мережі в пакеті Cisco PacketTracer. На розробленій моделі було налаштовано: віртуальні підмережі VLAN, служба автоматичного розподілу адресного простору DHCP, служба трансляції адрес NAT та стандартні списки доступу ACL.

ВИСНОВКИ

Перший розділ роботи присвячено аналізу об’єкту, визначення актуальності та постановка задачі проектування, наведена кореляція питань безпекових рішень та телекомунікаційних мережі і інфраструктурних рішень, також приділена увага особливостям впровадження систем периметральної охорони.

У другому розділі магістерскьої роботи проведено аналіз і класифікація систем охорони об’єктів і їх периметру. Обрані основні технології для реалізації пермитральної безпеки об’єкту – Індустріального парку Біла Церква.

В третьому розділі виконаний апаратний синтез мережі, визначені основні види обладнання для розбудови мережі.

В четвертій главі дипломної роботи було проведено імітаційне моделювання роботи IP-мережі. Був розроблений план та схема розподілу IP-адресного простору для мережі. Для сегментації активних пристроїв мережі використовується технологія віртуальних мереж – VLAN, кількість таких мереж відповідає інформаційній моделі. Була розроблена імітаційна модель мережі в пакеті Cisco PacketTracer. На розробленій моделі було налаштовано: віртуальні підмережі VLAN, служба автоматичного розподілу адресного простору DHCP, служба трансляції адрес NAT та стандартні списки доступу ACL.

ПЕРЕЛІК ПОСИЛАННЬ

1. https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D0%B4%D1%83%D1%81%D1%82%D1%80%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%BF%D0%B0%D1%80%D0%BA
2. http://zakon3.rada.gov.ua/laws/show/5018-17
3. https://mind.ua/publications/20186816-industrialni-parki-v-ukrayini-shcho-ce-take-i-chi-vdastsya-yih-reanimuvati
4. https://www.me.gov.ua/documents/Download?id=697dc9b1-05ea-47d4-b6d6-430dd2a4190c ОГЛЯД СТАНУ РОЗБУДОВИ МЕРЕЖІ ІНДУСТРІАЛЬНИХ ПАРКІВ В РОЗРІЗІ РЕГІОНІВ УКРАЇНИ
5. https://valtek.com.ua/ru/system-integration/security-control-system/integrated-security-systems/perimeter-security-systems
6. https://valtek.com.ua/ru/system-integration/security-control-system/integrated-security-systems/perimeter-security-systems
7. http://www.ipcom.club/ohrana-perimetra
8. http://guarda.ru/infra_red/18/
9. https://www.bramy.ru/videonablyudenie/vidy-sistem-videonablyudeniya.html

Додаток А. Охорона праці та безпека життєдіяльності

А.1 Характеристика умов праці

Труд працівників системи служби безпеки телекомунікаційного підрозділу, дуже інтенсивний та напружений, який потребує значні витрати розумової, емоційної та фізичної енергії. Працівники тісно пов'язані з комп'ютерною технікою. При роботі з комп'ютерною технікою людина піддається впливу багатьох шкідливих та небезпечних факторів: електромагнітних полів (діапазон радіочастот ВЧ, УВЧ, СВЧ), інфрачервоного та іонізуючого випромінювань, шуму та вібрації, статичної електрики та ін.

Робота з комп'ютером характеризується значною розумовою напруженістю та нервово – емоційним навантаження операторів, високою напруженістю зорової праці та достатньо великим навантаженням на м'язи рук при роботі з клавіатурою.

В процесі роботи з комп'ютером необхідно дотримуватися правильного режиму праці та відпочинку.

Ці фактори можуть привести до професійних захворювань таких, як комп'ютерна алергія, радіохвильова хвороба, захворювання шкіри, синдром Сіка, язва шлунку, комп'ютерний зоровий синдром, стрес, кистьовий тунельний синдром.

Діяльність працівників відділу:

– моніторинг активного обладнання мережі, виявлення відмов та аварійних ситуацій на обладнанні;

– оповіщення відповідних підрозділів про виникаючі аварії;

– аналіз виникаючих аварій;

– організація оперативних дій по усуненню аварій, координація роботи технічних служб;

– підтримка актуального статусу аварії;

– контроль та координація дій операторів;

– формування звітів;

– робота, за потребою, з оргтехнікою (факс, принтер, копіювальний апарат) та Інтернетом.

Відділ моніторингу мережі розташовується на другому першому будівлі АПК поверсі в приміщенні з установленою технікою згідно з СНиП II-90-81 «Виробничі будівлі промислових підприємств», загальна площа приміщення становить 30 м², а загальний обсяг – 90 м³.

А.2 Вимоги до виробничих приміщень

А.2.1 Освітлення

Правильно спроектоване та виконане освітлення покращує умови зорової роботи, знижує втому, сприяє підвищенню продуктивності труда, оказує благотворний вплив на виробниче середовище, надаючи позитивний психологічний вплив на працівника, підвищує безпеку праці та знижує травматизм.

Недостатнє освітлення призводить до напруження зору, послаблює увагу, призводить до передчасної втоми. Надмірна яскравість викликає осліплення, роздратування та різь в очах. Неправильний напрям освітлення на робочому місці може створювати різкі тіні, відблиски, дезорієнтованість працівника. Всі ці причини можуть призвести до нещасного випадку або профзахворюваннь, цьому важливий правильний розрахунок освітлення.

Згідно з СНиП II-4-79 в приміщенні необхідно застосовувати систему комбінованого освітлення.

При виконанні робіт категорії високої зорової точності (найменший розмір об’єкта розрізнення 0,3…0,5 мм) величина коефіцієнта природнього освітлення (КПО) повинна бути не нижче 1,5%, а при зорової роботі середньої точності (найменший розмір об’єкта розрізнення 0,5…1,0 мм) КПО повинен бути не нижче 1%. В якості джерел штучного освітлення зазвичай використовуються

люмінесцентні лампи типа ЛБ або ДРЛ, які попарно об’єднуються до світильників, які повинні розташовуватися над робочими поверхнями рівномірно.

Вимоги до освітлення у приміщеннях, де встановлені комп’ютерна техніка, наступні: при виконанні зорових робіт високої точності загальна освітленість повинна складати 300 лк, а комбінована – 750 лк; аналогічні вимоги при виконанні робіт середньої точності – 200 и 300 лк відповідно.

Крім того все поле зору повинно бути освітлене достатньо рівномірно – це основна гігієнічна вимога. Іншими словами, степінь освітлення приміщення та яскравість екрану комп’ютера повинні бути приблизно однаковими, тому що яскраве світло у районі периферійного зору значно збільшує напругу очей та, як наслідок, призводить до їх швидкої втоми.

А.2.2 Параметри мікроклімату

Параметри мікроклімату можуть змінюватися в широких межах, в той час як необхідною умовою життєдіяльності людини є підтримка постійності температури тіла завдяки терморегуляції, тобто здатності організму регулювати віддачу тепла до навколишнього середовища. Принцип нормування мікроклімату – створення оптимальних умов для теплообміну тіла людини з навколишнім середовищем.

Комп’ютерна техніка є джерелом суттєвих тепловиділень, що може призвести до підвищення температури та зниженню відносної вологи в приміщенні. У приміщенні, де встановлені комп’ютери, повинні дотримуватися певні параметри мікроклімату. В санітарних нормах СН 245-71 встановлені величини параметрів мікроклімату, які створюють комфортні умови. Ці норми встановлюються залежно від пори року, характеру трудового процесу та характеру виробничого приміщення.

Об’єм приміщень, в яких розташовані робочі місця працівників відділу моніторингу, не повинен бути менш ніж 19,5 м³/людину з урахуванням максимального числа одночасно працюючих за зміну

Таблиця А.1 – Параметри мікроклімату для приміщення з комп’ютерами

Пора року	Параметри мікроклімату	Величина
Холодна	Температура повітря	22…24 ºС
	Відносна вологість	40…60 %
	Швидкість руху повітря	До 0,1 м/с
Тепла	Температура повітря	23…25 ºС
	Відносна вологість	40…60 %
	Швидкість руху повітря	0,1…0,2 м/с

Таблиця А.2 – Норми подачі свіжого повітря в приміщення, де розташована комп’ютерна техніка

Характеристика приміщення	Об’ємні витрати свіжого повітря, що подається в приміщенні м³/на одну людину в годину
Об’єм до 20 м³ на людину 20…40 м³ на людину Більш ніж 40 м³ на людину	Не менш ніж 30 Не менш ніж 20 Природня вентиляція

Для забезпечення комфортних умов використовуються як організаційні методи (раціональна організація проведення робіт в залежності від пори року та доби, чергування праці та відпочинку), так й технічні засоби (вентиляція, кондиціювання повітря, опалювальна система).

А.2.3 Електромагнітне та іонізуюче випромінювання

Максимальний рівень рентгенівського випромінювання на робочому місці взагалі не перевищує 10 мкбер/г, а інтенсивність ультрафіолетового та інфрачервоного випромінювань від екрану монітору лежить у межах 10…100 мВт/м².

Таблиця А.3 – Допустимі значення параметрів неіонізуючих електромагнітних випромінювань (згідно з СанПиН 2.2.2.542-96)

Параметр	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні монітору	10 В/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні монітору	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати для дорослих користувачів	20 кВ/м

Для зниження дії цих видів випромінювань рекомендується застосовувати монітори з пониженим рівнем випромінювань, встановлювати захисні екрани, а також дотримуватися регламентованих режимів праці та відпочинку.

А.3 Ергономічні вимоги до робочого місця

Робоче місце та взаємне розташування всіх його елементів повинно відповідати антропометричним, фізичним та психологічним вимогам. Велике значення має також характер праці. При організації робочого місця у відділі моніторингу повинні бути дотримані наступні основні вимоги: оптимальне розміщення обладнання, яке входить у склад робочого місця та достатній робочий простір, який дозволяє здійснювати всі необхідні рухи та пересування.

Ергономічними аспектами у даному випадку є висота робочої поверхні, розміри простору для ніг, вимоги до розташування документів на робочому місці (наявність та розміри підставки для документів, можливість різного розміщення документів, відстань від очей користувача до екрану, документа, клавіатури та ін.), характеристики робочого крісла, вимоги до поверхні робочого столу, регулювання елементів робочого місця.

Головними елементами робочого місця оператора телекомунікаційного підрозділу є стіл та крісло. Основним робочим положенням є положення сидячи.

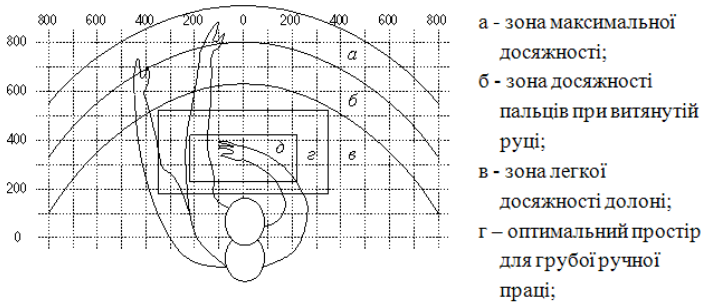
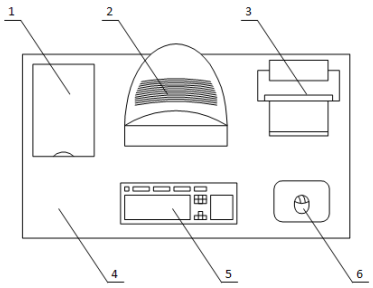


Рисунок А.1 – Зони досяжності рук в горизонтальній площині

Робоча поза сидячи викликає мінімальну втому оператора. Раціональне планування робочого місця передбачає чітку послідовність та постійне розміщення предметів, засобів праці та документації. Те, що потрібно для виконання роботи частіше, розташовано в зоні легкої досяжності робочого простору.

Оптимальне розміщення предметів праці та документації у зонах досяжності: дисплей розміщується в зоні а (у центрі), системний блок розміщується у передбаченій ніші столу, клавіатура – у зоні г/д, миша – у зоні в (праворуч), сканер – у зоні а/б (ліворуч), принтер знаходиться у зоні а (праворуч), документація, яка необхідна при роботі – в зоні легкої досяжності долоні – в.



1 – сканер, 2 – монітор, 3 – принтер, 4 – поверхня робочого столу,
5 – клавіатура, 6 – маніпулятор типу «миша»

Рисунок А.2 – Розміщення основних та периферійниих складових ПК

Для комфортної роботи стіл повинен відповідати наступним вимогам:

– висота столу повинна бути обрана з урахуванням можливості сидіти вільно, в комфортній позі, при необхідності опираючись на підлокітники;

- нижня частина столу повинна бути сконструйована таким чином, щоб оператор зручно сидів, не мусив піджимати ноги;
- поверхня столу повинна мати властивості, які виключають появлення відблисків у полі зору;
- конструкція столу повинна передбачати наявність висувних ящиків (для зручності зберігання документації, канцелярії, літератури);
- висота робочої поверхні рекомендована в межах 680 – 760 мм. Висота поверхні, на яку встановлюється клавіатура, повинна бути близько 650 мм.

Велике значення надається характеристикам робочого крісла. Так, рекомендована висота крісла над рівнем знаходиться у межах 420 – 550 мм. Поверхня сидіння м'яка, передній край закруглений, а кут нахилу спинки – регульований.

Необхідно передбачити при проектуванні можливість різного розміщення документів: збоку від монітору та ін. Крім цього, у випадках, коли монітор має низьку якість зображення, відстань від очей до екрану роблять більшою (близько 700 мм).

Розташування екрану:

- відстань зчитування (0,6 …0,7 м);
- кут зчитування, напрямком погляду на 20º нижче горизонталі до центру екрану, при цьому екран перпендикулярний цьому напрямку;

Повинна також передбачатися можливість регулювання екрану:

- за висотою +3 см;
- за нахилом від -10º до +20º відносно вертикалі;
- у лівому та правому напрямках.

Велике значення також надається правильній робочій позі оператора. При незручній робочій позі можуть з'являтися біль у м'язах, суглобах та сухожиллях. Вимоги до робочої пози оператора:

- голова не повинна бути нахиленою більш ніж на 20º;
- плечі повинні бути розслабленими;
- лікті – під кутом 80º…100º;

– передпліччя та кісті рук – у горизонтальному положенні.

Причина неправильної пози операторів обумовлена наступними факторами: клавіатура знаходиться досить високо, немає місця для руки та кісті, недостатньо простору для ніг.

Задля здолання цих недоліків даються загальні рекомендації: краще клавіатура, що пересувається, повинні бути передбачені спеціальні засоби для регулювання висоти столу, клавіатури та екрану, а також підставка для рук.

Суттєве значення для продуктивної та якісної роботи на комп'ютерах має розміри знаків, щільність їх розташування, контраст та співвідношення яскравості символів та фону екрану. Якщо відстань від очей оператора до екрану дисплею складає 60…80 см, то висота знаку повинна бути не менше ніж 3 мм, оптимальне співвідношення ширини та висоти знаку складає 3:4, а відстань між знаками – 15…20% їх висоти. Співвідношення яскравості фона екрану та символів – від 1:2 до 1:15.

Під час роботи монітор потрібно встановлювати на відстань 50 – 60 см від очей. Верхня частина дисплея повинна бути на рівні очей або трохи нижче. Коли людина дивиться прямо перед собою, його очі відкриваються ширше, ніж коли він дивляться вниз. За рахунок цього площина обзору значно збільшується, викликає тим самим зневоднюючи очі. Якщо екран встановлений дуже високо, а очі широко відкриті, порушується функція моргання, що призводить до швидкої втоми.

Створення комфортних умов праці та правильне естетичне оформлення робочих місць на виробництві має велике значення як для полегшення труда, так й для підвищення його привабливості, що позитивно впливає на продуктивність праці.

А.4 Планування телекомунікаційного підрозділу

Відповідно до наведеного аналізу рекомендується розташувати меблі наступним чином

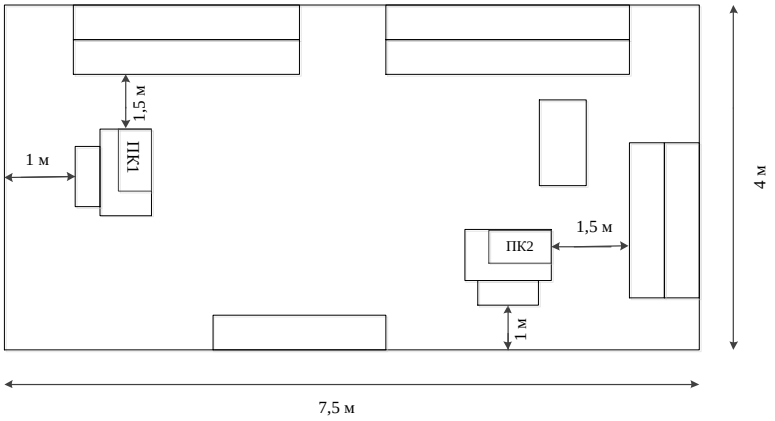


Рисунок А.3 – Розташування робочих місць відділу моніторингу згідно з ГОСТ

Облаштованість робочих місць відповідає вимогам санітарних норм та в приміщенні площею 30 м² та об’ємом 90 м³ можна розташовувати два робочих місць з ПК.

А.5 Розрахунок освітленості

Зазвичай штучне освітлення виконується за допомогою електричних джерел світла двох видів: ламп накалювання та люмінесцентних ламп. Будемо використовувати люмінесцентні лампи, які порівняно з лампами накалювання мають ряд суттєвих переваг:

- за спектральному складу світла вони близькі до денного, природнього світла;
- володіють більш високим ККД (у 1,5 – 2 рази вище, ніж ККП ламп накалювання);

– володіють підвищеною світловіддачею (у 3 -4 рази вище, ніжу ламп накалювання);
– більш тривалий термін дії.

Розрахунок проводиться для кімнати площею 30 м², довжина якої 7,5 м, ширина 4 м, висота 3 м. Приміщення має світлу побілку: коефіцієнт відбиття стелі Рп = 70%, стін Рс=50%. Висота робочих поверхонь столів $h_р$ = 0,7 м. Для освітлення приймаємо світильники типу ЛБ40-1, які підвішуються до стелі h_c=0,35 м. Мінімальна освітленість за нормами Е =400 лк.

Визначимо висоту підвісів світильників над підлогою:

$$h_о = H - h_с = 3 - 0,32 = 2,68 \text{ м} \quad (А.1)$$

Визначаємо висоту підвісу світильника над робочою поверхнею:

$$h = h_о - h_р = 2,68 – 0,7 = 1,98 \text{ м} \quad (А.2)$$

Визначаємо рекомендовану відстань між світильниками:

$$L = 0,7 \times H = 0,7 \times 3 = 2,1 \text{ м} \quad (А.3)$$

Розрахуємо необхідну кількість світильників:

$$N = \frac{A \times B}{L^2} = \frac{4 \times 7,5}{2,1^2} = 6,8 \approx 7 \text{ шт.} \quad (А.4)$$

Приймаємо 8 світильників (за розрахунками не менше 7), враховуючи розміри приміщення розміщуємо їх у два ряди по 4 штуки.

Для визначення кількості світильників визначимо світловий потік, який падає на поверхню, за формулою:

$$F = \frac{E \times K \times S \times Z}{N \times n \times \eta}, \quad (А.5)$$

де F – потік, який потрібно розрахувати, Лм;

Е – нормативна мінімальна освітленість, Лк (визначається за таблицею), у даному випадку Е = 400 Лк

К – коефіцієнт запасу, що враховує зменшення світового потоку лампи в результаті забруднення світильників у процесі експлуатації (його значення залежить від типу приміщень та характеру робіт, що в ньому проводяться. У нашому випадку К=1,5).

S – площа приміщення, що освітлюється (S = 30 м²).

Z – відношення середньої освітленості до мінімальної (зазвичай дорівнює 1,1…1,2, для люмінесцентних ламп Z = 1,1).

N – кількість світильників;

n – кількість ламп у світильнику;

η – коефіцієнт використання (виражається відношенням світового потоку, який падає на поверхню, до сумарного потоку всіх ламп та розраховується у долях одиниць, залежить від характеристик світильника, розмірів приміщення, забарвлення стін та стелі, які характеризуються коефіцієнтами відбиття від стін (Рс) та стелі (Рп)), значення коефіцієнтів Рс та Рп: 50% та 70% відповідно. Значення n визначимо за таблицею коефіцієнтів використання різних світильників. Для цього розрахуємо індекс приміщення за формулою:

$$I = \frac{S}{h \times (A+B)}, \qquad \text{(А.6)}$$

де:

S – площа приміщення

h – висота підвісу

А – ширина приміщення

В – довжина приміщення

Підставимо значення:

$$I = \frac{30}{2{,}68 \times (4 + 7{,}5)} = 0{,}97$$

Знаючи індекс приміщення І, визначаємо η =0,42.

Використовуємо світильник типу ОД, кожний з них комплектується двома лампами:

$$F = \frac{400 \times 1,5 \times 30 \times 1,1}{2 \times 8 \times 0,42} = 2946 \text{ лм}$$

Загальна електрична потужність усіх світильників становить:

$$\sum Pсв = P \times N = 2 \times 40 \times 8 = 640 \text{ Вт}$$

А.6 Розрахунок рівня шуму

Рівень шуму, який виникає від кількох некогерентних джерел, які працюють одночасно, розраховується на основі принципів енергетичного підсумування випромінювань окремих джерел:

$$L_{\Sigma} = 10 \lg \sum_{i=1}^{i=n} 10^{0,1 L_i}, \quad \text{(А.7)}$$

де L_i – рівень звукового тиску i – го джерела шуму;

n – кількість джерел шуму

Звичайне робоче місце оператору оснащено наступним обладнання: вінчестер у системному блоці, вентилятори систем охолодження, монітор, клавіатура, принтер та сканер.

Таблиця А.4 – Рівні звукового тиску різних джерел

Джерело шуму	Рівень шуму, дБ
Жорсткий диск	40
Вентилятор	45
Монітор	17
Клавіатура	10
Принтер	45
Сканер	42

$$L_{\Sigma} = 10\times\lg(10^{4}+10^{4,5}+10^{1,7}+10^{1}+10^{4,5}+10^{4,2}) = 49{,}5 \text{ дБ}$$

Отримане значення не перевищує допустимий рівень шуму на робочому місці оператору відділу моніторингу, що дорівнює 75 дБ (ГОСТ 12.1.003-83). До того ж периферійні пристрої як сканер та принтер рідко коли використовуються одночасно, крім того безпосередня присутність оператору при роботі принтера необов'язкова, адже принтер забезпечений механізмом автоподачі аркушів, тому ця цифра буде нижча.

А.7 Мікроклімат робочого місця

Витрату повітря в приміщенні з додатковим тепловиділенням визначається за формулою:

$$L = \frac{Q_{\text{над}}}{\text{c}\times\text{p}(t_{\text{в}}-t_{\text{н}})}, \text{м}^3/\text{год} \qquad \text{(А.8)}$$

де $Q_{\text{над}}$ – надлишкове виділення тепла в робочому приміщенні, ккал/год.;

с – теплоємність повітря (0,237 ккал/кг);

р – обсягова вага повітря (1,226 кг/м³);

$t_{\text{в}}$ – температура витяжного повітря (30ºС);

$t_{\text{н}}$ – температура повітря, що подається (20ºС);

Розрахуємо надлишкове надходження тепла по формулі:

$$Q_{\text{над}} = Q_{\text{уст}} + Q_{\text{пер}} + Q_{\text{осв}} + Q_{\text{ср}}, \qquad \text{(А.9)}$$

де $Q_{\text{уст}}$ - виділення тепла від устаткування;

$Q_{\text{пер}}$ – виділення тепла робітниками;

$Q_{\text{осв}}$ – надходження тепла від електричного освітлення;

$Q_{ср}$ – надходження тепла від сонячної радіації через вікна.

Визначимо виділення тепла від устаткування по формулі:

$$Q_{уст} = P \times К_а \times К_б \times 860 \quad \text{(А.10)}$$

Р – сумарна потужність устаткування, кВт/год.;

$К_а$ – коефіцієнт установленої потужності (0,95);

$К_б$ – коефіцієнт одночасної роботи (1,0).

$$Q_{уст} = [(x_1 \cdot k_1) + (x_2 \cdot k_2) + (x_3 \cdot k_3) + (x_4 \cdot k_4)] \cdot К_а \cdot К_б \cdot 860 \quad \text{(А.11)}$$

Розрахуємо:

$$Q_{уст} = [(6 \cdot 0{,}5) + (6 \cdot 0{,}1) + (1 \cdot 0{,}4) + (1 \cdot 6{,}3)] \cdot 0{,}95 \cdot 1 \cdot 860 = 3268 \quad \text{ккал/год.}$$

Визначимо виділення тепла від обслуговуючого персоналу за допомогою формули:

$$Q_{пер} = n \times g \quad \text{(А.12)}$$

n - кількість працюючих;

g - кількість тепла, що виділяє один працівник за годину (100 ккал/год.)

Розрахуємо:

$Q_{пер}$ = 2 х 100 = 200 ккал/год.

Визначимо надходження тепла від електричного освітлення за допомогою формули:

$$Q_{осв} = E_м \cdot g_1 \cdot S \quad \text{(А.13)}$$

$E_м$ - нормована освітленість для цієї зорової роботи приймаємо рівним 400 лк;

g_1 - питоме тепловиділення на 1 м^2 підлоги при 1 лк освітленості (для люмінесцентних ламп - 0,05 ккал/год.).

S - площа приміщення, м^2.

$$Q_{осв} = 400 \cdot 0{,}05 \cdot 30 = 600 ккал/год.$$

Визначимо надходження тепла від сонячної радіації через вікна за допомогою формули:

$$Q_{ср} = F \cdot g_2 \cdot K_{осл}, \qquad (А.14)$$

де F - площа віконних прорізів (1,55 м^2).

g_2 - кількість тепла, що надходить через 1 м^2 віконного прорізу (65 ккал/год.).

$К_{осл}$ - коефіцієнт ослаблення, приймаємо - 0,4.

Розрахуємо:

$Q_{ср}$=1,55·65·0,4 = 40,3 ккал/год.

Визначимо кількість надлишкового тепла:

$Q_{над}$= 3268 + 200 + 600 + 40,3 = 4108,3 ккал/год.

Визначимо витрати повітря в приміщенні:

$$L = \frac{4108{,}3}{0{,}237 \cdot 1{,}226 \cdot (30 - 20)} = 1414 м^3/год$$

Існуюча в наявності система кондиціонування і вентилювання має продуктивність 2000 куб. м./годину, що задовольняє необхідним нормативам.

Параметри мікроклімату на робочих місцях регламентуються ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень». Відповідно доданих санітарних норм температура повітря, швидкість руху повітря і відносна вологість у холодні періоди року повинна складати 22-24 градуса по Цельсію, 0,1 метра в секунду і 40-60 % відповідно. У теплі періоди

року температура повітря повинна складати 23-25 градусів Цельсія, рухливість повітря 0,1-0,2 метрів секунду, вологість 40-60 %. Температура може коливатися від 22 до 26 градусів Цельсія при збереженні всіх інших параметрів мікроклімату. Вище зазначені норми цілком відповідають фактичним даним приміщення відділу моніторингу.

А.8 Пожежна безпека

Найважливішою умовою роботи будь-якого підприємства є дотримання правил пожежної охорони.

У приміщенні телекомунікаційного підрозділу основні міри для забезпечення пожежної безпеки визначає Інструкція про заходи пожежної безпеки для службових приміщень. Вона є обов’язковою для виконання всіма співробітниками.

В інструкції про засоби пожежної безпеки для службових приміщень забороняється:

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

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

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

– захаращувати підступи до засобів пожежогасіння, використовувати пожежні крани, рукави і пожежний інвентар не по призначенню, зберігати

документи, різні матеріали, предмети й інвентар у шафах (нішах) інженерних комунікацій;

– курити (крім спеціально відведених для цього адміністрацією місць, позначених написом «Місце для паління» і забезпечених урною чи попільницею з матеріалу, що не горить), проводити зварювальні й інші вогневі роботи без оформлення відповідного дозволу, застосовувати легкозаймисті рідини.

По закінченню роботи необхідно:

– оглянути приміщення, переконатися у відсутності порушень, що можуть спричинити пожежу;

– відключити освітлення, електроживлення приладів і устаткування.

Електромережі, електроприлади і апаратура повинні експлуатуватися тільки у справному стані. У випадку виявлення ушкоджень електромереж, вимикачів, розеток ті інших електровиробів варто негайно відключити їх і вжити необхідних заходів до приведення їх в пожежобезпечний стан.

А.9 Безпека при надзвичайних ситуаціях на підприємстві

Об’єктом забезпечення на предмет визначення надзвичайних небезпек та їх наслідків є службове приміщення підприємства зв’язку. Однією із вірогідних загроз може бути раптове виникнення пожару внаслідок короткого замикання в електромережах або розрядів статистичної електрики, що може привести до пошкодження і руйнування будівлі, устаткування, комунікацій, виділення токсичних продуктів горіння.

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

Підприємство повинно бути обладнаним мережею протипожежного водо забезпечення, установками виявлення та гасіння пожеж відповідно вимогам

нормативно-технічних документів. Кожний працівник повинен чітко знати та виконувати вимоги ППБ та протиаварійний режим на об’єкті, уміти користуватися наявними вогнегасниками, іншими первинними засобами пожежогасіння і знати місце їхнього перебування.

Меблі й устаткування повинні розміщатися таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (шириною не менше 1 м). Евакуаційні шляхи і виходи необхідно постійно держати вільними, нічим не захаращувати. Засоби протипожежного захисту в приміщеннях потрібні триматися у справному стані.

У випадку виявлення пожежі слід:

– негайно повідомити державну пожежну охорону за телефоном «101», вказати при цьому адресу, кількість поверхів, місце виникнення пожежі, наявність людей, своє прізвище;

– повідомити про пожежу керівництву, а в нічний час черговому охоронцю;

У разі можливості почати гасіння пожежі наявними засобами, організувати зустріч пожежних підрозділів.

При виникненні пожежі у початковій стадії її розвитку випромінюється тепло, токсичні продукти згоряння, імовірні руйнування будівельних споруд. Тому слід як можна швидше провести евакуацію людей із палаючої будівлі. Показником ефективності евакуації є час, протягом якого працівники можуть при потрібності залишити окремі приміщення і будівлю в цілому. Безпека евакуації досягається тоді, коли час евакуації не перевищує час настання критичної фази розвитку пожежі, тобто часу від початку пожежі до досягнення граничних для людини впливів факторі пожежі (критичних температур, ступені задимлення, зниження концентрації кисню и т.п.). Число евакуаційних виходів повинно бути не менш двох. Вони повинні розташовуватися розосереджено. Мінімальна відстань l між найбільш віддаленими один від одного евакуаційними виходами із приміщення визначається за формулою:

$$l=1{,}5\sqrt{P}\ , \qquad \text{(А.15)}$$

де Р – периметр приміщення, м.

$l = 1{,}5\times\sqrt{2 \times (7{,}5 + 4)} = 7{,}2$ м

Двері на шляхах евакуації повинні відкриватися у напрямку виходу із будівлі (приміщення).

У кожному приміщенні на видному місці повинен бути вивішений план евакуації при пожежі.

При пожежі обов'язково необхідно враховувати небезпечні чинники і механізм їх дії на людину.

При виникненні пожежі, після виклику пожежної охорони, необхідно попередити про це усіх, хто знаходиться поруч, після чого евакуюватися самому і по можливості допомогти евакуюватися іншим, особливо особам літнього віку і дітям, попереджаючи при цьому виникнення паніки. З метою обмеження циркуляції повітря, яке здатне збільшувати швидкість горіння, покидаючи приміщення, закрийте за собою усі двері, якщо це можливо.

Якщо пожежа виникла в приміщенні над вами і безпосередньої загрози для вас не спостерігається, то бажано виконати заходи по зниженню можливих втрат від води яку проливають при гасінні пожежі. Для цього необхідно відключити всі електроприводи та прикрити їх поліетиленовою плівкою. Значно гірше, якщо пожежа виникла в приміщенні над вами – потрібно оцінити обстановку и якщо є впевненість, що ще не має сильної задимленості з високою температурою, потрібно негайно покинути приміщення, рухаючись до виходу по коридорам і сходовим кліткам.

Користуватися ліфтом категорично забороняється, за винятком ліфтів, які спеціально призначені для транспортування пожежної охорони. Шахта ліфта є шляхом для поширення диму і отруйних продуктів горіння, до того ж при пожежі ліфт часто відключають і можна опинитися в пастці при пожежі.

Якщо ви знаходитеся в приміщенні де немає пожежі, але відрізани вогнем, димом, високою температурою від головних шляхів евакуації, то в першу чергу необхідно заважити доступу диму и продуктів горіння в це приміщення. Для чого

необхідно негайно закрити усі щілини у дверях та під ними змоченими водою ганчірками, рушниками, робочими халатами та інш.

Якщо приміщення все ж заповнено димом, необхідно підповзти до вікна, закрити при цьому рот та ніс змоченою тканиною, яка грає роль фільтру та в певної мірі захищає від продуктів горіння.

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

А.10 Висновки

У заключному розділі було висунуто вимоги щодо облаштування робочого місця оператора системи служби безпеки телекомунікаційного підрозділу та приміщення взагалі. Було наведено розрахунки освітленості, рівня шуму та мікроклімату. Розраховані величини задовольняють всі вимоги згідно с санітарними правилами та нормами:

- світловий потік F = 2946 Лм, тому використовуємо 8 світильників;
- рівень шуму L = 49,5 Дб;
- витрати повітря в приміщенні L =1414 м³/год.