ДВНЗ «Донецький національний технічний університет»
Навчально-науковий інститут комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)
Кафедра автоматики та телекомунікацій
(повна назва кафедри)

«До захисту допущено»
Завідувач кафедри автоматики та телекомунікацій
_____ Валерій ПОЦЕПАЄВ
(підпис) (ім'я та прізвище)
«___» _____ 2025 р.

Випускна кваліфікаційна робота

бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Проектування телекомунікаційної структури готельного комплексу монастиря «Franziskanerinner von Route»

Виконав студент 4 курсу, групи ТКР-21
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

Колісник Олександр Сергійович
(Прізвище, Ім'я та По-батькові) (підпис)

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

Рецензент Ph.D., доц. каф. ПМІ _____ Микита АЛЕКСАНДРОВ
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Нормоконтроль:
Дар'я ЖУКОВСЬКА
17.06.2025 р.

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

Студент _____
(підпис)

Дрогобич – 2025 р.

ДВНЗ «Донецький національний технічний університет»

Навчально-науковий інститут комп'ютерно-інформаційних технологій та автоматизації

(повне найменування інституту, назва факультету)

Кафедра автоматики та телекомунікацій

(повна назва кафедри)

Захист відбувся _____

(дата)

з оцінкою_____

Секретар ЕК _____

(підпис)

Випускна кваліфікаційна робота

бакалавра

Тема: «Проектування телекомунікаційної структури готельного комплексу монастиря «Franziskanerinner von Route»

Виконавець, студент
гр. ТКР-21 _____ Олександр КОЛІСНИК
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Керівник _____ Гліб СТУПАК
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Консультанти: _____ Анна ВОРОПЄВА
(підпис, дата, Ім'я ПРІЗВИЩЕ)

_____ Дар'я ЖУКОВСЬКА
(підпис, дата, Ім'я ПРІЗВИЩЕ)

_____ Олександр СЕРГІЄНКО
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Нормоконтроль _____ Дар'я ЖУКОВСЬКА
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Дрогобич – 2025 р.

Державний вищий навчальний заклад

"Донецький національний технічний університет"

Навчально-науковий інститут комп'ютерно-інформаційних технологій та автоматизації

Кафедра Автоматика та телекомунікації

Освітньо-кваліфікаційний рівень бакалавр

Галузі знань 17 Електроніка та телекомунікації
(шифр і назва)

Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри АТ
Валерій ПОЦЕПАЄВ
«____» _____2025 року

З А В Д А Н Н Я

НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Колісніку Олександру Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) «Проектування телекомунікаційної структури готельного комплексу монастиря «Franziskanerinner von Route»
керівник проекту (роботи) Ступак Гліб Володимирович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від 11.04.2025 року № 115

2. Строк подання студентом проекту (роботи)_____

3. Вихідні дані до проекту (роботи)_____
Технічна документація та матеріали з переддипломної практики, характеристика об'єкту та вимоги до проєктування мереж

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): аналіз поточних потреб готелю у телекомунікаційних послугах, визначення функціональні та технічні вимоги; концепція конвергентної IP-мережі та архітектуру; опис мережевих технологій та протоколів; структурна та функціональна схеми мережі; вибір активного та пасивного мережевого обладнання; імітаційне моделювання мережі

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
план поверхів, структурна схема мережі, функціональна схема мережі, схема розміщення обладнання, схема з'єднань

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Ступак Г.В., ст. викл. каф. АТ		
2	Воропаєва А.О., доц. каф. АТ		
3	Жуковська Д.О., ст. викл. каф. АТ		
Додаток А	Сергієнко О. І. к.т.н., доц. каф. УГВіОП		
Нормо-контроль	Жуковська Д.О., ст. викл. каф. АТ	-	17.06.2025 р.

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз об’єкту	01.05.2025	
2	Розробка архітектури мережі	15.05.2025	
3	Апаратний синтез та основні налаштування	05.06.2025	
4	Охорона праці та безпека під час надзвичайних ситуаціях на підприємстві	08.06.2025	

Студент _____ **Олександр КОЛІСНИК**
(підпис) (прізвище та ініціали)

Керівник роботи _____ **Гліб СТУПАК**
(підпис) (прізвище та ініціали)

ЛИСТ ЗАУВАЖЕНЬ

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

АНОТАЦІЯ

Колісник, О.С. «Проектування телекомунікаційної структури готельного комплексу монастиря «Franziskanerinner von Route» / Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» зі спеціальності 172 Телекомунікації та радіотехніка. – ДВНЗ «ДонНТУ», Дрогобич, 2025.

Пояснювальна записка: 93 стор., 9 рис., 13 табл., 20 посилання.

Кваліфікаційна робота бакалавра присвячена розробці сучасної конвергентної IP-мережі для готельного комплексу «Franziskanerinner von Route». Актуальність роботи зумовлена необхідністю створення високоефективної та безпечної телекомунікаційної інфраструктури.

Метою роботи є розробка та обґрунтування архітектури конвергентної IP-мережі, що забезпечить надання сучасних телекомунікаційних послуг.

У ході роботи проведено аналіз потреб готелю (до 213 осіб, 794 активних підключення, навантаження 1470 Мбіт/с), обґрунтовано концепцію ієрархічної трирівневої мережі на базі Fast/Gigabit Ethernet та Wi-Fi 6. Розроблено структурну та функціональну схеми, використано 802.1q, QoS, NAT та ACL для безпеки та ефективності. Здійснено вибір та обґрунтування активного мережевого обладнання, переважно від Cisco,. Пасивна частина представлена повноцінною СКС на компонентах Molex. Працездатність розробленої мережі та коректність рішень підтверджено імітаційним моделюванням.

Ключові слова: КОНВЕРГЕНТНА МЕРЕЖА, IP-ТЕЛЕФОНІЯ, IPTV, СКУД, IOT, CISCO, MOLEX, HTNG, СКС, МОДЕЛЮВАННЯ.

ЗМІСТ

ВСТУП

Актуальність роботи полягає у нагальній потребі створення сучасної, високоефективної та безпечної телекомунікаційної інфраструктури для готельного комплексу «Franziskanerinner von Route». В умовах поточної реконструкції готелю виникає необхідність переосмислення застарілих підходів і впровадження принципово нових мережевих та архітектурних рішень. Сучасний готельний бізнес вимагає не лише надійного доступу до Інтернету, а й інтеграції різноманітних послуг, таких як IP-телефонія, IPTV/VoD, системи контролю доступу (СКУД) та Інтернет речей (IoT). Застосування конвергентних рішень, що відповідають галузевим стандартам Hospitality Technology Next Generation, дозволить значно підвищити якість обслуговування гостей, оптимізувати операційні процеси, посилити безпеку та забезпечити конкурентні переваги на ринку гостинності.

Мета роботи – розробка та обґрунтування архітектури конвергентної IP-мережі для готельного комплексу «Franziskanerinner von Route», що забезпечуватиме надання сучасних телекомунікаційних послуг відповідно до вимог Hospitality Technology Next Generation (HTNG).

Завдання проектування/дослідження:

1. Провести аналіз поточних потреб готельного комплексу у телекомунікаційних послугах та визначити ключові функціональні та технічні вимоги до проектованої мережі.
2. Обґрунтувати концепцію побудови конвергентної IP-мережі та розробити її архітектуру, включаючи вибір мережевих технологій та протоколів.
3. Розробити структурну та функціональну схеми мережі, відобразивши взаємодію її компонентів.
4. Здійснити вибір та обґрунтування активного мережевого обладнання (маршрутизаторів, комутаторів, точок доступу, пристроїв IP-телефонії, відеоспостереження) відповідно до

визначених вимог.

5. Визначити перелік та обґрунтувати вибір пасивних компонентів структурованої кабельної системи (СКС).
6. Провести імітаційне моделювання розробленої мережевої моделі та перевірити її працездатність.

Об’єктом в роботі виступає готельний комплекс «Franziskanerinner von Route» як єдиний об'єкт для впровадження телекомунікаційної інфраструктури.

Предметом є телекомунікаційна інфраструктура готельного комплексу, що охоплює її архітектуру, компоненти, технології та принципи функціонування.

Методи дослідження: У роботі були використані такі наукові методи дослідження:

- системний аналіз – для комплексного вивчення готельного комплексу як об'єкта проектування, визначення взаємозв'язків між підсистемами телекомунікаційної інфраструктури;
- порівняльний аналіз – для зіставлення різних мережевих технологій, протоколів та моделей обладнання з метою вибору найбільш оптимальних рішень;
- метод моделювання – для створення віртуальної моделі проектованої мережі в середовищі Cisco Packet Tracer, що дозволило імітувати роботу мережевих компонентів, тестувати конфігурації та перевіряти працездатність системи;
- метод розрахунку – для визначення необхідної пропускної здатності мережі, розрахунку трафіку та обґрунтування вимог до продуктивності обладнання.

Структура та загальний обсяг випускної кваліфікаційної роботи. Робота складається зі вступу, 3 основних розділів, висновків, переліку посилань на 20 джерел та 2 додатків. Загальний обсяг роботи становить 92 сторінок, 9 рисунків та 13 таблиць.

1 АНАЛІЗ ОБ’ЄКТУ

1.1 Загальна характеристика об’єкту проєктування

В якості об’єкту проєктування у випускній кваліфікаційній роботі виступає готельний комплекс, що знаходиться на території монастиря «Franziskanerinner von Route», що розташований у Німеччині, за адресою Klostergasse 6, 88339 Bad Waldsee.

Монастир сестер-францисканок у Реуте, має глибоку історію, що сягає 19 століття. Його заснування пов'язане з п'ятьма жінками, які в 1848 році в Ехінгені започаткували спільноту, присвячену служінню Богові через допомогу страждаючим людям. Ця спільнота стала першою новою чернечою громадою в тодішньому Королівстві Вюртемберг. У 1869 році вони переїхали до Реуте, де придбали покинуту будівлю францисканського монастиря, який став їхнім постійним осередком у 1870 році. Зі збільшенням паломників та прихожан, у монастирі був відкритий невеликий готельний комплекс. Комплекс знаходиться у мальовничій місцевості Верхньої Швабії, оточеній природними ландшафтами, неподалік від історичного центру міста Бад-Вальдзее (рис. 1.1) .

Рисунок 1.1 – Загальний вигляд монастиря та готельного комлексу

Готельний комплекс представляє собою будівлю з п’ятьма поверхами, на кожному з яких розташовано близько 10 комфортабельних номерів для гостей, і пропонує розвинену інфраструктуру, що включає:

- затишний ресторан з традиційною та європейською кухнею;
- зону відпочинку та читальні кімнати;
- розвинену систему інженерних комунікацій, включаючи автономне водопостачання, енергозабезпечення та систему очищення стічних вод [1].

Телекомунікаційна інфраструктура готельного комплексу сьогодні представляє собою Wi-Fi інфраструктуру з доступом до мережі Інтернет. Як такої складової послуг локального голосового зв’язку, системи кабельного чи IP-телебачення, системи гучного оповіщення, системи відеоспостереження, системи контролю доступу в готельному комплексі немає.

У жовтні 2023 року розпочалася генеральна реконструкція материнського дому монастиря з метою його оновлення та відкриття для ширшої спільноти. У рамках цього проекту заплановано створення нових житлових приміщень, гостьових зон та просторів для відвідувачів і проведення заходів. Цей проект отримав підтримку від уряду землі Баден-Вюртемберг як «інноваційний проект»

Оскільки сучасний рівень телекомунікаційного забезпечення потребує модернізації, важливим завданням є розробка ефективної та якісної телекомунікаційної інфраструктури. Вона забезпечить стабільний інтернет-зв’язок та інтеграцію цифрових технологій для покращення обслуговування гостей та підвищення рівня безпеки.

1.2 Визначення ключових типів послуг

Сучасний готельний комплекс, яким після реконструкції має стати готель на території монастиря «Franziskanerinner von Route» повинен забезпечувати

належний рівень комфорту та безпеки для постояльців.

Крім загальноприйнятих стандартів телекомунікацій, особливу увагу при розробці готельної інфраструктури слід приділяти галузевим рекомендаціям, зокрема розробленим Hospitality Technology Next Generation (HTNG). HTNG — провідна світова асоціація, що сприяє стандартизації та інтеграції технологій гостинності, що є ключем до забезпечення взаємодії та ефективності готельних систем. Основна HTNG місія – сприяти розробці та впровадженню технологій наступного покоління у готельній сфері та сфері розміщення через співробітництво та партнерство [2].

Пристрої, програми, мобільність і постійна потреба в зростаючій швидкості та пропускній здатності, а також інтегровані послуги значно впливають на індустрію гостинності та готельного бізнесу. Гості все частіше очікують таких самих або кращих послуг у дорозі, як і вдома. Не тільки технології, орієнтовані на гостей, повинні бути передовими, але й мережа Back of House (BoH) повинна вдосконалюватися разом із цим технологічним зростанням, щоб підтримувати програми та послуги, необхідні для роботи готелю.

Пристрої, операції та інші програми для гостей, що використовуються сьогодні, зазвичай не враховувалися під час проектування, будівництва або реконструкції більшості готелів. Застарілі інфраструктурні мережні рішення для готельних комплексів використовують спеціалізовану інфраструктуру для кожної програми та послуги. Це створює ефект ізоляції для кожної системи, необхідної для готелю. Наприклад, телефонна, відео та високошвидкісна системи доступу до Інтернету (HSIA) мають власну інфраструктуру, що працює паралельно (рис. 1.2). Крім того, існує багато систем керування номерами (RMS) та систем керування будівлями (BMS), які потребують власної, виділеної інфраструктури.

З розвитком програм та послуг вони все частіше переходять на інтернет-протокол (IP) та технологію Ethernet для зв'язку. Для підтримки готелю потрібно все більше послуг, і деякі з цих послуг демонструють експоненціальне

зростання вимог до пропускної здатності. Ця еволюція надає можливість об'єднати різні ізольовані мережі в єдину спільну інфраструктуру (рис. 1.2).

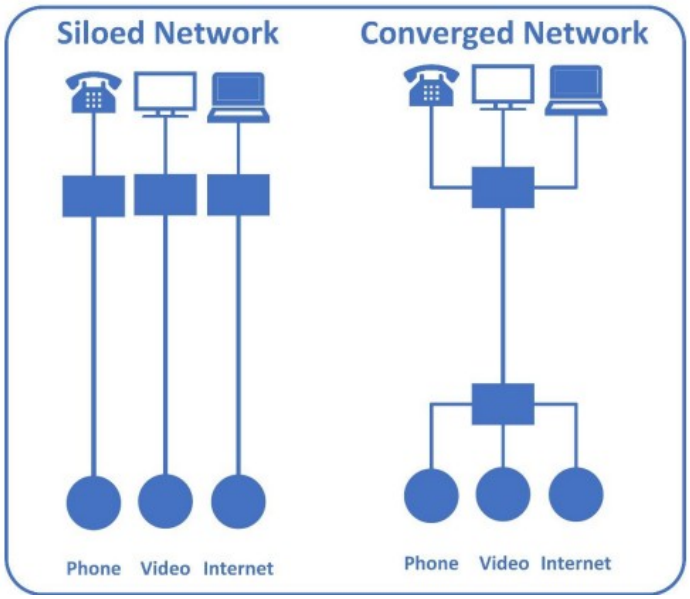

Рисунок 1.2 – Ізольована та конвергентна мережна інфраструктура

Бізнес-кейс для конвергентної інфраструктури передбачає об'єднання деяких або всіх цих послуг по всій будівлі в єдину інфраструктуру з можливістю їх підтримки. Це означає, що конвергентна інфраструктура повинна підтримувати поточні вимоги до пропускної здатності всіх програм та послуг, а також передбачати майбутні вимоги до пропускної здатності як гостей, так і ВоН [3].

З точки зору інфраструктурного рішення, готельний номер сьогодні повинен бути інтегрований як з окремими сервісами, що призначені для постояльців так і з загальними сервісами та службами управління будівлею в цілому. На рис. 1.3 показані основні пристрої які створюють навантаження на мережу передачі даних з огляду на кожний індивідуальний готельний номер [3]. Номери готелю налаштовуються для підтримки кількох режимів обслуговування, орієнтованих на гостей, що потребують надійної кабельної та бездротової інфраструктури. Для того щоб забезпечити різні режими адаптації, інфраструктура номеру повинна мати окрім класичного набору послуг ще й

набір сенсорів Інтернету речей для забезпечення належного рівня безпеки та комфорту гостя.

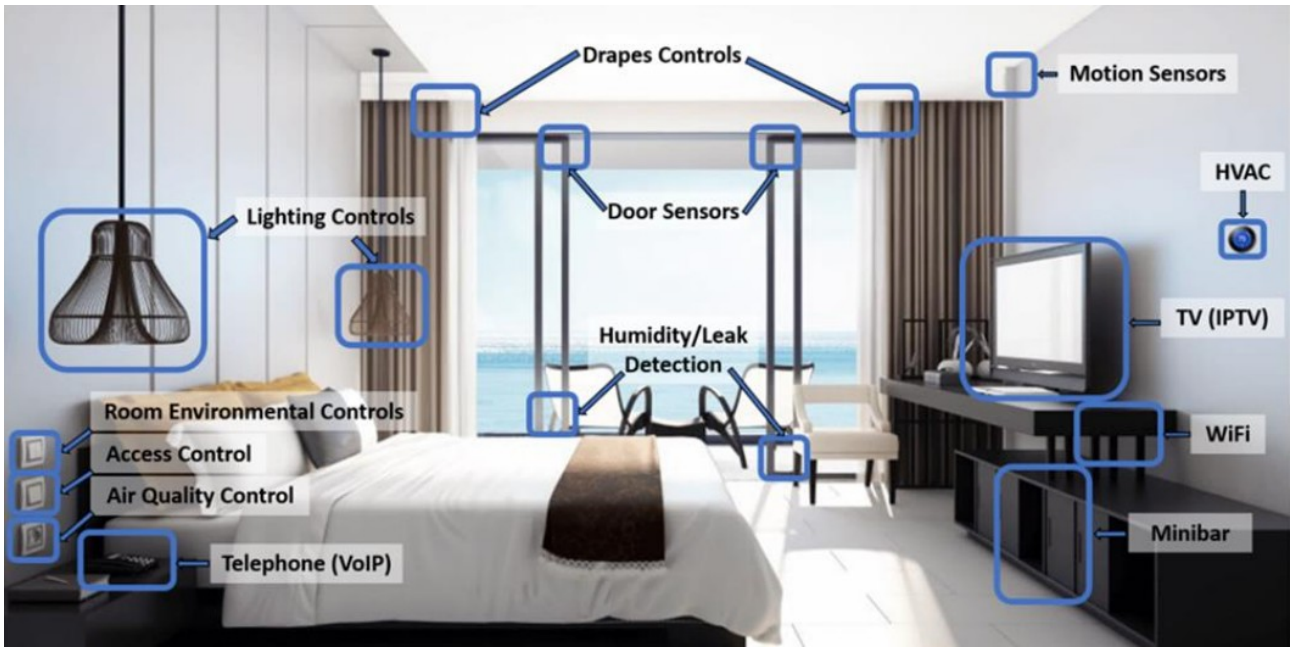

Рисунок 1.3 – Інфраструктурні рішення готельного номеру

Кожен з цих сервісів може потребувати подібних або різних мережевих протоколів, але все одно потребує надійної мережевої інфраструктури для підтримки всіх мережевих протоколів. Крім того, розгортання деяких або всіх програм та функцій, показаних на рис. 1.3, може потенційно зменшити витрати на утримання та обслуговування номеру завдяки сучасним засобам автоматизації та моніторингу.

Виходячи з сучасних вимог, телекомунікаційна мережа готелю – це не просто доступ до Інтернету, а комплексна система, що забезпечує комфорт, безпеку та ефективність як для гостей так і для персоналу.

Нижче наведемо основні функції та послуги, що має надавати мережна інфраструктура відповідно до рекомендацій [4].

Для постояльців телекомунікаційна інфраструктура повинна забезпечувати та надавати такі послуги:

1. Високошвидкісний доступ до Інтернету (Wi-Fi або дротовий):

– безкоштовний базовий доступ – швидкість достатня для перегляду

веб-сторінок, електронної пошти та соціальних мереж;

- преміум-доступ (платний або для VIP-гостей) – висока швидкість, мала затримка, гарантована пропускна здатність для потокового відео, онлайн-ігор, відеоконференцій;
- стабільне покриття WiFi – роумінг по всьому готелю (номери, вестибюлі, ресторани, конференц-зали, зони відпочинку);
- підтримка кількох пристроїв – можливість одночасного підключення смартфонів, ноутбуків, планшетів.

2. IP-телефонія (VoIP):

- внутрішній зв'язок – дзвінки між номерами, на рецепцію, до ресторану, тощо;
- зовнішній зв'язок –здійснення міжміських та міжнародних дзвінків відповідно до тарифів готелю;
- додаткові сервіси – «Будильник», «Не турбувати», голосова пошта, доступ до інформації про готель.

3. Інтерактивне телебачення (IP-TV):

- вибір телеканалів – місцеві, національні, міжнародні канали на різних мовах;
- відео за запитом (VoD) – бібліотека фільмів, серіалів, мультфільмів (безкоштовно або платно);
- інформація про готель – меню ресторану, розклад подій, послуги готелю, карта готелю;
- послуги готелю – замовлення їжі в номер, бронювання процедур та додаткових послуг, виклик таксі, перевірка рахунку;
- персоналізовані повідомлення – привітання, нагадування, спеціальні пропозиції.

4. Доступ до функцій розумного номера (IoT):

- керування освітленням, шторами, кліматом з пульта дистанційного керування номера, смартфона або IP-TV;

– можливість налаштування сценаріїв (наприклад, «режим сну», «режим перегляду фільмів»).

5. Системи безпеки та оповіщення:

– доступ до систем контролю доступу (електронні ключі-картки);

– система пожежної безпеки та гучномовного оповіщення.

Для співробітників готелю телекомунікаційна інфраструктура повинна забезпечувати та надавати такі послуги:

1. Корпоративна IP-телефонія:

– Інтерком – голосові дзвінки між відділами, співробітниками;

– зовнішній зв'язок – доступ до зовнішніх ліній з можливістю встановлення цін та контролю;

– розширені функції – конференц-виклики, переадресація викликів, групи викликів, автовідповідач, голосова пошта;

– інтеграція з CRM/PMS – автоматичне відображення інформації про клієнта під час вхідного дзвінка.

2. Високошвидкісний інтернет та корпоративна мережа:

– доступ до внутрішніх ресурсів – сервери, бази даних, файлові сховища, принтери;

– доступ до хмарних сервісів – системи управління готелями (PMS), бухгалтерські програми, системи бронювання;

– віртуальні приватні мережі (VPN) – безпечний віддалений доступ для співробітників, які працюють поза готелем.

3. Система управління готелем (PMS):

– доступ до PMS – мережа є основою для системи реєстрації, бронювання, управління номерами, виставлення рахунків.

– інтеграція з іншими системами – CRM, платіжні системи, POS-термінали ресторанів.

4. Система безпеки:

– IP-відеоспостереження – моніторинг камер відеоспостереження в

режимі реального часу, архівування записів;

- системи контролю доступу (СКД) – управління доступом персоналу до різних частин готелю, облік робочого часу, управління доступом до номерів для постояльців та гостей;
- система пожежної сигналізації та оповіщення – швидке реагування на надзвичайні ситуації та ідентифікація осередків займання.

5. Система управління будівлею (BMS) – моніторинг та керування інженерними системами готелю такими як електропостачання, освітлення, вентиляція, кондиціонування, опалення, ліфти.
6. Системи позиціонування та визначення місцезнаходження – для відстеження персоналу, інвентарю у надзвичайних ситуаціях.

Виходячи з перерахованих рекомендацій та специфіки об’єкта проєктування, в табл. 1.1 наведемо перелік послуг для двох категорій абонентів.

Таблиця 1.1 – Перелік послуг мережної інфраструктури

№	Послуга	Гості	Персонал
1	IP-телефонія з виходом до ТМЗК	+	+
2	IPTV, відео за запитом	+	+
3	Інтернет WiFi	+	+
4	Інтернет з підключенням Ethernet		+
5	Локальна мережа		+
6	IP-відеоспотереження		+
7	IoT, керування номерами	+	+
8	IoT, керування будівлею (BMS)		+
9	Система гучного оповіщення	+	+
10	Пожежна сигналізація		+
11	Система контроля доступу	+	+

1.3 Аналіз абонентського складу

Під аналізом абонентського складу розуміють зазвичай характеристику кількості кінцевих користувачів тими чи іншими послугами, але на практиці дана термінологія охоплює значно ширше значення. Зокрема сюди входять всі типи пристроїв, що можуть бути під'єднані до телекомунікаційної інфраструктури безпосередньо використовуючи проводове чи безпроводове підключення, а також пристрої чи служби що мають можливість віддалено підключатись до мережі і використовувати цифровий інформаційний простір і відповідні сервіси (доприкладу це можуть бути співробітники, що працюють віддалено, служби охорони та моніторингу з можливістю перегляду відеорахівів).

Визначення кількості абонентів, користувачів та обладнання, яке буде підключатись до мережної інфраструктури є одним з ключових етапів проєктування будь-якої телекомунікаційної мережі. Від точності визначеної кількості точок підключення залежить як інфраструктурна компонента, а саме наявність кабельної розводки, так і обраний тип обладнання в залежності від розрахованих параметрів навантаження.

Як вже зазначалось раніше, готельний комплекс представляє собою п'яти поверхову будівлю в середньому з 10 номерами для гостей на поверсі, а також ресторан, зону відпочинку, адміністративну частину прачечні для загального користування, стійку адміністратора, конференц зону та читальні простори і зони відпочинку в загальних просторах в холах на поверхах готелю.

На рис.Б.1-Б.3 в додатку Б, наведено поверховий план об'єкту проєктування. Номерний фонд представляє собою двомісні, тримісні та чотиримісні номери (табл. 1.2). Кожен з номерів, публічних зон та офісно-адміністративних приміщень мають бути обладнані відповідним устаткуванням та точками для підключення до телекомунікаційної інфраструктури готельного комплексу згідно номенклатурою послуг та групами користувачів, що наведені в табл. 1.1.

Таблиця 1.2 – Класифікацій приміщень за поверхами

Поверх	№ приміщення	Тип
1	001-005, 101-110	Двомісний номер
	006	Тримісний номер
	007, 009	Адміністративне приміщення
	008	Двокімнатний чотиримісний номер
	3, 4	Хол, зона ресепшн
	WC	Санвузли, прачечна
2	201-204, 209-211	Двомісний номер
	205, 208	Двокімнатний чотиримісний номер
	206, 207	Тримісний номер
	5	Конференц зона
3	301-309	Двомісний номер
	6	Відпочинкова зона, читальня
	Кухня, Прачена	
4	401-404, 408-410	Двомісний номер
	405, 407	Двокімнатний чотиримісний номер
	406	Ресторан
	7	Відпочинкова зона, читальня
5	501-509	Двомісний номер
	8	Відпочинкова зона, читальня
	Кухня, Прачена	

Як виходить з наведеної таблиці (табл. 1.2), максимальна кількість постояльців, що одночасно можуть перебувати на території готельного комплексу у 55 номерах становить 123 особи (94 у двомісних номерах, 9 у тримісних номерах, 20 у чотиримісних). У випадку проведення масових заходів, до прикладу обслуговування конференцій, то розрахункова кількість відвідувачів становить 70 осіб. Загальна кількість обслуговуючого персоналу становить 10 осіб (1 адміністратор, 2 охоронця, 4 прибиральниці, 2 кухаря, 1

офіціант). Отже, таким чином максимальна кількість осіб, що може перебувати на території готелю становить 213 осіб.

Відповідно до проведеної класифікації послуг (табл. 1.1, рис. 1.3) та експлікації приміщень на кожному поверху згідно з табл. 1.2 та рис. Б.1-Б.3 у додатку Б необхідно визначити та класифікувати кількість абонентських та користувальницьких пристроїв, типи підключень до телекомунікаційної інфраструктури як безпосередньо з приміщення готелю так і з зовнішніх мереж для надання відповідних послуг. В табл. 1.3 зведена сумарна класифікація типів абонентських пристроїв та термінального устаткування.

Таблиця 1.3 – Типи та кількість кінцевого термінального устаткування

Найменування	Кількість	Примітка
IPTV	63	55 в номерах, 8 у зонах загального користування та адміністративній частині
IP-телефон	67	55 в номерах, 12 у зонах загального користування та адміністративній частині
IP-камера	16	Встановлені загальних просторах
Датчик протипожежної безпеки	96	Встановлено в номерах та в зонах загального користування
Мобільні пристрої	416	Максимальна кількість персональних мобільних пристроїв співробітників та відвідувачів, з розрахунку по два гаджети на одну особу
IoT номери	55	Точки підключення контролерів для керування мікрокліматом в номерах
IoT BMS та СКУД	69	63 точки підключення СКД у приміщеннях, 6 контролерів IoT BMS
Стаціонарне підключення	12	4 персональні комп’ютери, 2 POS-термінали, 6 сервери та BMS обладнання

Як бачимо, телекомунікаційна інфраструктура готелю повинна забезпечувати надійне підключення з гарантованими параметрами та комфортну роботу в мережі що найменше для 794 пристроїв, які можуть знаходитись одночасно на території готелю. Окрім цього варто передбачити можливість підключення ззовні до підсистем BMS, відеоспостереження, протипожежної безпеки та СКУД.

1.4 Розрахунок параметрів навантаження

Розрахунок параметрів навантаження дає можливість оцінити потребу у пропускній здатності активного та пасивного обладнання телекомунікаційної інфраструктури а також визначити необхідний рівень швидкості каналу для зовнішнього підключення до провайдера Інтернет послуг. Розрахунок параметрів навантаження базується на методиці, що викладена у [5] та частково на власному досвіді та судженнях, бо як такої універсальної методології розрахунку, яка б враховувала всі аспекти не існує.

Для проведення розрахунку трафіку треба спиратись на такі вхідні дані:

- тип готелю (бутик, середній, великий комплекс);
- номерний фонд;
- заповнюваність постояльцями та їх кількість;
- тип постояльців (бізнес-туристи – стабільний відеозв'язок; молодь та активні туристи – стрімінг, соцмережі; сім'ї з дітьми – ігри, потокове відео; літні люди – голосовий та відеозв’язок);
- середнє значення кількості пристроїв на користувача чи номер (це можуть бути як персональні пристрої так і стаціонарні, що забезпечують безперебійну діяльність готелю та надання різноманітних послуг гостям та постояльцям);
- перелік послуг що надаються постояльцям, гостям, адміністрації та персоналу;

- характеристики послуг, що надаються мережею (пропускна здатність, інтенсивність використання);
- зони покриття з підвищеним навантаженням або ж збільшеною концентрацією абонентських терміналів (конференц-зали, ресторани і т.д.).

Маючі всі ці дані, можна переходити до розрахунку. Можна використовувати спрощену формулу, а можна застосувати підхід заснований на ймовірнісних показниках та характеристиках послуг, абонентської активності та тривалості сеансів зв'язку, як це описано в [5]. Більш точні моделі використовують статистику розподілу Пуассона або Ерланга для розрахунку навантаження голосового трафіку та відеодзвінків. В основі розрахунку навантаження послуг пов'язаних з передачею даних без особливих вимог до QoS також беруть ймовірнісні моделі Ерланга, але при розрахунку використовують найгірший сценарій для оцінки пікового навантаження. Для оцінки необхідної пропускної здатності телекомунікаційної інфраструктури в готельному комплексі скористаємось спрощеним підходом (1.1):

$$S=N\times P\times K\times B\times C \qquad (1.1);$$

Де:

S – питома пропускна здатність для Інтернету;

N – кількість номерів;

P – середня кількість пристроїв на номер;

K – середня заповнюваність (частка);

B – середній бітрейт на пристрій для споживання тієї чи іншої послуги, Мбіт/с;

C – коефіцієнт одночасного використання.

Отже, виходячи з наведеної формули необхідно для кожного типу трафіку визначити середній бітрейт для послуг, і визначити на яких типах кінцевих пристроїв можуть бути використані послуги, що надаються мережею.

В табл. 1.4 наведено відповідність послуг, що надаються мережею, до кінцевих термінальних пристроїв і пристроїв користувачів.

Таблиця 1.4 – Відповідність послуг та пристроїв

Термінальний пристрій	Кількість	Послуги
IPTV	63	IPTV, відео за запитом
IP-телефон	67	IP-телефонія з виходом до ТМЗК, Система гучного оповіщення
IP-камера	16	IP-відеоспотереження
Датчик протипожежної безпеки	96	Локальна мережа
IoT номери	55	Локальна мережа, Інтернет з підключенням Ethernet, Система контроля доступу, IoT керування номерами
IoT BMS та СКУД	69	Локальна мережа, Інтернет з підключенням Ethernet, Система контроля доступу, IoT керування номерами та будівлею (BMS)
Мобільні пристрої	416	Інтернет WiFi
Стаціонарне підключення	12	Інтернет з підключенням Ethernet, Локальна мережа, IP-відеоспотереження IoT керування номерами та будівлею (BMS), система гучного оповіщення, пожежна сигналізація, система контроля доступу

Для кожного з типів послуг необхідно визначити ключові параметри, які необхідні для проведення розрахунків трафіку на послуги і загального навантаження на телекомунікаційну інфраструктуру.

Найбільший обсяг трафіку в готельній інфраструктурі – доступ до Інтернет, який включає:

- базовий перегляд веб-сторінок та регулярне оновлення електронної пошти – 0,5-1 Мбіт/с на пристрій;
- соціальні мережі та месенджери – 1-2 Мбіт/с;
- перегляд HD-відео (Netflix, YouTube) – 3-5 Мбіт/с;
- UHD (4K) стрімінг – 15-25 Мбіт/с;
- відеоконференції – 1-3 Мбіт/с;
- онлайн-ігри – 0,5-2 Мбіт/с.

Коефіцієнт одночасного використання для доступу до Інтернет може лежати в межах 0,05-0,7, через те, що не всі гості одночасно користуються всіма сервісами на повну потужність. Доступ до мережі Інтернет для постояльців, гостей, адміністрації та персоналу буде виконуватись через безпроводову мережу. Для стаціонарних точок, підключення буде виконуватись за технологією Ethernet, зі швидкістю до 100 Мбіт/с, при цьому рівень утилізації каналу не перевищуватиме 50%, таким чином можна говорити що підключення для стаціонарних ПК матиме швидкість в 50 Мбіт/с.

У випадку IP-телефонії (VoIP) обсяг трафіка залежить від активності абонентів та розподілу викликів за напрямками. Як показує досвід, то для гостей готелю інтенсивність викликів в годину найбільшого навантаження становить 1, а тривалість виклику не перевищує 30 с., для персоналу ці значення дорівнюють 5 та 120 с. відповідно. Також важливим є тип голосового кодека та технологія за якою побудована мережа. Для проведення розрахунків будемо використовувати кодек без стиснення – G.711. Пропускна здатність для одного мовного каналу з урахуванням службової інформації що міститься у заголовках кадрів не перевищує 100 Кбіт/с. Коефіцієнт одночасного використання для цієї послуги доцільно застосовувати тільки для постояльців

готелю, і він дорівнюватиме 0,3.

Так само як і у випадку з VoIP, для послуги IPTV та VoD розрахунковий трафік залежить від якості зображення (розподільної здатності) та інтенсивності користування послугою. Щодо якості, то на сьогоднішній день використовують три основних варіанти розподільної здатності які відрізняються за питомою пропускною здатністю:

- SD (стандартна роздільна здатність) – 1,5-3 Мбіт/с на канал;
- HD (висока роздільна здатність) – 5-10 Мбіт/с на канал;
- UHD (ультра висока роздільна здатність) – 15-30 Мбіт/с на канал.

Стандартом дефакто в готельному бізнесі на сьогоднішній день є HD-якість відео за запитом та IPTV, то ж в подальших розрахунках використаємо значення в 10 Мбіт/с на один канал. Пропускна здатність локального сегменту мережі не залежить від кількості каналів, а залежить від кількості пристроїв, які встановлені в готелі, тож на кількість каналів та розмір архіву VoD ми не зважаємо. Коефіцієнт одночасного використання для цієї послуги дорівнюватиме 0,5, так як не всі номери одночасно переглядають відео, бо це в першу чергу залежить від віку постояльців та наявності в них відповідних гаджетів.

Послуга відеоспостереження дечім нагадує послуги IPTV, але через трохи нижчу розподільну здатність та більш ефективні кодеки, трафік, що генерується однією камерою становить 4 Мбіт/с. При розрахунку будемо враховувати найбільш важкий з точки зору використання сценарій – постійний запис з коефіцієнтом одночасного використання 1, хоча зазвичай в системах відеоспостереження використовується підхід з записом по події – спрацюванням по тривозі чи по руху.

Системи IoT керування номерами та будівлею (BMS), система гучного оповіщення, пожежна сигналізація, системи контроля доступу зазвичай генерують відносно невеликий обсяг трафіку (невеликі пакети даних, невеликий бітрейт), але велика кількість пристроїв може створювати значну кількість сесій. Для такого типу трафіку важливіше забезпечити низьку

затримку та надійність ніж високу швидкість, або ж використовувати технології traffic shaping і забезпечити окрему гарантовано полосу пропускання в загальному каналі. Доречно для даної послуги виділити смугу пропускання 2 Мбіт/с для кожного окремого контролера з гарантованими параметрами QoS.

В табл. 1.5 зведені ключові характеристики послуг, які будуть використовуватись для подальших розрахунків.

Таблиця 1.5 – Параметри послуг, що надаються мережею

Послуга	Бітрейт, Мбіт/с	Коефіцієнт одночасного використання
Інтернет WiFi серфінг	1	0,4
Інтернет WiFi соціальні мережі	2	0,6
Інтернет WiFi відео HD	5	0,2
Інтернет WiFi UHD-стрімінг	20	0,05
Інтернет WiFi відеоконференції	3	0,1
Інтернет WiFi онлайн-ігри	2	0,3
Інтернет + стаціонарний Ehernet	50	0,5
IP-телефонія постояльці	0,1	0,05
IP-телефонія адміністрація та персонал	0,1	0,2
IPTV та VoD	10	0,5
Відеоспостереження	4	1
IoT керування номерами та будівлею (BMS), система гучного оповіщення, пожежна сигналізація, системи контроля доступу	2	1

У відповідності до даних, викладених в табл. 1.3-1.5 проведемо оцінку трафіку в мережі готелю скориставшись формулою 1.1 з урахуванням коефіцієнту заповнюваності готелю на рівні 80% (для персоналу 100%). Результати розрахунку за категоріями трафіку наведено у табл. 1.6.

Таблиця 1.6 – Результати розрахунку трафіку на мережу

Послуга	Розрахункове значення трафіку, Мбіт/с
Інтернет WiFi серфінг	133,12
Інтернет WiFi соціальні мережі	199,68
Інтернет WiFi відео HD	166,4
Інтернет WiFi UHD-стрімінг	166,4
Інтернет WiFi відеоконференції	49,92
Інтернет WiFi онлайн-ігри	99,84
Інтернет + стаціонарний Ehernet	240
IP-телефонія постояльці	0,252
IP-телефонія адміністрація та персонал	0,08
IPTV та VoD	252
Відеоспостереження	51,2
IoT керування номерами та будівлею (BMS), система гучного оповіщення, пожежна сигналізація, системи контроля доступу	110,4

Загальне навантаження на мережу становить 1469,292 Мбіт/с.

Отримане значення навантаження на мережу є орієнтовним і базується як на особистих судженнях так і на статистичних даних, що отримані на підставі аналізу літературних джерел. Враховуючи цей фактор, важливим є застосування ще однієї ймовірнісної величини, а саме так званого коефіцієнту запасу, який дозволить врахувати вибухоподібну природу мережного трафіку, яка зумовлена фрактальністю деяких процесів. Його значення береться в межах 20%, і застосовується у випадку прогнозування навантаження саме на сегмент Інтернету, для інших типів навантаження зазвичай ця величина не застосовується через порівняно великий запас за пропускною здатністю на

фізичному рівні. Це треба враховувати в подальшому при оцінці необхідної пропускної здатності зовнішнього каналу Інтернет.

Висновки до розділу 1

В якості об'єкта проектування в кваліфікаційній роботі бакалавра виступає готельний комплекс «Franziskanerinner von Route», предметом є телекомунікаційна інфраструктура.

Актуальність проведення розробки нової мережі продиктована тим, що зараз готельний комплекс перебуває на етапі реконструкції, і відповідно потребує переосмислення і абсолютно нових мережних та архітектурних рішень. Мережа що проєктується повинна бути конвергентною та відповідати галузевим стандартам Hospitality Technology Next Generation (HTNG), що відповідає потребам готельної сфери. Телекомунікаційна інфраструктура буде забезпечувати можливість високошвидкісного доступу до Інтернет, голосового IP-зв’язку, ITPV&VoD, впровадження технологій СКУД та IoT для покращення процесу управління готелем.

Проаналізувавши об’єкт проєктування з метою визначення кількості кінцевих пристроїв, було визначено що загальна кількість осіб, що можуть одночасно перебувати на території готельного комплексу становить 213 осіб, а кількість активних підключень до мереж може становити до 794 (сюди входять як смартфони та Smart TV, так і IP-камер та IoT-контролери). Використання адаптивної методики розрахунку трафіку показало що загальне навантаження на мережу складе приблизно 1469,292 Мбіт/с. В подальшому, визначившись з структурою та ієрархією мережі варто провести розрахунки за окремими напрямками – зовнішній та внутрішній, з урахуванням топологічного рішення в середині будівлі та за її межами.

2 РОЗРОБКА АРХІТЕКТУРИ МЕРЕЖІ

2.1 Концепція побудови мережі

Мережа що проєктується для готельного комплексу має бути уніфікованою, і надавати різні послуги за характеристиками зважаючи на їх номенклатуру. Такі мережі мають назву конвергентних.

Конвергентна мережа – мережна інфраструктура, що здатна передавати різні типи трафіку (голос, відео, дані) через єдине спільне середовище з використанням одного набору протоколів та технологій. Це повна протилежність традиційним «ізольованим» або «паралельним» мережам, де кожен тип послуг використовує власну, незалежну інфраструктуру [6]:

- окремі телефонні лінії з власною кабельною інфраструктурою;
- окрема коаксіальна мережа для кабельного телебачення;
- окрема мережа Ethernet для доступу до Інтернет;
- окремі мережі для підсистем безпеки, автоматизації тощо.

Такий підхід на сьогодні є невиправдано дорогим у впровадженні, складним в управлінні та обслуговуванні, а також неефективним у використанні ресурсів. З розвитком IP-технологій та зростанням вимог до пропускної здатності, конвергенція набуло широкого проникнення.

Сьогодні конвергентні мережі характеризуються:

- використанням IP-протоколу, що дозволяє використовувати стандартне мережеве обладнання для всіх послуг;
- наявністю єдиної фізичної інфраструктури (дротова або бездротова), яка побудована у відповідності до регламентів структурованих кабельних систем (СКС) для підтримки передачі IP-трафіку;
- можливістю застосування політик QoS для визначення пріоритетів обробки критичного трафіку, гарантуючи його якість навіть під час

пікових навантажень;

- розподілом мережі на незалежні сегменти з використанням технологій віртуальних локальних мереж VLAN в рамках єдиної фізичної інфраструктури.

Основною перевагою побудови саме конвергентних мереж є можливість застосування централізованого управління з можливістю здійснювати моніторинг, налаштування та діагностику всіх інтегрованих служб з єдиної платформи управління (NMS – система управління мережею), що спрощує обслуговування. Окрім цього варто відзначити, що за допомогою саме конвергентних мереж готелям вдається:

- зменшити капітальні витрати (CAPEX);
- зменшити експлуатаційні витрати (OPEX);
- пришвидшити розгортання та розширення з можливістю масштабування;
- покращити рівень безпеки, надійності та відмовостійкості.

Конвергентні мережі повинні відповідати трирівневій ієрархічній архітектурі: ядро, розподіл, доступ.

Рівень ядра (Core Layer) цей найвищий рівень, і він відповідає за загальну безпеку мережі, керування, моніторинг та аналіз трафіку. Може бути реалізований на базі одного або двох маршрутизаторів, залежно від обраної концепції організації демілітаризованої зони (DMZ).

Рівень розподілу (Distribution Layer) призначений для перерозподілу трафіку за відповідними напрямками і логічної ізоляції потоків різних додатків. Ключовим архітектурним компонентом є комутатор другого або третього рівня моделі OSI.

Рівень доступу (Access Layer) це найнижчий рівень мережної ієрархії, який призначений для надання прямого доступу до мережі кінцевим користувачам та спеціальному мережевому термінальному обладнанню.

2.2 Розробка архітектури IP-мережі

IP-мережа об'єкта являє собою традиційну локальну комп'ютерну систему з розширеними можливостями, призначену для забезпечення користувачів доступом до Інтернету та локальних мережевих ресурсів, а також для реалізації функцій контролю доступу з елементами IoT та організації систем відеоспостереження.

Як зазначалося раніше, архітектура проектованої мережі відповідатиме трирівневій ієрархічній моделі (ядро, розподіл, доступ). Вибір мережевих технологій взаємодії є важливим етапом у процесі проектування мереж будь-якого рівня складності.

Традиційно основну роль у локальних мережах відіграють протоколи канального рівня. Для стабільної роботи їх мережева структура повинна бути чітко визначена. Наприклад, популярний протокол канального рівня Ethernet спочатку був розроблений для паралельного підключення всіх вузлів до єдиного середовища передачі. Однак в останні роки спостерігається тенденція до поступової відмови від використання спільних середовищ передачі даних на користь активного використання комутаторів. У такій схемі кожен кінцевий вузол підключається до станції через окрему лінію зв'язку. Для забезпечення надійної взаємодії мережевих пристроїв, оптимальної якості обслуговування та економічного обґрунтування вибору обладнання проект передбачає використання технологій Ethernet, включаючи Fast Ethernet та Gigabit Ethernet. Ці стандарти забезпечують відповідну швидкість передачі даних (10 Мбіт/с, 100 Мбіт/с або 1000 Мбіт/с) та підтримку різних типів середовищ передачі.

Для високошвидкісних каналів зв'язку рівня розподілу буде застосовано Gigabit Ethernet. Цей вибір обґрунтований оптимальністю для агрегації трафіку у зовнішній канал та перерозподілу даних на рівні ядра мережі. Основна концепція Gigabit Ethernet полягає у збереженні фундаментальних принципів класичної технології Ethernet при досягненні бітової швидкості 1000 Мбіт/с.

Фізичний рівень Gigabit Ethernet є складнішим і більш технологічним, що дозволяє використовувати різноманітні кабельні системи: багатомодовий волоконно-оптичний кабель та кручену пару категорії 5e, 6 або 7. Застосовність даної технології для мережі готельного комплексу визначається наступними факторами:

- максимальна довжина сегмента до 2 км для багатомодового волоконно-оптичного кабелю та 100 м для крученої пари;
- базова швидкість до 1000 Мбіт/с є достатньою для надання заявлених послуг зв'язку;
- механізми надійної доставки, навіть не зважаючи на те, що у Gigabit Ethernet не має вбудованого механізму надійної доставки інформації на канальному рівні, у випадку, коли пропускна здатність мережі значно перевищує максимальне розрахункове навантаження, наявний запас пропускної здатності забезпечить достатню надійність надання послуг.

Таким чином, для рівня розподілу та ядра мережі буде в подальшому використана технології Gigabit Ethernet як є найбільш оптимальної з точки зору вимог до якості обслуговування та співвідношення швидкісно-економічних показників. На рівні доступу необхідно використовувати технологію Fast Ethernet, що дозволить ефективно здійснювати агрегацію трафіку на рівні розподілу без створення вузьких місць

Крім того, проект передбачає використання нерозповсюджуваного сегмента, а саме для підключення термінальних пристроїв гостей та персоналу готелю. Стандарти Wi-Fi, розроблені Інститутом інженерів з електротехніки та електроніки (IEEE) у рамках серії 802.11, постійно вдосконалюються, пропонуючи вищі швидкості, кращу ефективність та нові можливості. Для спрощення ідентифікації Wi-Fi Alliance ввів зрозуміліші позначення, починаючи з Wi-Fi 4 [9]. В табл. 2.1 проведемо розширене порівняння сімейства стандартів [10].

Таблиця 2.1 – Розширене порівняння сімейства стандартів WiFi

Характеристика	802.11b (Wi-Fi 1)	802.11a (Wi-Fi 2)	802.11g (Wi-Fi 3)	802.11n (Wi-Fi 4)	802.11ac (Wi-Fi 5)	802.11ax (Wi-Fi 6/6E)	802.11be (Wi-Fi 7)
Частоти	2.4 ГГц	5 ГГц	2.4 ГГц	2.4 ГГц, 5 ГГц	5 ГГц	2.4 ГГц, 5 ГГц, 6 ГГц (6E)	2.4 ГГц, 5 ГГц, 6 ГГц
Теоретична швидкість (макс. на пристрій)	11 Мбіт/с	54 Мбіт/с	54 Мбіт/с	До 600 Мбіт/с	До 3.5 Гбіт/с (залежить від конфігурації)	До 9.6 Гбіт/с	До 46 Гбіт/с
Ширина каналу	20 МГц	20 МГц	20 МГц	20, 40 МГц	20, 40, 80, 80+80, 160 МГц	20, 40, 80, 80+80, 160 МГц	20, 40, 80, 80+80, 160, 320 МГц
Модуляція	DBPSK, DQPSK, CCK	OFDM	OFDM	OFDM	256-QAM	1024-QAM	4096-QAM
MIMO	Немає	Немає	Немає	До 4x4 (SU-MIMO)	До 8x8 (DL MU-MIMO Wave 2)	До 8x8 (UL/DL MU-MIMO)	До 16x16 (UL/DL MU-MIMO)
Переваги	Дуже дешевий, поширений	Висока швидкість (для свого часу)	Зворотна сумісність з 802.11b, краща швидкість	Значний приріст швидкості, використання 2.4/5 ГГц, MIMO	Гігабітні швидкості, MU-MIMO, фокус на 5 ГГц	Підвищена ефективність у завантажених мережах, OFDMA, TWT, підтримка 2.4/5/6 ГГц	Дуже високі швидкості, MLO, 320 МГц канали, 4K-QAM, покращена робота в щільних середовищах
Недоліки	Дуже повільний, схильний до перешкод	Короткий радіус дії, не проникає крізь стіни	Короткий радіус дії, схильний до перешкод (2.4 ГГц)	Середні швидкості в завантажених 2.4 ГГц, обмежений MU-MIMO	Тільки 5 ГГц (для високих швидкостей), обмежений MU-MIMO	Вимагає сумісного обладнання, дорожче, 6 ГГц може бути недоступний у деяких регіонах	Ще дорожче, вимагає нового обладнання, стандарт ще фіналізується, 6 ГГц може бути недоступний

Для сучасного готельного комплексу, з огляду на високі вимоги до пропускної здатності, стабільності, безпеки та великої кількості одночасних підключень, доцільно орієнтуватися на такі стандарти:

- Wi-Fi 6 (802.11ax) – цей стандарт забезпечує надійність і ефективність роботи, суттєво підвищуючи продуктивність у середовищах із високим навантаженням завдяки технологіям OFDMA та MU-MIMO. Він підтримує частоти 2.4 ГГц і 5 ГГц, що дозволяє досягти балансу між широтою покриття та швидкістю передачі даних;
- Wi-Fi 6E (802.11ax) – цей стандарт є оптимальним вибором, додаючи чистий 6 ГГц діапазон. Це покращує швидкість, знижує

затримки та стає чудовим варіантом для VIP-гостей або застосувань із високими вимогами до продуктивності.

– Wi-Fi 7 (802.11be) – відкриває можливості для надзвичайно високої швидкості та ефективності. Це чудовий вибір для готелів, які прагнуть бути лідерами у впровадженні новітніх технологій і готові інвестувати в перспективу, особливо для підтримки сучасних мультимедійних сервісів та IoT-рішень.

Виходячи з перспективи довгострокового використання мережі, доцільно використовувати стандарт Wi-Fi 6 (802.11ax).

З огляду на різноманіття абонентських груп та наявну фізичну інфраструктуру, мережа що проєктується потребує ефективного логічного структурування. Для досягнення цієї мети планується використовувати низку мережевих технологій, а саме: технології взаємодії пристроїв на канальному рівні, віртуальні приватні мережі (VPN), віртуальні локальні мережі (VLAN), службу динамічного налаштування хостів (DHCP) та протокол всеохоплюючого дерева (STP).

Основою логічного структурування є технологія VLAN. Її інтеграція в мережеві комутатори дозволяє вирішити два фундаментальні завдання:

– підвищення продуктивності;
– ізоляція та безпека трафіку.

Передача кадрів гарантується виключно до вузла призначення в межах кожної віртуальної мережі, що оптимізує використання пропускної здатності, також досягається ефективна ізоляція окремих сегментів мережі, що посилює контроль доступу для користувачів та забезпечує захист від широкомовних штормів та компрометуючих дій зловмисників.

Для забезпечення взаємодії різних віртуальних мереж у рамках загальної мережі необхідно використання єдиної бази віртуальних підмереж для всього мережного сегменту. Це може бути реалізовано або апаратно (за допомогою окремого маршрутизатора), або програмно (вбудовані функції комутатора). Існує кілька методів організації VLAN, зокерма це групування портів з

використанням MAC-адрес, або ж застосування тегів у кадрах (власні протоколи та стандарти IEEE 802.1q) та залучення функціональності мережевого рівня. Під час створення VLAN на основі одного комутатора групування портів є найбільш доцільним. Такий підхід мінімізує обсяг ручної роботи, оскільки адміністратору потрібно лише пов'язати кожен порт із заздалегідь визначеними віртуальними мережами, але з огляду на те, що в мережна інфраструктура буде побудована на великій кількості комутаторів та безпроподових точок доступу, такий підхід є недоцільним, і буде застосована технологія IEEE 802.1q з додаванням відповідних тегів до кадрів [11].

Для забезпечення функціонування всіх мережних служб для кінцевих термінальних пристроїв необхідно розподілити адресний простір та призначити IP-адреси. Призначення IP-адрес у мережі може виконуватися двома шляхами, статично або динамічно.

Статичне призначення IP-адрес передбачає ручне та постійне призначення унікальних IP-адрес кожній робочій станції або термінальному пристрою користувача. Цей метод ефективний для мереж зі стабільною та передбачуваною кількістю вузлів. Однак для готельних комплексів, які характеризуються високою динамікою підключення та відключення користувацьких пристроїв, статичне призначення є недоцільним. У готелі призначення статичних адрес виправдане лише для адміністративної та керуючої мережі, активного мережевого обладнання та спеціалізованої комп'ютерної мережі (це може бути підсистема адміністративних робочих станцій, відеоспостереження, IoT підсистеми керування готелем та номерами, підсистема контролю доступу).

Динамічне призначення IP-адрес відбувається автоматично за допомогою служби DHCP (Dynamic Host Configuration Protocol), коли пристрої підключаються до мережі. IP-адреси можуть призначатися як постійно, так і тимчасово – з певним терміном оренди та можливістю пов’язати їх з унікальною MAC-адресою. Враховуючи специфічні характеристики готельного комплексу та відсутність потреби в довгострокових асоціаціях адрес для

більшості пристроїв гостей, динамічне призначення є оптимальним рішенням для більшої частини мережі [12].

Для надійного функціонування мережі необхідно передбачити резервування, зокрема це може бути як резервування активного обладнання так і створення кільцевих фізичних топологій. Використовувати схему резервування 1+1 з гарячою заміною для активного мережного обладнання (по суті дублювання обладнання на комутаційних вузлах) не є доцільним через те що його легше замінити за потреби, а ось резервування на рівні фізичних з'єднаннь кабельної інфраструктури виглядає більш логічним. Тож доцільно застосовувати кільцеві з'єднання, але як відомо протокол Ethernet з комутаторами другого або третього рівня не дозволяє роботи такі підключення. Вирішенням цієї задачі є протокол Spanning Tree Protocol (STP). STP був спеціально розроблений для підтримки кільцевих та інших резервних з'єднань у мережах Ethernet та запобігання петель. Алгоритм Spanning Tree дозволяє мережевим комутаторам автоматично створювати оптимальну деревоподібну конфігурацію з'єднань. Це має вирішальне значення, оскільки для нормальної роботи комутатора необхідно уникати замкнутих маршрутів. Вони можуть бути створені як навмисно (для резервування), так і ненавмисно через складність мережевих з'єднань. Комутатори, що підтримують STP, автоматично формують активну структуру дерева з'єднань. Це забезпечує безперебійну конфігурацію без петель, водночас дозволяючи резервні шляхи у разі виходу з ладу основного шляху [13].

2.3 Технології надання базових послуг

Для забезпечення голосового зв'язку з можливістю інтеграції системи гучного оповіщення необхідно обрати технологію побудови даного сегменту мережі з можливістю надання відповідного функціоналу. Мережа повинна забезпечувати не лише якісний зв'язок, але й широкі можливості для клієнтів,

відповідаючи високим стандартам обслуговування. Основний перелік функцій включає:

- автоматичне пробудження з функцією «Будильник» на заданий час;
- управління зовнішнім зв’язком з можливість відкриття чи обмеження дзвінків на зовнішні лінії;
- контроль дзвінків на спеціальні номери з регулювання доступу до міжміських, мобільних і безкоштовних номерів;
- захист внутрішніх номерів з функцією обмеження доступу до внутрішньої мережі, за винятком рецепції;
- підтримка конференц-зв’язку для організації дзвінків за участю внутрішніх та зовнішніх абонентів;
- реалізація функцій, характерних для готельного бізнесу;

Тип підключення мережі голосового зв’язку до зовнішнього сегменту залежить від постачальника телефонного зв’язку, але комутаційна система повинна бути універсальною і підтримувати варіанти аналогових, цифрових (ISDN BRI, PRI, E1) і IP-з’єднань через Ethernet.

Адміністрування може здійснюватися як локально, так і дистанційно. Деякі функції повинні бути доступними для самостійного використання з боку гостей або персоналу готелю, що підвищить зручність керування системою. Для забезпечення надійності необхідно дублювати дані викликів на центральному комп’ютері оператора станції.

Найдоцільнішим рішенням для забезпечення всього згаданого функціоналу є впровадження IP-МініАТС, які існують у вигляді програмного чи апаратного забезпечення.

Програмні IP-АТС з відкритим кодом є економічно вигідними, але потребують високого рівня технічної компетенції для обслуговування, через ризик збоїв у роботі програм або серверів. Це може вплинути на стабільність системи загалом.

Натомість апаратні IP-АТС від провідних брендів (Nortel, Panasonic, Cisco, LG, Siemens) пропонують високу надійність і широкий функціонал. Такі

системи забезпечують стабільність роботи навіть при високих навантаженнях [14].

При виборі обладнання важливо визначитися з основним протоколом IP-телефонії. Найпоширенішими є H.323 та SIP (Session Initiation Protocol).

Протокол SIP був розроблений пізніше за H.323 і враховує його недоліки, завдяки чому вважається більш оптимальним для сучасних IP-мереж. H.323 використовує двійковий формат повідомлень, що вимагає суворої стандартизації можливостей пристроїв для забезпечення сумісності. На відміну від нього, SIP оперує текстовим форматом повідомлень, що забезпечує вищу гнучкість: пристрій просто ігнорує повідомлення, які він не розуміє. Крім того, SIP-протокол є простішим у реалізації та функціонує за аналогією з HTTP-протоколом, що значно спрощує роботу з ним порівняно з H.323. Таким чином, для проектованої мережі IP-телефонії протокол SIP є рекомендованим вибором [15]. Розглянемо роботу даного протоколу більш детальніше.

На рис. 2.1 наведена типова архітектурна реалізації послуги IP-телефонії у відповідності до протоколу SIP.

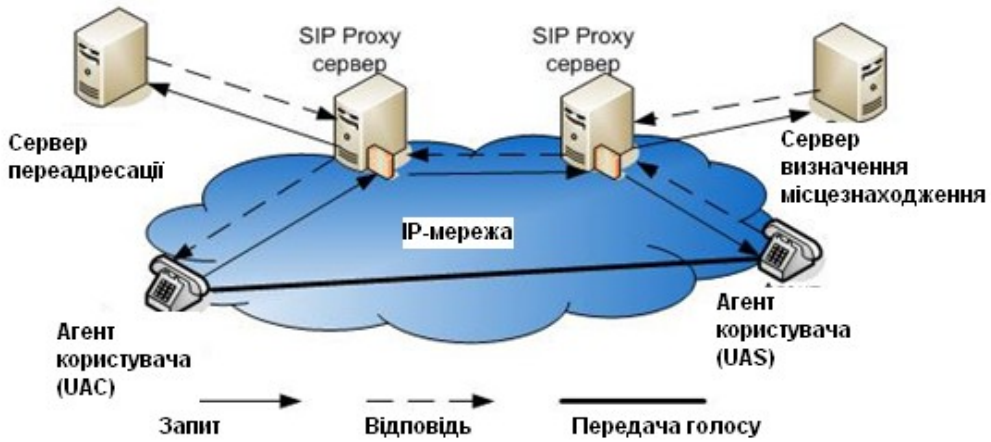

Рисунок 2.1 – Архітектура надання послуги IP-телефонії за протоколом SIP

SIP працює за клієнт-серверною моделлю, яка складається з кількох основних компонентів:

- SIP-клієнти (User Agents) – кінцеві пристрої чи програми, що ініціюють або приймають SIP-сесії (програмні телефони (Softphones), застосунки для комп'ютерів чи мобільних пристроїв, або ж апаратні IP-телефони, спеціалізовані пристрої на базі Ethernet.
- шлюзи (Gateways) – пристрої, які перетворюють SIP-сигнали у формати, підтримувані традиційними телефонними мережами (PSTN);
- SIP-сервери – забезпечують маршрутизацію, обробку та керування запитами. Виділяють такі типи серверів (Проксі-сервер (Proxy Server) який виконує функцію посередника між клієнтами, обробляючи маршрутизацію та автентифікацію; реєстратор (Registrar Server) який приймає запити на реєстрацію, зберігаючи актуальну інформацію про розташування клієнтів; сервер переадресації (Redirect Server) що надає клієнтам адресу іншого сервера для відновлення маршруту; сервер місцезнаходження (Location Server) що може бути вбудований у реєстратор чи проксі-сервер, відповідає за інформацію про поточне місцезнаходження користувачів.

Алгоритм реалізації сеансу зв'язку наведено нижче:

1. Реєстрація. Після підключення до мережі SIP-клієнт надсилає запит REGISTER на реєстратор, де зберігається його IP-адреса та прив'язується до SIP URI (вигляду user@domain.com).
2. Ініціація дзвінка. Користувач А (той, хто телефонує) вводить SIP URI користувача В. Запит INVITE формується SIP-клієнтом і надсилається на проксі-сервер для подальшої обробки. У запиті передаються медіа-параметри через SDP (Session Description Protocol).
3. Пошук і маршрутизація. Проксі-сервер шукає отримувача через сервер місцезнаходження, дізнаючись актуальну IP-адресу

користувача B. Потім запит перенаправляється до отримувача.

4. Встановлення дзвінка. Відповідь на запит INVITE може мати різний статус: 100 Trying: Заявка отримана; 180 Ringing: Телефон абонента дзвонить; 200 OK: Дзвінок прийнято. Після завершення обміну інформацією клієнти готові до передачі голосових або мультимедіа даних.
5. Передача медіа. Голос/відео передаються безпосередньо між клієнтами через RTP-протокол.
6. Завершення дзвінка. Запит BYE сигналізує про завершення сесії а інший SIP-клієнт відповідає 200 OK, підтверджуючи завершення сесії, і таким чином з’єднання розривається.

На відміну від протоколу H.323, SIP використовує текстовий формат, схожий на HTTP. Це забезпечує більшу гнучкість і спрощує процес розробки та налагодження. Адміністратор легко розуміє структуру цих повідомлень, а пристрої, що не розпізнають певний заголовок, просто його ігнорують, забезпечуючи кращу сумісність. SIP інтегрується з іншими протоколами і може бути адаптований для підтримки нових функцій, що робить його перспективним для різноманітних застосувань. Попри наявність серверів сигналізації, виклики можуть встановлюватися безпосередньо між клієнтами після завершення первинного узгодження. Це зменшує навантаження на сервер, роблячи мережу більш ефективною. SIP оперує уніфікованими ідентифікаторами ресурсів для звернення до користувачів не лише за номером телефону, але й за SIP-адресою. Протокол підтримує передачу сигнальних даних як через UDP, так і через TCP, що дає змогу вибирати оптимальний транспорт залежно від задач і не вводить додаткових обмежень, а також дана особливість да змогу значно покращити якість та надійність з’єднаннь з гарантуванням доставки [16].

SIP забезпечує надійну платформу для реалізації голосового і відеозв'язку у сучасних мережах, включаючи корпоративні інфраструктури і готелі.

Невід’ємною частиною загальної системи безпеки і запорукою

комфортного перебування є наявність системи відеоспостереження в загальнодоступних зонах і приміщеннях готелях. Така система здатна вивести безпеку на належний рівень і прицьому зберегти необхідний ступінь приватності.

Згідно з викладеними у першій главі даними, для об'єкта проектування було обрано мережеві пристрої – IP-камери – як основне обладнання для захоплення зображення. Для повноцінної роботи такої системи необхідно забезпечити передачу отриманих даних від камер через телекомунікаційну мережу до місця зберігання відеорахівів. Централізоване зберігання, аналіз, обробка та управління системою здійснюється за допомогою цифрових відеореєстраторів (DVR), які можуть бути реалізовані як у програмному, так і в апаратному варіанті [17]. На рис. 2.2 наведена типова схема реалізації системи відеоспостереження.

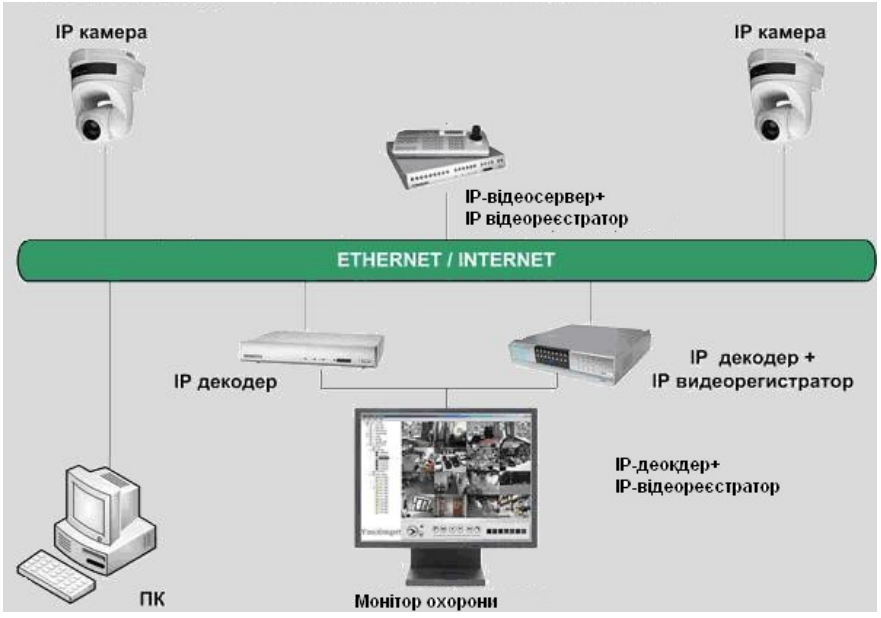

Рисунок 2.2 – Типова схема організації IP-відеоспостереження

Програмні DVR зазвичай працюють на платформі персональних комп'ютерів або серверного обладнання. До їх переваг відноситься:

– просте налаштування та зручний інтерфейс інтуїтивно зрозумілий "human-friendly" інтерфейс, що спрощує як початкову

конфігурацію, так і подальше управління;

- масштабованість клієнтських підключень через підтримку значної кількості віддалених клієнтів, обмеження яких залежать переважно від операційної системи та мережевої інфраструктури.

Незважаючи на вказані переваги є і ряд недоліків:

- невисокий рівень надійності через застосування стандартних ПК як відеосервера знижує стабільність роботи порівняно з апаратними рішеннями;
- вразливість до зовнішнього втручання, бо саме такі системи більш схильні до кібератак та несанкціонованого доступу через використання стандартних операційних систем та програмного забезпечення;
- залежність продуктивності і швидкодії системи від апаратного забезпечення, а також зниження рівня надійності через використання стандартних компонентів;
- складність у роботі з архівами через складну ієрархію файлової системи і нестандартні розміри даних.

Апаратні DVR на відміну від програмних, представляють собою спеціалізовані пристрої, створені виключно для завдань відеоспостереження. До їх переваг можна віднести:

- високу надійність завдяки використанню оптимізованих операційних систем та спеціалізованих компонентів які забезпечують стабільну роботу без збоїв;
- захищеність від зловмисного впливу через використання пропрієтарних програмних рішень і продуктів;
- висока продуктивність через оптимізацію для відеопотоків, що гарантує швидкий запис і перегляд даних;
- компактні розміри;
- простота інтеграції на рівні пристроїв plug-in-play;
- енергоефективність та низький рівень шуму через спеціально

сконструйовані архітектурні рішення;

– можливість підключення з використанням технології.

Але якщо порівнювати з програмними рішеннями, то апаратні DVR звісно мають і деякі недоліки:

– складність налаштування первинної конфігурації;
– обмеження дискового простору бо апаратно система може бути розрахована на певну кількість портів для підключення дисків, хоча це обмеження не є дуже суттєвим через зростання обсягів дисків і використання новітніх технологій та кодеків з оптимізації відео;
– вартість системи більша ніж використання програмних рішенньь;
– необхідність побудови додаткових систем захисту та авторизації для підключення як з локального сегменту мережі так і з глобального для проведення налаштувань чи перегляду архівів.

Попри окремі недоліки, апаратні відеореєстратори демонструють значну перевагу над програмними рішеннями і навіть над рішеннями що використовують хмарні технології. Враховуючи сукупність їхніх характеристик, функціональних можливостей та високий рівень надійності забезпечення високих стандартів безпеки та підвищення ефективності системи відеоспостереження у готельному комплексі доцільно віддавати перевагу саме апаратним відеореєстраторам. Підключення IP-камер до відеосерверів буде реалізовано через локальну IP-мережу, що буде функціонувати в межах готельного комплексу.

Організація системи IPTV та VoD для готельного комплексу може бути реалізована через два основних підходи.

Перший підхід передбачає створення власного програмно-апаратного комплексу, що включає розгортання головної станції. Така станція має забезпечувати прийом, обробку, кодування та розподіл контенту у межах внутрішньої мережі готелю.

Другий підхід полягає у використанні послуг стороннього провайдера. У цьому випадку готова послуга IPTV та VoD надається спеціалізованими

постачальниками і транслюється через існуючу інфраструктуру готелю.

Зважаючи на загальну кількість телевізійних приймачів у готелі, яка становить 63 одиниці, і відповідно створення та підтримка власної серверної платформи для IPTV та VoD є економічно недоцільним рішенням. Витрати на придбання, налаштування та подальше обслуговування такого комплексу перевищують потенційні вигоди від використання стороннього провайдера.

У зв'язку з цим оптимальним рішенням для забезпечення функціонування IPTV та VoD в готельних номерах є залучення послуг стороннього провайдера. Це дозволяє мінімізувати капітальні витрати та уникнути складності технічного обслуговування. Для інтеграції такої послуги необхідно облаштувати кожен телевізійний приймач спеціалізованим пристроєм – приставкою Set-Top Box (STB). Цей компонент виконує декодування IP-сигналу та його конверсію у формат, що відповідає вимогам телевізійного приймача.

Сучасні готелі прагнуть впроваджувати рішення, які забезпечують комплексне підвищення безпеки, автоматизацію процесів і підвищення комфорту для гостей. Сьогодні розроблено багато технологій, адаптованих як для готельного бізнесу, так і для приватного використання. Особливої уваги заслуговують системи контролю й управління доступом (СКУД), інтегровані пожежні сигналізації та інновації, які пропонує Інтернет речей (IoT).

СКУД для готелів представляє собою потужний інструмент, що поєднує апаратне та програмне забезпечення. Завдяки цим системам автоматизуються рутинні процеси, водночас підвищуючи рівень сервісу й безпеки. Основні функції СКУД спрямовані на:

- автоматизацію доступу з надання гостям можливості входу до номера за допомогою ідентифікатора (наприклад, картки) у межах оплаченого періоду проживання;
- автоматичну виписку та блокування доступу до номера після завершення строку проживання, усуваючи можливість входу за старим ідентифікатором;
- моніторинг присутності осіб у номері;

- охоронну функцію з активацію охорони номера при виході відвідувачів із сигналізацією у разі несанкціонованого доступу;
- примусове налаштування охорони з дистанційною постановкою за запитом служби безпеки;
- контроль персоналу і моніторинг ефективності роботи обслуговуючого персоналу та виявлення випадків несанкціонованого проникнення;
- генерацію звітів.

СКУД інтегрує різні програмно-апаратні засоби й дозволяє впроваджувати такі додаткові функції:

1. Автоматичне вмикання світла в коридорі під час входу до номера.
2. Повне відключення живлення в номері (окрім важливих систем) при виході всіх гостей.
3. Контроль використання мінібару персоналом за відсутності гостей.
4. Контроль доступу до технічних приміщень у номері.
5. Реєстрацію всіх подій (наприклад, спрацьовування датчиків, читання ідентифікаторів, перехід контролера на резервне живлення) у базі даних із фіксацією дати, часу й коду ідентифікатора.
6. Складання звітів на основі подій, часу чи інших параметрів.
7. Передачу даних до стандартних готельних систем (PMS – Property Management System) для автоматизації обліку послуг і виставлення рахунків.

Програмне забезпечення СКУД передбачає інтеграцію зі стандартними програмними платформами для автоматизованої передачі інформації про час перебування гостей і використані послуги. Це забезпечує точний розрахунок і спрощує загальні операції. СКУД являє собою інтегроване мережне рішення в загальну телекомунікаційну інфраструктуру з власними осередками мережних сегментів для підключення відповідної підсистеми датчиків до контролерів, що встановлені в кожному окрему готельному номері чи периметрі охоронної зони..

Системи пожежної сигналізації інтегрована з центральною мережею готелю та СКУД для забезпечення швидкого реагування в екстрених ситуаціях. Гучне оповіщення реалізовано через термінальні пристрої IP-телефонії, що встановлену в номерах та просторах загального користування. Основні функції системи пожежної сигналізації включають:

- раннє виявлення пожежі, що досягається завдяки роботі димових, теплових і комбінованих сповіщувачів, встановлених у номерах, коридорах, технічних приміщеннях і громадських зонах;
- автоматичне сповіщення про небезпеку через світлові й звукові сигнали, а також передача інформації на центральний моніторинговий пульт і при необхідності повідомлення відповідних служб;
- інтеграція з іншими системами об'єкта для виконання таких завдань як розблокування електронних замків для забезпечення вільної евакуації під час тривоги; автоматичне перемикання ліфтів у режим «пожежна безпека» із примусовим опусканням на перший поверх; активація систем димовидалення та підпору повітря; вимкнення систем вентиляції з метою запобігання поширенню диму.

Більшість цих функцій та компонентів СКУД, пожежної та охоронної сигналізації інтегрується завдяки системі Інтернету речей (IoT). Цей підхід дозволяє підключати різноманітні пристрої й датчики до мережі для збору даних, моніторингу та дистанційного керування. У контексті готельного бізнесу IoT у поєднанні з СКУД та іншими системами виконує такі функції:

- автоматизоване освітлення;
- клімат-контроль;
- контроль інженерних комунікацій;
- персоналізований сервіс.

Для виконання цих функцій навколо контролерів IoT будується окрема мережна підсистема як використанням слабострумових мереж так і безпроводових рішень.

СКУД у поєднанні з пожежною сигналізацією та IoT створює ефективну цифрову екосистему для VIP-готелів. Це рішення підвищує рівень безпеки та автоматизації обслуговування, а також значно покращує досвід гостей, що є надзвичайно важливим для комплексів такого класу.

2.4 Структурна організація мережі

Як вказувалось вище, мережа готельного комплексу побудована на трирівневій ієрархічній моделі, детально зображеній на рис. Б.4, додаток Б,. Така схема забезпечує оптимальну продуктивність, безпеку та керованість.

Основу мережі становлять три головні елементи: маршрутизатори Router_DMZ_out, Router_DMZ_in і комутатор Switch_Serv які по суті утворюють ядро мережі. Маршрутизатор Router_DMZ_out виконує функцію міжмережевого екрану, захищаючи внутрішню мережу від зовнішніх загроз і забезпечуючи безпечне з'єднання з зовнішнім каналом Інтернет. Router_DMZ_in забезпечує маршрутизацією внутрішнього трафіку і розподіляє мережеві ресурси між різними сегментами. Комутатор Switch_Serv відповідає за швидкісне підключення всього серверного обладнання готелю до мережевого ядра. Топологія зв'язків на рівні ядра організована за принципом зірки, що дозволяє централізовано керувати і забезпечувати високу пропускну здатність завдяки технології Gigabit Ethernet.

Інтеграція мережі IP-телефонії виконується через безпосереднє приєднання до маршрутизатора Router_DMZ_in. Телефонна інфраструктура готелю інтегрована з основною IP-мережею, що дає змогу підключити всі IP-телефони через єдину телекомунікаційну мережу. З'єднання між IP-МініАТС та маршрутизатором здійснюється за технологією Fast Ethernet.

Рівень розподілу та доступу утворений комутаторами Switch_Floor_№№0-5 з кільцевою топологією. Цей сегмент управляється маршрутизатором рівня розподілу і він забезпечує зв'язок між кільцем та ядром.

Як і у випадку з ядром, технологія Gigabit Ethernet забезпечує високу пропускну здатність для цього сегмента.

До комутатори Switch_Floor_№№0-5 мають бути підключені усі активні пристрої в номерах і загальних зонах готелю, включаючи:

- персональні комп'ютери адміністрації та персоналу;
- бездротові точки доступу WiFi;
- IP-телефони;
- IP-камери зовнішнього спостереження;
- телевізійні приставки для IP-телебачення;
- контролери IoT та СКУД.

Підключення всього цього обладнання до мережі на рівні доступу виконується за технологією Fast Ethernet, що відповідає актуальним потребам в пропускній здатності для таких пристроїв. В деяких випадках точково використана технологія PoE.

2.5 Функціональна схема мережі

Функціональна схема мережі, детально на рис. Б.5, додаток Б, демонструє її структурну організацію, фізичні зв'язки, топологію, застосовані технології та функціональне призначення основних компонентів на рівнях ядра, розподілу та доступу. Замість докладного аналізу конфігурацій портів активного обладнання, що є зрозумілим безпосередньо зі схеми, опишемо функціональні аспекти організації мережі та механізми забезпечення послуг.

Маршрутизатори на рівні ядра відіграють ключову роль, виконуючи функції маршрутизації трафіку, створення демілітаризованої зони (DMZ) для підвищення рівня захисту мережі, а також забезпечення виходу до глобальної мережі Інтернет. На цьому рівні маршрутизатори під’єднані до комутаторів рівня розподілу за допомогою технології Gigabit Ethernet, що дозволяє ефективно агрегувати трафік із рівня доступу. Підключення кінцевих

користувачів здійснюється до комутаторів рівня доступу через технологію Fast Ethernet, яка оптимально підходить для типової клієнтської інфраструктури, включаючи персональні комп’ютери та ноутбуки.

Загальна архітектура IP-мережі базується на технології Ethernet із використанням як фізичного середовища оптичних і мідних кабелів. Додатково передбачено бездротовий сегмент (Wi-Fi), який виконує допоміжну функцію й здебільшого спрямований на забезпечення доступу до Інтернету для мобільних користувачів. Управління мережею та забезпечення взаємодії між обладнанням здійснюється за допомогою стеку протоколів TCP/IP, який виступає основою для комунікації між ключовими компонентами мережі та кінцевими пристроями.

Для забезпечення повноцінного функціонування мережі та реалізації різних видів послуг інтегровано низку спеціалізованих протоколів, серед яких DHCP, 802.1Q, NAT, TCP/IP, UDP, HTTP, FTP, H.263, H.264, RTP, RTSP, IGMP, STP.

Протокол DHCP (Dynamic Host Configuration Protocol) необхідний для автоматизації процесу розподілу IP-адрес разом із додатковими мережевими параметрами серед кінцевих пристроїв мережі. Служба DHCP впроваджена на маршрутизаторі Router_DMZ_in. Інфраструктура включає сім окремих адресних просторів, які розроблені для забезпечення логічної сегментації мережі та оптимізації управління:

1. Службовий адресний простір для мережної інфраструктури.
2. СКУД та IoT застосунки.
3. Кабельні підключення для персональних комп'ютерів і ноутбуків адміністрації та персоналу.
4. Користувачі бездротового сегменту мережі.
5. IP-телефони.
6. IPTV-приставки (STB).
7. Відеоспостереження (камери).

Видача IP-адрес здійснюється динамічно, не враховуючи фіксацію MAC-

адрес за винятком пристроїв у бездротовому сегменті, де встановлено обмеження терміну дії (лізинг). Для інших сегментів передбачено постійне надання динамічних адрес.

Протокол 802.1q (VLAN) забезпечує логічний поділ активних пристроїв у межах єдиної фізичної мережевої інфраструктури на віртуальні локальні мережі (VLAN). Реалізація VLAN на базі 802.1q суттєво оптимізує продуктивність шляхом локалізації широкомовних доменів, а також покращує безпеку через трафікову ізоляцію між сегментами мережі. У мережевій архітектурі передбачено кілька VLAN для потреб різних груп користувачів, які за своєю кількістю та функціональним призначенням співпадають з наявними DHCP адресними просторами. Використання протоколу 802.1q об'єднує комутатори рівня доступу й розподілу з ядровим маршрутизатором, що функціонує на третьому рівні моделі OSI.

Служба NAT (Network Address Translation) необхідна для перетворення приватних локальних IP-адрес в публічні IP-адреси, і забезпечує доступ внутрішніх пристроїв до Інтернет. NAT активовано на маршрутизаторі Router_DMZ_out. Ця служба має критичне значення, оскільки вона гарантує вихід усіх пристроїв локальної мережі до глобальної мережевої інфраструктури.

Протокол прикладного рівня HTTP (Hypertext Transfer Protocol) забезпечує доступ до веб-ресурсів глобальної мережі Інтернет.

Протокол прикладного рівня FTP (File Transfer Protocol) використовується для передачі файлів між комп’ютерами через мережу.

Протоколи H.263 та H.264 використані для системи відеоспостереження бо є стандартами для кодування відео, які визначають набір правил, що забезпечують відеотрансляції та IP-телефонію. H.264 (AVC) є сучаснішим і найбільш популярним рішенням у порівнянні з H.263.

Для реалізації потокових сервісів IPTV використовуються UDP, HTTP, RTP, RTSP, IGMP.

UDP (User Datagram Protocol) призначений для передачі потокового мультимедійного контенту, з пріоритетом швидкості передачі даних над гарантованою доставкою.

HTTP використовується для забезпечення інтерактивних сервісів, таких як навігація в меню чи доступ до додаткових можливостей IPTV.

RTSP (Real-Time Streaming Protocol) забезпечує управління потоками мовлення, дозволяючи користувачам контролювати відтворення.

RTP (Real-Time Transport Protocol) забезпечує безпосередню передачу аудіо- та відеоданих у режимі реального часу.

IGMP (Internet Group Management Protocol) дозволяє організувати управління мультикаст-потоками, надаючи пристроям можливість підключатися до груп для отримання каналів IP-телебачення або залишати їх, при цьому оптимізуючи мережевий трафік.

Для підвищення надійності мережі використовується протокол STP (Spanning Tree Protocol). Він попереджає утворення мережевих кілець і широкомовних штормів у Ethernet-мережах. Це особливо актуально в умовах кільцевих топологій, які застосовуються для забезпечення резервування. Протокол STP реалізований на комутаторах рівня розподілу в мережах з кільцевою топологією (1000BaseLX), забезпечуючи їх стабільність і відмовостійкість.

Висновки до розділу 2

В другому розділі розділ випускної кваліфікаційної роботи при проєктуванні мережної телекомунікаційної інфраструктури основний акцент зроблено на принципах конвергенції, ієрархічній побудові, виборі оптимальних технологій та протоколів для надання послуг.

В якості базового рішення використовується концепція побудови конвергентної мережі. Це рішення є ключовим, оскільки дозволяє передавати

всі типи трафіку (голос, відео, дані, системи безпеки та автоматизації) через єдине фізичне та логічне середовище на базі IP-протоколу. Такий підхід радикально відрізняється від застарілих «ізольованих» мереж. Єдину фізичну інфраструктуру, побудовану відповідно до стандартів структурованих кабельних систем (СКС). При програмному налаштуванні будуть застосовані політики QoS (Quality of Service) для пріоритетної обробки критичного трафіку. Розподіл мережі на незалежні сегменти виконано за допомогою технології VLAN 802.1q для підвищення безпеки та ефективності. Також застосовуються служба NAT та ACL для підвищення безпеки надійності з двохзонною демілітаризованою зоною.

Архітектура мережі відповідає трирівневій ієрархічній моделі: ядро, розподіл та доступ, яка забезпечує надання доступу до Інтернету та локальних мережевих ресурсів, IP-телефонії, IPTV та VoD, а також для інтеграції функцій контролю доступу (СКУД) з елементами Інтернету речей (IoT) та систем відеоспостереження.

Вибір мережевих технологій базується на стандартах Ethernet, зокрема Fast Ethernet (100 Мбіт/с) для рівня доступу та Gigabit Ethernet (1000 Мбіт/с) для високошвидкісних магістральних каналів на рівнях розподілу та ядра. Бездротовий сегмент мережі (Wi-Fi) доповнює дротову інфраструктуру, надаючи мобільний доступ до Інтернету і буде побудований на базі рекомендацій стандарту Wi-Fi 6 (802.11ax).

Для послуг мережі обрані основні архітектурні рішення і необхідні протоколи та технології. На підставі проведеного аналізу були розроблені та описані основні схемотехнічні рішення, а саме структурна та функціональна схеми.

3 АПАРАТНИЙ СИНТЕЗ ТА ОСНОВНІ НАЛАШТУВАННЯ

3.1 Вибір обладнання

Відповідно до структурної та функціональної схем в мережі готелю передбачено використання двох базових маршрутизаторів: Router_DMZ_in та Router_DMZ_out. Вибір пристроїв буде грунтуватись на критеріях, що були визначені в попередніх розділах:

- продуктивність – мінімальна пропускна здатність пристроїв має становити не менше 1 Гбіт/с;
- підтримка протоколів та функціоналу – 802.1q, OSPF, EIGRP, DHCP, NAT;
- безпека – створення списків доступу ACL;
- керування трафіком –QoS, CoS;
- конфігурація портів – 2 x SC 1000BaseLX, 1x RJ-45 100BaseT; 3 x SC 1000BaseLX для побудови високошвидкісних оптичних каналів.

Зазначені технічні вимоги слугують основою для подальшого аналізу і порівняння моделей обладнання від провідних виробників. Результати цього аналізу будуть викладені у табл. 3.1 [18].

Таблиця 3.1 – Порівняння маршрутизаторів

	D-Link DIR-100F	Cisco 3845	MikroTik CCR1036 12G-4S
Типи маршрутизуємих фізичних інтерфейсів	1xSC GE	2xRJ-45 GE, 4xSC GE	4xRJ-45 GE, 4xSC GE
Продуктивність	4 Гбіт/с	12 Гбіт/с	16 Гбіт/с
Пітримка IP- телефонії/ IPTV	так/так	Cisco Call Manager/так	так/так
Підтримка проктолів	OSPF, DHCP, NAT	802/q, OSPF, Eigrp, VLAN, DHCP, NAT	802/q, OSPF, DHCP, NAT
Форм-фактор	1 U	3 U	1 U
Енергоспоживання, Вт	20	150	60
Резервування блока живлення	ні	так	ні

Враховуючи критерії якості та функціональності, оптимальним вибором є обладнання виробництва Cisco.

В якості основного внутрішнього маршрутизатора Router_DMZ_in обрано Cisco 3845. Цей пристрій є потужною та захищеною платформою, здатною одночасно забезпечувати широкий спектр критично важливих послуг:

- передача даних, голосу та відео;
- безпека з вбудованими механізмами захисту;
- можливість інтеграції Wi-Fi.

Маршрутизатори серії Cisco 3800, до якої належить 3845, вирізняються високою продуктивністю, доступністю та надійністю, необхідними для масштабування бізнес-додатків у вимогливих корпоративних середовищах. До його ключових особливостей можна віднести вбудовану систему безпеки та спрощене керування за допомогою Cisco Router and Security Device Manager (SDM); модульність платформи з широким набором підтримуваних інтерфейсів; два вбудовані маршрутизовані порти 10/100/1000 Мбіт/с з можливістю підключення до 112 комутованих портів 10/100 Мбіт/с з PoE для живлення IP-телефонів та інших пристроїв і повна сумісність з Cisco CallManager Express (до 240 користувачів) та рішеннями для віддалених об'єктів Cisco SRST (до 720 користувачів) для забезпечення безперервної роботи голосового зв'язку навіть при втраті з'єднання.

Завдяки своїй потужності та багатофункціональності, Cisco 3845 може виконувати роль не лише Router_DMZ_in, але й замінити МініАТС, комутатор поверху Switch_Floor №0 та комутатор для серверів Switch_Serv. Для цього його необхідно доукомплектувати двома модулями WIC-24ESW (24 порти RJ-45 100BaseTX з підтримкою PoE).

В якості зовнішнього маршрутизатора Router_DMZ_out обрано Cisco 1811 з серії Cisco 1800. Це рішення зумовлено необхідністю уніфікованого керування мережею та повної сумісності з іншим обладнанням Cisco. Дане сімейство маршрутизаторів є сімейством початкового рівня з інтеграцією сервісів, розробленими для забезпечення потреб невеликих офісів та

організацій у безпечному доступі до корпоративних мереж та Інтернету. Ключові переваги Cisco 1811 включають:

- апаратне прискорення шифрування трафіку та можливість його подальшого збільшення за допомогою опціонального модуля VPN;
- функціональність системи запобігання вторгненням та міжмережевого екрану;
- модульна конструкція з доступними слотами HWIC (сумісними з інтерфейсними модулями HWIC, WIC та VWIC) та гніздами AIM для сервісних модулів, що забезпечує гнучкість конфігурації.

Цей вибір дозволяє створити надійну, безпечну та керовану мережеву інфраструктуру для готельного комплексу, використовуючи перевірені рішення від провідного виробника.

Для організації підключення кінцевих користувачів та термінального обладнання необхідно обрати відповідні комутатори та точки бездротового доступу. Визначення критеріїв для вибору комутаторів базується так само як і для всього переліку активного устаткування розрахунках, виконаних у першому розділі, а також на основі розроблених структурної та функціональної схем. Основні вимоги до комутаторів такі:

- кількість та тип портів: 48xRJ-45 100 BaseTX із підтримкою PoE, 2xSC 1000 BaseLX;
- пропускна здатність не менш як 1 Гбіт/с;
- рівень OSI: L3;
- підтримка технологій VLAN, 802.1q, CoS, STP;
- можливість стекування;
- сумісність із монтажем у стандартну телекомунікаційну шафу розміру 19 дюймів.

У табл. 3.2 представлено перелік варіантів комутаторів, які в більшій чи меншій мірі відповідають зазначеним критеріям і можуть бути використані для побудови мережі і проведено відповідний порівняльний аналіз.

Таблиця 3.2 – Типи комутаторів

	DES-3200-52P	Cisco Small Business 500 (SF500-48P-K9-G5)	HP 1905-48-PoE
Типи фізичних інтерфейсів	48xRJ-45 10/100 Base, PoE, 2xRJ-45 10/100/1000 Base, 2xSFP	48xRJ-45 10/100 Base, PoE, 2xRJ-45 10/100/1000 Base, 2xSFP	48xRJ-45 10/100 Base, PoE, 2xRJ-45 10/100/1000 Base, 2xSFP
Продуктивність	16 Гбіт/с	33,6 Гбіт/с	16 Гбіт/с
Рівень OsI	L3	L3	L3
Підтримка протоколів	LACP, IPv6, VLAN, MSTP, ACL, STP, RSTP.	LACP, IPv6, VLAN, MSTP, ACL, STP, RSTP.	LACP, IPv6, VLAN, MSTP, ACL
Форм-фактор	1 U	1 U	1 U
Енергоспоживання, Вт	472	345	291
Резервування блока живлення	ні	так	ні

На основі проведеного аналізу та враховуючи можливість стандартизації та уніфікації по за ознакою єдиного виробника мережевого обладнання, раціональним варіантом є впровадження комутатора Cisco Small Business 500 (SF500-48P-K9-G5).

Стековані керовані комутатори серії Cisco Small Business 500 представляють собою високоефективне рішення, яке значно збільшує комутаційні можливості для малих і середніх підприємств. комутатора Cisco Small Business 500 (SF500-48P-K9-G5) характеризується наявністю 48 портів із підтримкою швидкості 10/100 Мбіт/с і 4 гігабітних комбо портів. Їх комутаційна здатність досягає 33,6 Гбіт/с, а продуктивність переадресації становить 13,10 мільйонів пакетів за секунду. Крім того, усі 48 портів забезпечують підтримку технології PoE, що підвищує ефективність використання ресурсу мережі і можливість підключення додаткового обладнання з дистанційним живленням [18].

Вимоги до кінцевого обладнання телефонної мережі базуються на впровадженні IP-телефонів, які забезпечують сучасну комунікаційну інфраструктуру:

– фізичний інтерфейс RJ-45 із підтримкою стандарту 100Base-TX та

Power over Ethernet (PoE);

– протокол IP-телефонії – SIP.

Враховуючи вибір маршрутизатора Cisco 3845, який підтримує програмне забезпечення Cisco CallManager для реалізації функцій IP-АТС, доцільною є інтеграція телефонних апаратів виробництва Cisco. Такий підхід гарантує повну сумісність компонентів системи, оптимізує процеси інтеграції та спрощує адміністрування телекомунікаційної інфраструктури. Порівняння стандартних моделей телефонних апаратів наведено в табл. 3.3 [18].

Таблиця 3.3 – Порівняльна характеристика IP-телефонів

	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

Для встановлення в готельних номерах та адміністративних приміщеннях обрано Cisco Unified SIP CP-3911. Це IP-телефон початкового рівня, що забезпечує базовий функціонал, необхідний для комфортного зв'язку гостей та персоналу з такими характеристиками:

– конференц-зв'язок, утримання виклику, можливість вибору однієї з двох ліній, відключення звуку, гучний зв'язок, голосова пошта;

– дисплей 2-рядковий, 24-символьний, що підтримує відображення номера абонента та історії дзвінків;

– підтримка IEEE 802.3af Power over Ethernet.

Для організації безпроводового сегменту буде використано також обладнання Cisco – точка доступу Cisco C9105AXI-E. Cisco Catalyst 9100 — це інноваційна серія точок доступу корпоративного рівня, призначена для забезпечення високотехнологічного підключення до мережі Інтернет. Моделі серії розроблені для задоволення потреб високотехнологічних компаній і підприємств, які ставлять в пріоритет високу продуктивність, надійність і безпеку мережевої інфраструктури. Серед ключових характеристик даних точок доступу слід відзначити підтримку стандарту Wi-Fi шостого покоління (802.11ax), який забезпечує утричі вищу швидкість передачі даних. Пристрої здатні здійснювати одночасну роботу на всіх частотних діапазонах, обладнані гігабітним інтерфейсом для підключення до мережі, а також мають енергоефективний режим. Крім того, реалізована підтримка технології довіри Cisco Secure Trust, яка забезпечує автентичність апаратного та програмного забезпечення.

Додатковими перевагами є сертифікація стандарту Wi-Fi 6, використання трьох радіомодулів (2,4 ГГц, 5 ГГц і модуль Bluetooth Low Energy 5.0), а також підтримка передових технологій передачі даних, таких як OFDMA та MU-MIMO з конфігурацією 4x4. Усе це робить серію Cisco Catalyst 9100 оптимальним рішенням для впровадження високопродуктивних і надійних мереж у професійному середовищі [18].

Система відеоспостереження готельного комплексу включатиме IP-камери та пристрої для зберігання відеоконтенту, зокрема відеореєстратори. До камер висуваються такі основні вимоги:

– наявність порту RJ-45 100BaseTX для підключення до мережі;
– підтримка Power over Ethernet (PoE);
– підтримка відеокодека H.264;
– здатність працювати в умовах слабкого освітлення або повної темряви.

На основі цих критеріїв був виконаний аналіз кількох моделей камер,

результати порівняння наведено у табл. 3.4.

Таблиця 3.4 – Порівняльна характеристика відеокамер

	FOSCAM FI8904	Linovision IPC-VEC8242F-EI	Trans TR-2MIPR140
Кодек	MJPEG	H.264/MJPEG	H.264
Підключення до мережі	RJ-45 100 BaseT, PoE	RJ-45 100 BaseT, PoE	RJ-45 100 BaseT, PoE
Нічне спостереження	20 м	20 м	45
Оптичний зум	ні	так	так
Тип матриці	1/4" CMOS (1,2 MPix)	1/3" CMOS (1,3 MPix)	1/3" CMOS 1600 x 1200! (2 MPix)
Клас захисту	IP 66	IP 66	IP 66

На основі проведеного аналізу для системи відеоспостереження готелю була вибрана IP-камера Linovision IPC-VEC8242F-EI. Ця камера оптимально підходить до відеореєстратора Linovision NVR-9164S, який відзначається потужною продуктивністю та великою ємністю. Він підтримує одночасне підключення до 64 камер і оснащений 16 роз'ємами SATA II для підключення жорстких дисків, що дозволяє зберігати значний обсяг відеоархівів. Також пристрій має 8 ГБ оперативної пам’яті для швидкої та ефективної обробки даних [18].

Система контролю доступу має бути інтегрованою з рішеннями IoT та підсистемами пожежної та охоронної сигналізації. Також важливим аспектом є можливість інтеграції систем управління будівлею та окремими номерами і що не менш важливо необхідно подбати про безпекову складову комплексу в цілому. У випадку розрізненості підсистем дуже важко вибудовувати політики безпеки в мережному середовищі, тому доцільно обирати інтегровано рішення. В табл. 3.5 наведена порівняльна характеристика основних вендорів – виробників платформ та інтегрованих рішень, що використовуються як в готельному бізнесі так і в сфері управління інфраструктурою та інженерними мережами будівель.

Таблиця 3.5 – Порівняння комплексних рішень в галузі СКУД та IoT

Характеристика	ASSA ABLOY Global Solutions	dormakaba	SALTO Systems	Cisco Meraki (як інтегратор)	Schneider Electric (як GRMS/IoT інтегратор)
Основна спеціалізація	Готельні електронні замки, сейфи, мінібари	Готельні замки, СКУД, дверні рішення	Бездротові та хмарні СКУД, електронні замки	Мережева інфр., хмарне управління, IoT, відео-спостереження	Системи управління готельними номерами (GRMS), енерго-ефективність, автоматизація
Типи ключів	Магнітні картки, RFID, NFC, Bluetooth (Mobile Access)	Магнітні картки, RFID, NFC, Bluetooth (Mobile Access)	RFID, NFC, Bluetooth (JustIN Mobile)	- (інтегрується з рішеннями партнерів)	RFID, Bluetooth, фізичні кнопки
Тип зв'язку замків	Онлайн (Ethernet/Wi-Fi), Офлайн,	Онлайн, Офлайн,	Бездротовий (SALTO SVN - Virtual Network), Онлайн,	- (інтеграція через партнерів)	Дротовий, бездротовий (IoT протоколи)
Інтеграція з PMS	Дуже висока, глибока інтеграція (стандарт де-факто)	Дуже висока, глибока інтеграція	Висока, через API	Платформа Meraki може інтегрувати дані	Висока, для GRMS та BMS (Building Management System)
Централізоване управління	Так, спеціалізовані ПЗ (Visionline, Vostio)	Так, спеціалізовані ПЗ	Так, спеціалізовані ПЗ (SALTO ProAccess SPACE)	Хмарна платформа для мережевої інфраструктури (Meraki Dashboard)	Єдина платформа для GRMS та енергоменеджменту
Інтеграція з IoT/GRMS	Обмежена, здебільшого через партнери	Обмежена, здебільшого через партнери	Так, через відкриті API та партнерства	Сильна, як основа для "Connected Hotel" (мережевий шар для IoT)	Дуже сильна, фокус на комфорті номера та енергоефективності
Рівень безпеки	Високий, перевірені рішення	Високий, перевірені рішення	Високий, гнучкі рівні доступу	Високий (як мережева основа)	Високий (як частина загальної системи безпеки)
Переваги для готелю	Надійність, глобальний стандарт, мобільний доступ.	Комплексні рішення, дверна фурнітура, надійність.	Гнучкість, бездротові технології, легке розширення, інновації.	Єдине вікно управління IT-інфр., глибока аналітика.	Енергоефективність, автоматизація комфорту номерів, інтеграція з BMS.

Аналізуючи представлені варіанти можна виокремити нетипове на перший погляд рішення, а саме Cisco Connected Hotel. До його переваг в порівнянні з конкурентами можна віднести можливість реалізації повноцінного керування всією інфраструктурою готелю починаючи від замка на дверях і закінчюючи доступом до мережі Інтернет для окремих користувачів і впровадженні спеціалізованих списків доступу і набору послуг. Також варто відзначити глибокий рівень інтеграції з хмарними і безпековими рішеннями. Тож

Концепція Cisco Connected Hotel являє собою цілісну стратегію та комплексний набір рішень для формування сучасної, інтегрованої і розумної мережевої інфраструктури в готельному секторі. Основні елементи та можливості Cisco Connected Hotel:

- конвергентна IP-мережа;
- висока пропускна здатність;
- розширений Wi-Fi для гостей і персоналу;
- персоналізований доступ;
- пріоритизація трафіку (QoS);
- IP-телефонія та уніфіковані комунікації;
- інтеграція з CRM і PMS;
- відеонагляд на основі IP-технологій;
- СКУД (інтеграція електронних замків провідних виробників (VingCard, dormakaba, SALTO тощо);
- IoT у готельних номерах;
- моніторинг і керування інженерними системами.

Окрім базових функцій, особлива увага даного рішення приділена питанню кібербезпеки, а саме використанню міжмережевих екранів, технологій VPN та сегментації мережі завдяки VLAN, що дає можливість реалізувати безпечний доступ із віддалених локацій до корпоративної інфраструктури.

В дане рішення одразу інтегрована системи попередження та запобігання вторгненням (IPS/IDS) з постійним моніторингом мережевої активності, що

допомагає вчасно виявляти та блокувати підозрілу поведінку.

Керування інфраструктурою здійснюється за допомогою платформи Cisco Meraki, яка використовується для моніторингу та адміністрування всіх компонентів мережевої інфраструктури, включаючи точки доступу Wi-Fi, комутатори, маршрутизатори та відеокамери [19].

IP-мережа готелю передбачає використання Структурованих Кабельних Систем (СКС), що гарантує універсальну платформу для передачі даних різних типів, включаючи голосовий трафік, відео та стандартний мережевий обмін. Виробником пасивних компонентів обираємо компанію Molex, яка надає 25 річну гарантію та забезпечує роботу мережі на протязі 40 років [20]. До складу пасивного обладнання входять кабелі, роз'єми, патч-панелі, розетки та монтажні стійки, призначені для розміщення активних компонентів. Відповідно до рекомендацій із проектування СКС були обрані наступні елементи:

1. Кабель:

- MOLEX UTP PowerCat кат. 5e (LSZH) – кручена пара для горизонтальної підсистеми доступу.

- MOLEX optic 4x50/100 – оптичний кабель для вертикальної підсистеми та магістралей.

2. Комутаційні панелі:

- 19" UTP, 24xRJ45, 1U, кат. 5e, Molex PowerCat – для крученої пари.

- 19", SC, 12xSC, Molex – для оптоволокона.

3. Монтажні шафи підлогові Molex 24U, 600x600 MODBOX III, для розміщення активного і пасивного обладнання.

4. Патч-корди:

- RJ45 Molex UTP 5e PVC 0.5m, сірі – для коротких з'єднань усередині шафи.

- RJ45 Molex UTP 5e PVC 2m, сірі – для більш гнучких з'єднань.

- Пігтейли SC – для підключення оптичних волокон.

5. Розетки Molex Office Block 2xRJ45, UTP, кат. 5e – для підключення термінального устаткування.

Усі кабелі та з'єднання між активним обладнанням будуть підключені до патч-панелей у комутаційних шафах. Схеми організації шаф та детальні схеми з'єднань представлені у додатках на рис. Б.6-Б.7.

3.2 Базові налаштування IP-мережі

Для перевірки параметрів безпеки розробимо спрощену імітаційну модель мережі, яка дозволить нам перевірити правильність прийнятих рішень щодо архітектури та логічної структуризації. В якості середовища імітаційного моделювання використаємо програмне забезпечення Cisco Packet Tracer.

На рис. 3.1 наведена схема розподілу адресного простору та віртуальних підмереж.

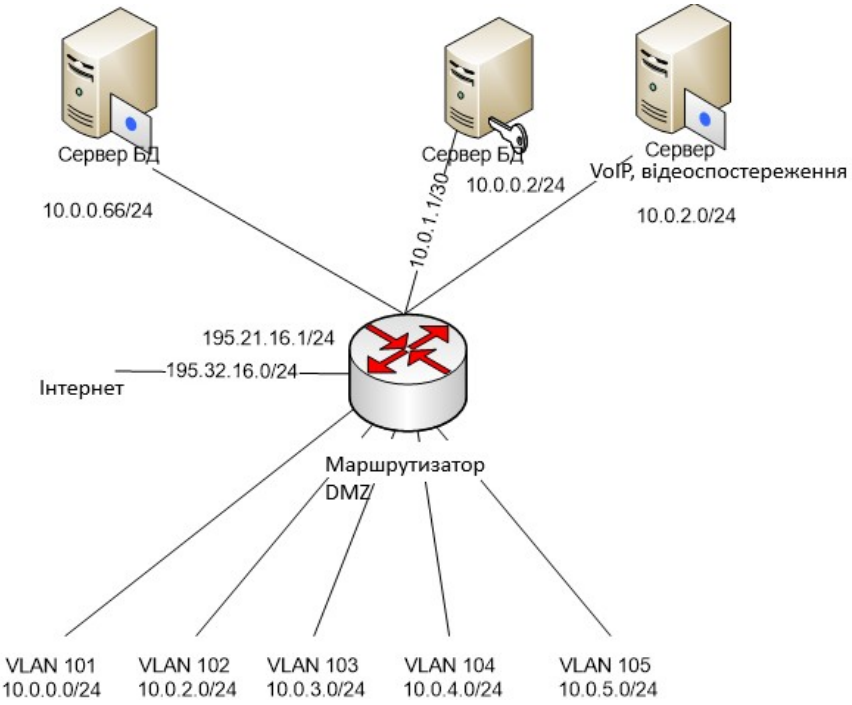

Рисунок 3.1 – Спрощена схема розподілу адресного простору

На підставі структурної, функціональної схеми та схеми розподілу адресного була розроблена схема моделі в Packet Tracer, яка наведена на рис. 3.2.

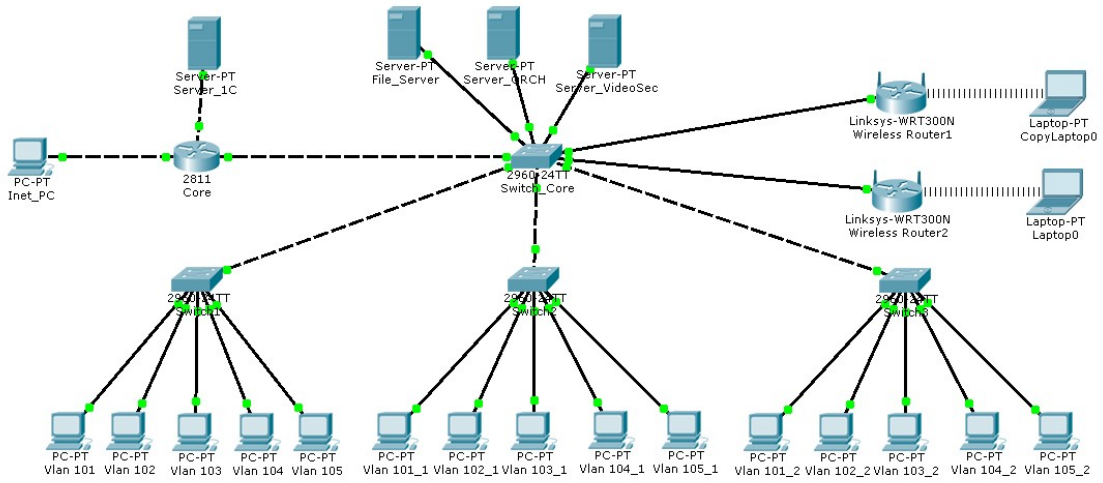

Рисунок 3.2 – Схема імітаційної моделі

Запропонована мережева структура базується на використанні центрального маршрутизатора Core. До його портів підключені зовнішній Інтернет-канал і сервер баз даних. До одного з комутованих портів цього маршрутизатора під'єднано комутатор розподілу Core, який виконує функцію підключення:

- групи серверного обладнання;
- двох точок бездротового доступу;
- трьох комутаторів рівня доступу.

Процес налаштування мережевого обладнання доцільно розпочинати знизу договори, тобто з комутаторів рівня доступу. Конфігурацію віртуальних мереж і налаштувань інтерфейсів комутатора Switch1 буде виконано відповідно до схеми, наведеної на рис. 3.1.

```
//входимо в режим конфігурування
Switch1>en
Switch1#conf t
Switch1(config)#
//створюємо логічні мережі VLAN
Switch1(config)#vlan 101
Switch1(config-vlan)#name Admin
Switch1(config)#vlan 102
Switch1(config-vlan)#name KKD
Switch1(config)#vlan 103
Switch1(config-vlan)#name Videosec
Switch1(config)#vlan 104
Switch1(config-vlan)#name Spivr
```

```
Switch1(config)#vlan 105
Switch1(config-vlan)#name WiFi
//налаштовуємо порти в режимі Access для відповідних VLAN
Switch1(config)#interface FastEthernet0/2
Switch1(config-if)#switchport access vlan 101
Switch1(config)#interface FastEthernet0/3
Switch1(config-if)#switchport access vlan 102
Switch1(config)#interface FastEthernet0/4
Switch1(config-if)#switchport access vlan 103
Switch1(config)#interface FastEthernet0/5
Switch1(config-if)#switchport access vlan 104
Switch1(config)#interface FastEthernet0/6
Switch1(config-if)#switchport access vlan 105
//налаштовуємо порт в бік комутатора Core в режимі Trunk
Switch1(config)#interface FastEthernet0/1
Switch1(config-if)#switchport mode trunk
```

Комутатори доступу Switch2 та Switch3 налаштовуються так само як комутатор Switch1.

Наступним кроком є налаштування портів комутатора Core, для якого необхідно провести таку конфігурацію:

- порти, спрямовані до комутаторів доступу встановити для роботи в режимі trunk, що забезпечить передачу трафіку кількох віртуальних мереж (VLAN) через одне фізичне з'єднання;
- створити потрібні VLAN для логічного розподілу мережевих сегментів;
- порти, направлені в бік до серверного обладнання налаштувати для роботи в режимі Access, що дозволить серверам підключатися до відповідних віртуальних мереж.

```
//входимо в режим конфігурування
Switch_Core>en
Switch_Core#conf t
//створюємо логічні мережі VLAN
Switch_Core(config)#vlan 101
Switch_Core(config-vlan)#name Admin
Switch_Core(config)#vlan 102
Switch_Core(config-vlan)#name KKD
Switch_Core(config)#vlan 103
Switch_Core(config-vlan)#name Videosec
Switch_Core(config)#vlan 104
Switch_Core(config-vlan)#name Spivr
Switch_Core(config)#vlan 105
Switch_Core(config-vlan)#name WiFi
//налаштовуємо порти в режимі Access для відповідних VLAN
Switch_Core(config)#interface FastEthernet0/5
Switch_Core(config-if)#switchport access vlan 101
Switch_Core(config)#interface FastEthernet0/6
```

```
      Switch_Core(config-if)#switchport access vlan 102
      Switch_Core(config)#interface FastEthernet0/7
      Switch_Core(config-if)#switchport access vlan 103
      Switch_Core(config)#interface FastEthernet0/8
      Switch_Core(config-if)#switchport access vlan 104
      Switch_Core(config)#interface FastEthernet0/9
      Switch_Core(config-if)#switchport access vlan 105
      //налаштовуємо порт в бік комутаторів доступ та маршрутизатора в режимі
Trunk
      Switch_Core(config)#interface FastEthernet0/1
      Switch_Core(config-if)#switchport mode trunk
      Switch_Core(config)#interface FastEthernet0/2
      Switch_Core(config-if)#switchport mode trunk
      Switch_Core(config)#interface FastEthernet0/3
      Switch_Core(config-if)#switchport mode trunk
      Switch_Core(config)#interface FastEthernet0/4
      Switch_Core(config-if)#switchport mode trunk
```

Перейдемо до налаштування точок бездротового доступу (рис. 3.3-3.4), для яких необхідно обрати частотний канал, режим роботи, SSID та вимкнути внутрішній DHCP сервер.

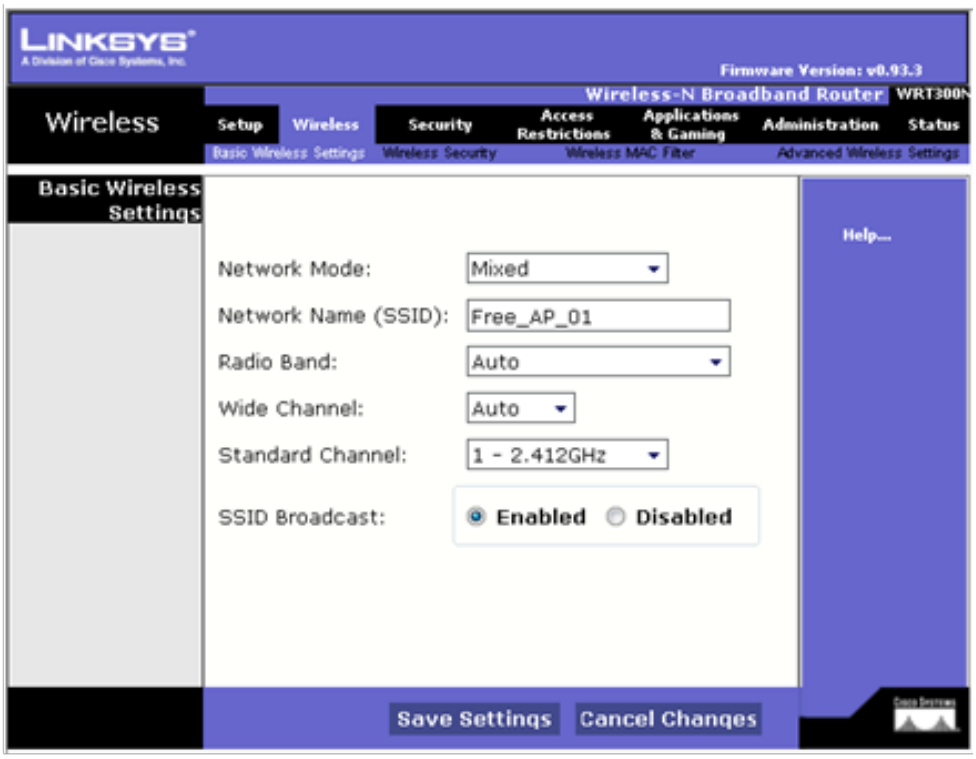

Рисунок 3.3 – Налаштування радіо інтерфейсу

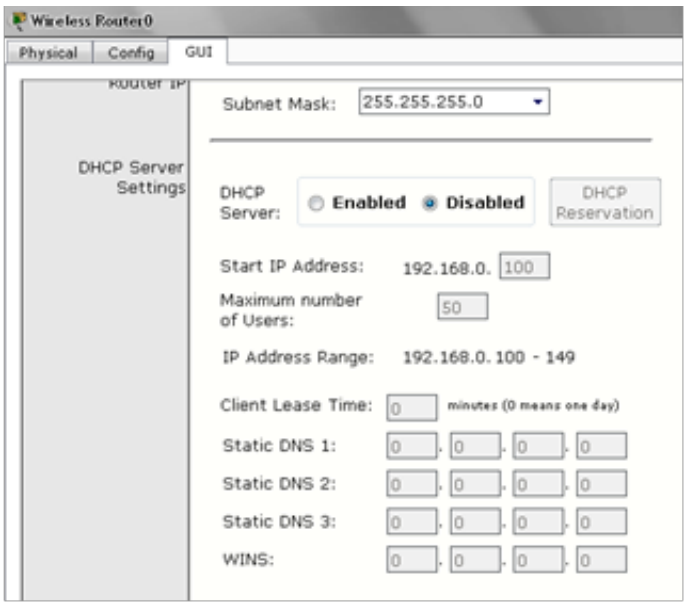

Рисунок 3.4 – Відключення внутрішньої служби DHCP

На всіх точках доступу проводимо аналогічні налаштування.

На маршрутизорі демілітаризованої зони необхідно налаштувати служби NAT та DHCP:

```
//входимо в режим конфігурування
Core>en
Core#conf t
//створюємо віртуальні підмережі
Core(vlan)# vlan 101 name Admin
VLAN 101 modified:
    Name: Admin
Core(vlan)#vlan 102 name KKD
VLAN 102 modified:
    Name: KKD
Core(vlan)#vlan 103 name Videosec
VLAN 103 modified:
    Name: Videosec
Core(vlan)#vlan 104 name Spivr
VLAN 104 modified:
    Name: Spivr
Core(vlan)#vlan 105 name WiFi
VLAN 105 modified:
    Name: WiFi
Core(vlan)#ex
APPLY completed.
Exiting....
Core#
//налаштовуємо IP-адреси віртуальних та фізичних інтерфейсів
Core#conf t
Core(config)#int vlan 101
Core(config-if)#ip addr 10.0.0.1 255.255.255.0
Core(config-if)#int vlan 102
Core(config-if)#ip addr 10.0.1.1 255.255.255.0
Core(config-if)#int vlan 103
Core(config-if)#ip addr 10.0.2.1 255.255.255.0
```

```
Core(config-if)#int vlan 104
Core(config-if)#ip addr 10.0.3.1 255.255.255.0
Core(config-if)#int vlan 105
Core(config-if)#ip addr 10.0.4.0 255.255.255.0
Core(config-if)#int fa 0/0
Core(config-if)#no shutdown
Core(config-if)#ip addr 195.21.16.1 255.255.255.0
Core(config-if)#int fa 0/1
Core(config-if)#no shutdown
Core(config-if)#ip addr 10.0.1.1 255.255.255.252
Core(config-if)#ex
//налаштовуємо порт комутатора маршрутизатора в режимі  trunk
Core(config)#int fa 0/3/0
Core(config-if)#no shutdown
Core(config-if)#switchport mode trunk
//активуємо службу  DHCP
Core(config)# ip dhcp pool Admin
Core(dhcp-config)#network 10.0.0.0 255.255.255.0
Core(dhcp-config)#default-router 10.0.0.1
Core(config)#ip dhcp pool KKD
Core(dhcp-config)#network 10.0.1.0 255.255.255.0
Core(dhcp-config)#default-router 10.0.1.1
Core(config)#ip dhcp pool Videosec
Core(dhcp-config)#network 10.0.2.0 255.255.255.0
Core(dhcp-config)#default-router 10.0.2.1
Core(dhcp-config)#ip dhcp pool Spivr
Core(dhcp-config)#network 10.0.3.0 255.255.255.0
Core(dhcp-config)#default-router 10.0.3.1
Core(dhcp-config)#ip dhcp pool WiFi
Core(dhcp-config)#network 10.0.4.0 255.255.255.0
Core(dhcp-config)#default-router 10.0.4.1
Core(dhcp-config)#ex
Core(config-if)#interface FastEthernet0/0
Core(config-if)#ip nat outside
Core(config)#ip access-list standard 10
Core(config-std-nacl)#permit 10.0.0.0 0.0.0.255
Core(config-std-nacl)#permit 10.0.4.0 0.0.0.255
Core(config-std-nacl)#deny any
Core(config)#ip nat inside source list 10 int fa 0/3/0 overload
```

Правила налаштування списків доступу викладені в табл. 3.6.

Таблиця 3.6 – Правила доступу

	Admin	WiFi	Videosec	KKD
Інтернет	+	+	-	-
Сервер БД	+	-	-	+
Сервер BMS	+	-	-	-
Відеоспотереження	+	-	+	-
Система ККД	+	-	-	+
Склад групи користувачів	персональні комп’ютери	мобільні пристрої	відеокамери	датчики та зчитувачі

Проведемо налаштування ACL для серверу BMS:

```
//створюємо список доступу
Core(config)#ip access-list standard 15
Core(config-std-nacl)#permit 10.0.0.0 0.0.0.255
Core(config-std-nacl)#deny any
Core(config-std-nacl)#ex
//накладаємо список доступу 15 на інтерфейс до якого підключений сервер
Core(config)#int fa 0/1
Core(config-if)#ip access-group 15 out
Core(config-if)#
```

Проведемо перевірку роботи за допомогою команди ping:

```
Packet Tracer PC Command Line 1.0
PC>tracert 10.0.0.66

Tracing route to 10.0.0.66 over a maximum of 30 hops:

  1   62 ms     16 ms     16 ms     10.0.0.1
  2   47 ms     31 ms     32 ms     10.0.0.66

Trace complete.

PC>tracert 195.21.16.2

Tracing route to 195.21.16.2 over a maximum of 30 hops:

  1   16 ms     16 ms     31 ms     10.0.0.1
  2   126 ms    32 ms     16 ms     195.21.16.2

Trace complete.

PC>tracert 10.0.0.34

Tracing route to 10.0.0.34 over a maximum of 30 hops:

  1   0 ms      16 ms     16 ms     10.0.0.1
  2   16 ms     16 ms     16 ms     10.0.0.1
  3   16 ms     17 ms     32 ms     10.0.0.1
  4   15 ms     46 ms     47 ms     10.0.0.1
  5   16 ms     16 ms     16 ms     10.0.0.1
  6   15 ms
Control-C
^C
```

Мережа успішно налаштована та функціонує без збоїв. Конфігурація розробленої моделі завершена, її працездатність підтверджено шляхом тестування за допомогою команди ping.

Висновки до розділу 3

Третій розділ кваліфікаційної роботи був присвячений вибору та

обґрунтуванню мережевого обладнання для готелю, враховуючи технічні вимоги і концепцію конвергентної мережі. Основною метою було підібрати оптимальне обладнання, яке забезпечить високу продуктивність, надійність, безпеку та ефективне функціонування систем комплексу.

В першій частині розділу проведено аналіз і вибір активного мережевого обладнання, зокрема обрано маршрутизатори демілітаризованої зони, комутатори ядра, розподілу/доступу, точки безпроводового доступу, IP-камери та DVR, пристрої IP-телефонії, вирішено питання щодо організації послуги IPTV+VoD, визначено спосіб загальної організації мережі готелю. Майже все активне обладнання вендора Cisco, окрім підсистеми відеоспостереження.

Пасивні компоненти представлені повноцінною СКС, яка побудована на компонентах компанії Molex і містить повний спектр обладнання – мідні та оптичні кабелі, комутаційні панелі, патч-корди та піг-тейли, телекомунікаційні шафи та термінальні розетки.

Також була проведена перевірка роботи мережі і коректності обраного обладнання і прийнятих проєктних та схемотехнічних рішень шляхом імітаційного моделювання в середовищі Cisco Pscket Tracer. Було сконфігуровано і проведено тестування конфігурацій VLAN, маршрутизації та портів за допомогою команди ping, що підтвердило коректність налаштувань і надійність взаємодії компонентів.

Загалом вибір та обґрунтування мережевого обладнання забезпечили створення масштабованої, безпечної й функціонально досконалої інфраструктури, яка відповідає сучасним вимогам для готельних комплексів.

ВИСНОВКИ

Кваліфікаційна робота присвячена проектуванню телекомунікаційної інфраструктури готельного комплексу «Franziskanerinner von Route». Актуальність цієї розробки зумовлена поточною реконструкцією готелю, що вимагає переосмислення та впровадження принципово нових мережевих та архітектурних рішень. Головною метою проекту було створення конвергентної мережі, що відповідає галузевим стандартам Hospitality Technology Next Generation (HTNG) і здатна задовольнити всі потреби сучасної готельної сфери.

В роботі проведено аналіз об'єкта проектування: готельний комплекс може одночасно приймати до 213 осіб; загальна кількість активних підключень включаючи смартфони, Smart TV, IP-камери та IoT-контролери – 794. Розрахунок показав, що навантаження на мережу дорівнює 1470 Мбіт/с.

Другий розділ кваліфікаційної роботи присвячений теоретичним засадам та принципам побудови телекомунікаційної інфраструктури. Ключовим рішенням є створення конвергентної мережі, яка дозволяє передавати всі типи трафіку – голос, відео, дані, дані систем безпеки та автоматизації через єдине фізичне та логічне середовище. На програмному рівні передбачено застосування політик QoS для пріоритетної обробки критичного трафіку. Розподіл мережі на незалежні сегменти виконано за допомогою технології VLAN 802.1q. Для забезпечення безпеки та надійності використовується служба NAT та ACL з двозонною демілітаризованою зоною DMZ.

Архітектура мережі відповідає трирівневій ієрархічній моделі (ядро, розподіл, доступ), яка забезпечує не лише доступ до Інтернету та локальних мережевих ресурсів, але й повноцінне функціонування IP-телефонії, IPTV та VoD, а також інтеграцію СКУД з IoT та систем відеоспостереження. Вибір мережевих технологій ґрунтується на стандартах Ethernet: Fast Ethernet для рівня доступу та Gigabit Ethernet для магістральних каналів на рівнях розподілу та ядра. Бездротовий сегмент мережі доповнює дротову інфраструктуру, надаючи доступ до Інтернет, побудований на базі стандарту Wi-Fi 6 (802.11ax).

На підставі проведеного аналізу були розроблені та описані основні схемотехнічні рішення, зокрема структурна та функціональна схеми мережі.

Третій розділ кваліфікаційної роботи присвячений вибору мережевого обладнання для готелю, з урахуванням технічних вимог та концепції конвергентної мережі. Основною метою було підібрати оптимальні компоненти, що забезпечать високу продуктивність, надійність, безпеку та ефективне функціонування усіх систем готельного комплексу.

У першій частині цього розділу проведено аналіз та вибір активного мережевого обладнання. Були обрані маршрутизатори демілітаризованої зони, комутатори ядра, розподілу/доступу, точки бездротового доступу, IP-камери та відеореєстратори (DVR), пристрої IP-телефонії. Також вирішено питання щодо організації послуги IPTV+VoD та загального способу організації мережі готелю. Важливо відзначити, що майже все активне обладнання обрано від провідного вендора Cisco, за винятком підсистеми відеоспостереження, що забезпечує високу сумісність та централізоване управління.

Пасивні частина представлена повноцінною СКС, побудованою на компонентах компанії Molex. Ця СКС включає повний спектр необхідного обладнання: мідні та оптичні кабелі, комутаційні панелі, патч-корди та піг-тейли, телекомунікаційні шафи та термінальні розетки.

Для перевірки роботи мережі та коректності обраного обладнання, а також прийнятих проектних та схемотехнічних рішень, було проведено імітаційне моделювання в середовищі Cisco Packet Tracer. В ході моделювання були сконфігуровані та протестовані конфігурації VLAN, маршрутизації та портів, що підтвердило коректність налаштувань та надійність взаємодії всіх компонентів мережі.

Загалом, вибір та обґрунтування мережевого обладнання в даній роботі забезпечили створення масштабованої, безпечної та функціонально досконалої інфраструктури, яка повністю відповідає сучасним вимогам, що пред'являються до готельних комплексів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kloster Reute. Franziskanerinnen von Reute. [Електронний ресурс]. – Режим доступу: https://www.kloster-reute.de/.

2. American Hotel & Lodging Association. Hospitality Technology Next Generation (HTNG). [Електронний ресурс]. – Режим доступу: https://www.ahla.com/htng.

3. American Hotel & Lodging Association. Next-Generation Infrastructure Webinar - 2023. [Електронний ресурс]. – Режим доступу: ttps://www.ahla.com/sites/default/files/NGI_Webinar-2023.pdf.

4. Hospitality Technology Next Generation. HTNG Next Generation Infrastructure Technology Guide. [Електронний ресурс]. – Режим доступу: https://www.ahla.com/sites/default/files/HTNG_NGI_Tech_Guide_10.23.pdf.

5. Дегтяренко І.В., Ступак Г.В. Методичні рекомендації до курсового проекту за курсом "Проектування засобів та систем телекомунікаційних мереж" : для студ. заоч. форми навчання за спец. 7.091402 «Телекомунікаційні системи та мережі». Донецьк : ДонНТУ, 2007. 43 с.

6. Гніденко М.П., Вишнівський В.В., Сєрих С.О., Зінченко О.В., Прокопов С.В. Конвергентна мережна інфраструктура : навчальний посібник. Київ : ФОП Гуляєва В.М., 2019. 180 с.

7. Царьов Р.Ю., Нікітюк Л.А., Резніченко П.І. Структуровані кабельні системи : навч. посіб. для студентів вищих навчальних закладів. Одеса : ОНАЗ ім. О.С. Попова, 2013. 260 с.

8. Крилов В.М. Структуровані кабельні системи. Київ : ДУТ, 2015. 112 с.

9. IMC. Технічна стаття. [Електронний ресурс]. – Режим доступу: http://new.imc.ua/blog/teh-statya3/.

10. IEEE 802.11 Working Group. IEEE 802.11. [Електронний ресурс]. – Режим доступу: https://www.ieee802.org/11/.

11. Fiberroad. VLAN Explained: What is VLAN, How Does it Work?.

[Електронний ресурс]. – Режим доступу: https://fiberroad.com/uk/resources/glossary/vlan-explained-what-is-vlan-how-does-it-work/.

12. CQR. Dynamic Host Configuration Protocol (DHCP). [Електронний ресурс]. – Режим доступу: https://cqr.company/ua/wiki/protocols/dynamic-host-configuration-protocol-dhcp/.

13. Вінницький національний технічний університет. 2.4.4. Протоколи та стандарти. [Електронний ресурс]. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/2.4.4.html.

14. Streamtele. IP-телефонія для бізнесу: повне керівництво для новачків. [Електронний ресурс]. – Режим доступу: https://streamtele.com/uk/ip-telefoniya-dlya-biznesa-polnoe-rukovodstvo-dlya-novichkov/.

15. Orhan Ergun. H.323 vs SIP. [Електронний ресурс]. – Режим доступу: https://orhanergun.net/h323-vs-sip.

16. Studfile.net. Лекції з Телекомунікаційних систем та мереж. [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/9962752/page:46/.

17. Ajax Systems. NVR vs DVR: ключові відмінності. [Електронний ресурс]. – Режим доступу: https://ajax.systems/ua/blog/nvr-vs-dvr-key-differences/.

18. ERC. Головна сторінка. [Електронний ресурс]. – Режим доступу: https://erc.ua/.

19. Cisco. Connected Hotel: Value Proposition (PDF). [Електронний ресурс]. – Режим доступу: https://www.cisco.com/web/ME/CCHS/images/cchs_value_proposition.pdf.

20. Molex. Home. [Електронний ресурс]. – Режим доступу: https://www.molex.com/en-us/home.

ДОДАТОК А – Охорона праці

А.1 Аналіз умов праці відділу технічної підтримки.

Відділ технічної підтримки оператора розташований у будівлі. Площа приміщення відділу технічної підтримки складає 50 м^2. Відділ технічної підтримки – сервісна структура, яка займається вирішенням технічних питань роботи мережі, проблем користувачів мережі з комп'ютерним обладнанням (як апаратним так і програмним забезпеченням) та оргтехнікою.

До основних видів діяльності відділу належать: забезпечення безперебійної роботи мережі; налагодження та підтримка мережевого обладнання; підтримка системного програмного забезпечення; забезпечення інформаційної безпеки мережі, контроль доступу, захист від віртуальних атак; підтримка та консультування користувачів мережі з приводу правил експлуатації мережі;

Діяльність працівників відділу напряму пов'язана з роботою на комп'ютерному обладнанні (ноутбук або стаціонарний комп'ютер) та користуванням мобільними телефонами. До основних шкідливих та небезпечних факторів виробничого середовища, пов'язаних з роботою на персональному комп'ютері відповідно ГОСТ 12.0.003-74 ССБТ «Опасные и вредные производственные факторы», НПАОП 0.00–1.28-10 «Правила охорони праці при експлуатації ОМ» належать: напруга зорових органів та пов'язане з нею перевтомлення; значне навантаження на кисті рук та пальці; тривале знаходження в сидячій позі, що викликає застійні явища в організмі; випромінювання різного виду (рентгенівське, електромагнітне, інфрачервоне, статистичні поля); механічні шуми, пов'язані з роботою кулера, дискового приводу, оргтехніки; іонізація повітря; виділення в повітря робочого приміщення різних хімічних речовин (озон, триметілфосфат, біфеніли).

Мобільний телефон є також джерелом електромагнітного випромінювання, на яке організм певним чином реагує. Наукові досліди

підтверджують негативний вплив таких пристроїв на мозок. Але вплив мобільного апарату на організм користувача і досі не є достатньо вивченим.

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

Усі ці фактори негативно впливають на здоров'я працівників відділу технічної підтримки та сприяють виникненню професійних захворювань: комп'ютерний зоровий синдром; радіохвильова хвороба; синдром висихання рогівки ока; кистьовий тунельний синдром; захворювання шкіри; захворювання кишкового тракту;серцево-судинні захворювання.

Негативними наслідками регулярного використання мобільного телефону є ослаблення пам'яті, часті головні болі, зниження уваги, напруга в барабанних перетинках, порушення сну, дратівливість та ін..

А.2 Заходи щодо поліпшення умов праці

Для зменшення шкідливого впливу негативних факторів виробничого середовища на працівників відділу технічної підтримки будуть вжити заходи щодо поліпшення їх умов праці. Розміщення робочих місць з ПК у підвальних приміщеннях та на цокольних поверхах заборонено. Кімната, у якій розташоване робоче місце з ПК має природне освітлення, яке здійснюється через світлові прорізи, орієнтовані переважно на північний схід. Віконні прорізи такого приміщення обладнані регульованими пристроями (жалюзі, завіски, зовнішні козирки). Також приміщення обладнане системою опалення, кондиціонування повітря, або припливно-витяжною вентиляцією для забезпечення оптимальних показників мікроклімату. Загальний контур заземлення будівлі виведений через розетку на кожне робоче місце з ПК. Забороняється для оздоблення інтер'єру приміщень з ПК застосовувати полімерні матеріали (деревинно-стружкові плити, шпалери, що миються,

рулонні синтетичні матеріали, шаруватий паперовий пластик тощо), що виділяють у повітря шкідливі хімічні речовини. У приміщеннях, де розташовано монітори, потрібно виконувати заходи щодо боротьби зі статичним полем. Був використаний спосіб відповідно до рекомендацій, а саме підтримка відносної вологості повітря на рівні 50-60%, заземлення усіх приладів, а також використання для підлоги антистатичного лінолеуму.

Площа на одне робоче місце з ПК відповідно ГОСТ 12.2.032-78, ССБТ. «Рабочее место при выполнении работ сидя. Общие эргономические требования» становить не менше ніж 6,0 $м^2$, а об'єм не менше ніж 20,0 $м^3$. Відстань від робочого місця з ПК до стіни з вікном становить не менше ніж 1,5 м; від інших стін – на відстані 1 м, а відстань між столами – 1,5 м.

Для зменшення шкідливого впливу негативних факторів виробничого середовища робоче місце з ПК відповідає наступним гігієнічним вимогам: екран та клавіатура розташовувані на оптимальній відстані від очей користувача, що становить 600...700 мм; висота робочої поверхні робочого столу є 800 мм; робочий стіл має простір для ніг заввишки не менше ніж 600 мм, завширшки не менше ніж 500 мм, завглибшки (на рівні колін) не менше ніж 450 мм, на рівні простягнутої ноги - ніж 650 мм.

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

Розташування робочих місць з ПК у відділі технічної підтримки згідно ГОСТ зображено на рис. А.1.

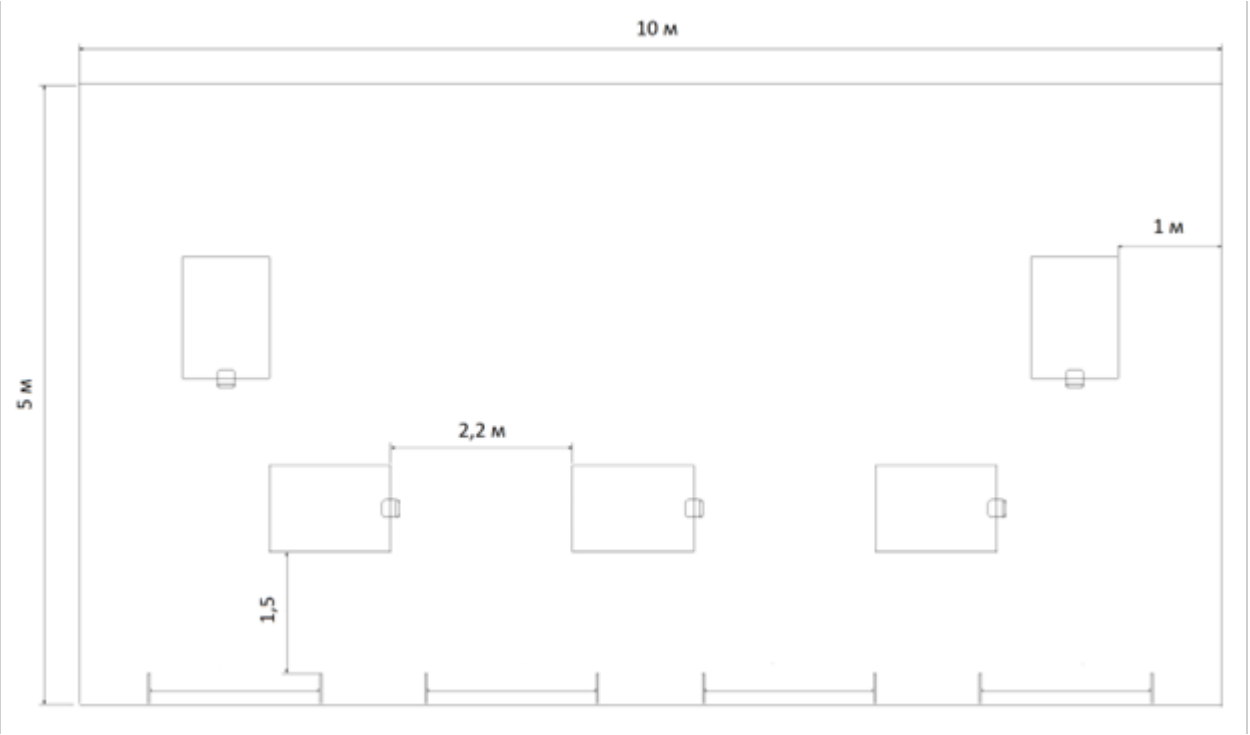

Рисунок А.1 - Облаштованість робочих місць із ПК відділу технічної підтримки

А.2.1 Мікроклімат робочого місця

У приміщенні відділу технічної підтримки є джерела тепловиділення, тому необхідно визначити необхідний умови його вентилювання.

Повітрообмін по теплу визначаємо по формулі:

$$L=\frac{Q_{над}}{c\times p(t_в-t_н)},\ м^3/год, \qquad (А.1)$$

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

с - теплоємкість повітря (0,237 ккал/кг°С);

р - обсягова вага повітря (1,226 кг/ $м^3$);

$t_в$ - температура витяжного повітря (30°С);

$t_н$ - температура приточного повітря (20°с).

Розрахуємо надлишкове надходження тепла за формулою:

$$Q_{над} = Q_{уст} + Q_{пер} + Q_{осв} + Q_{ср}, \quad (А.2)$$

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

$Q_{пер}$ - виділення тепла робітниками;

$Q_{осв}$ - надходження тепла від електричного освітлення;

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

Визначимо виділення тепла від устаткування за формулою:

$$Q_{уст} = P \times K_а \times K_б \times 860, \quad (А.3)$$

$$\text{Де } P = (x_1 \cdot k_1) + (x_2 \cdot k_2) + (x_3 \cdot k_3) + (x_4 \cdot k_4), \quad (А.4)$$

Де х1, х2, х3, х4- кількість системних блоків, моніторів, принтерів, кондиціонерів відповідно;

к1, к2, к3, к4- іх потужність

Р - сумарна потужність устаткування, кВт/год;

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

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

$$Q_{уст} = [(x_1 \cdot k_1) + (x_2 \cdot k_2) + (x_3 \cdot k_3) + (x_4 \cdot k_4)] \cdot K_а \cdot K_б \cdot 860 \text{ ккал/год}.$$

Розрахуємо:

$Q_{уст}$ =((5*0,5)+(5*0,1)+(3*0,6)+(1*10))*0,95*1*860=12092 ккал/год.

Визначимо виділення тепла від обслуговуючого персоналу за допомогою формули:

$$Q_{пер} = n \times g \quad (А.5)$$

де n - кількість працюючих;

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

Розрахуємо:

$Q_{пер}$ =5*100=500 ккал/год.

Визначимо надходження тепла від електричного освітлення за формулою:

$$Q_{осв}=E_м \cdot g_1 \cdot S, \quad (А.6)$$

де $E_м$ - 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.

Розрахуємо:

$Q_{осв}$ = 400*0,05*50=1000 ккал/год.

Визначимо надходження тепла від сонячної радіації через вікна по формулі:

$$Q_{ср} = F \cdot g_2 \cdot K_{осл}, \quad (А.7)$$

де F - площа віконних прорізів (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:

$Q_{ср}$= 8*65*0,4=208 ккал/год.

Визначимо кількість надлишкового тепла:

$Q_{над}$=12092+500+1000+208=13800 ккал/год.

Визначимо витрати повітря в приміщенні:

L=13800/(0,237*1,226)*(30-20)= 4749,42 м^3/год

Існуюча в наявності система кондиціонування і вентилювання має продуктивність 5000 м^3/год, 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 21-23 градуса по Цельсію, 0,1 метра в секунду і 40-60 % відповідно. У теплі періоди року температура повітря повинна складати 22-24 градусів Цельсія, рухливість повітря 0,2 метра за секунду, вологість 40-60 %. Вище зазначені норми цілком відповідають фактичним даним приміщення відділу технічної підтримки.

А.2.2 Розрахунок заземлення загального контуру заземлення будівлі, який повинен бути виведений через розетку на кожне робоче місце з ПК.

Для захисту від пробою напруги на ПК необхідно зробити розрахунок захисного заземлення, припустиме заземлення для устаткування з напругою до 1000 В не повинне перевищувати 4 Ом.

Визначимо розрахунковий опір ґрунту по формулі:

$R_{роз} = R_{зм} \cdot \varphi$,

де $R_{зм}$ - опір ґрунту, $R_{зм}$=100 Ом;

φ - кліматичний коефіцієнт, φ=1,5

$R_{роз}$ = 100*1,5=150 Ом.

Визначимо опір одного заземлювача по формулі:

$$R_0 = \frac{R_{роз}}{2 \cdot \pi \cdot l} \cdot \left(\ln \frac{2 \cdot l}{d} + \frac{1}{2} \cdot \ln \frac{4 \cdot H + l}{4 \cdot H - l} \right),$$

де l - довжина заземлювача, l=3 м;

d - діаметр заземлювача, d=0,12 м;

H - відстань від поверхні до середини заземлювача, H=1.5 м.

R_0=(150/2*3,14*3)*(ln (6/0,12)+1/2*ln (7/5))=32,39 Ом.

Визначимо кількість паралельно з'єднаних заземлювачів:

n= R_0/ $R_{дод} \cdot \eta$,

де η - коефіцієнт використання групового заземлювача, η =0,55.

n=32,39/4*0,55=15.

Визначимо довжину горизонтальної сполучної смуги по формулі:

$l_1=a\cdot(n-1)$,

де a - відстань між заземлювачами, а=4-7 м.

$l_1=6*(15-1)=84$ м.

Визначимо опір сполучної смуги по формулі:

$$R_{см}=(R_{роз}/2\cdot\pi\cdot l_1)\cdot\ln\frac{l_1^2}{d_1\cdot h}$$ Ом.

$R_{см}$=(150/(2*3,14*84))*ln (7056/0,06*0,8)=3,26 Ом.

Де d_1 - товщина смуги (0,06 м);

η см- коефіцієнт використання смуги (0,8);

Підставимо отримані значення й результуючий опір заземлюючого пристрою:

$$R=\frac{R_0\cdot R_{см}}{R_0\cdot\eta_{см}+R_{см}\cdot n\cdot\eta}$$,

де $\eta_{см}$ - коефіцієнт використання смуги, $\eta_{см}$ =0,8.

R=(32,39*3,26)/((32,39*0,8)+(3,93*15*0,8))=1,45 Ом.

Опір 1,45 Ом цілком припустимо.

А.3 Пожежна безпека

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

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

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

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

- 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;

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

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

В даному випадку виробниче приміщення, де розташовані комп’ютери займає площу 50 м^2. Категорія приміщення за вибухопожежною та пожежною небезпекою – В, оскільки в ньому знаходяться тверді горючі матеріали (папір,

меблі, тощо). Клас можливої пожежі – А. Згідно даних це приміщення, з огляду на мінімальне псування комп'ютерної техніки під час гасіння пожежі бажано оснастити двома вуглекислотними вогнегасниками типу ВВ – 5.

А.4 Безпека при надзвичайних ситуаціях

Об'єктом розгляду на предмет визначення надзвичайних небезпек та їх наслідків є електрообладнання. Однією із вірогідних загроз може бути раптове виникнення 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, взаімодію з власним складом пожежних підрозділів, а також застосування схем и засобів пожежогасіння з урахуванням заходів безпеки.

Корпус обладнаний 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 розташовані таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (шириною не менше 1 м). Евакуаційні шляхи і виходи необхідно постійно держуться вільними, нічим не захарашовані. Засоби протипожежного захисту в приміщеннях тримаються 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 його розвитку випромінюється тепло, накопичуються токсичні продукти згоряння, імовірні руйнування будівельних споруд. Тому слід як можна швидше провести евакуацію людей із палаючої будівлі. Показником ефективності евакуації є час, протягом якого працівники можуть при 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 у будівлі - два. Вони розташовувані розосереджено. Мінімальна відстань l між найбільш віддаленими один від одного евакуаційними виходами із приміщення визначається за формулою:

$$l=1{,}5\sqrt{P}\,,$$

де Р – периметр приміщення, м.

$l=1{,}5\sqrt{30}$ = 5,47 м

Двері на шляхах евакуації відкриваються у напрямку виходу із будівлі (приміщення). У кожному приміщенні на видному місці є вивішений план евакуації при пожежі. При пожежі обов'язково необхідно враховувати небезпечні чинники і механізм їх дії на людину. При виникненні пожежі, після виклику пожежної охорони, необхідно попередити про це усіх, хто знаходиться поруч, після чого евакуюватися самому і по можливості допомогти евакуюватися іншим, 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 під 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 людина знаходиться в приміщенні де немає пожежі, но відрізана вогнем, димом, високою температурою від головних шляхів евакуації, то в першу чергу необхідно заважити доступу диму и продуктів горіння в це приміщення. Для чого необхідно негайно закрити усі щілини у дверях та під ними змоченими водою ганчірками, рушниками, робочими халатами та інш.

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 звернути на себе увагу. Ніколи не можна стрибати через вікно без відомої на це необхідності (кожний другий стрибок з 4-г поверху при пожежі смертельний).

Висновки

В наведеній главі дипломного проекту розроблений комплекс заходів з охорони праці та безпеки в надзвичайних ситуаціях. Був проведений аналіз умов праці відділу технічної підтримки, розроблені заходи щодо поліпшення умов праці, а саме мікроклімату робочого місця, облаштування робочого кабінету. Проведений розрахунок контуру заземлення робочого місця. Розроблені заходи з пожежної безпеки та в випадку надзвичайних ситуацій.

ДОДАТОК Б – Графічний матеріал

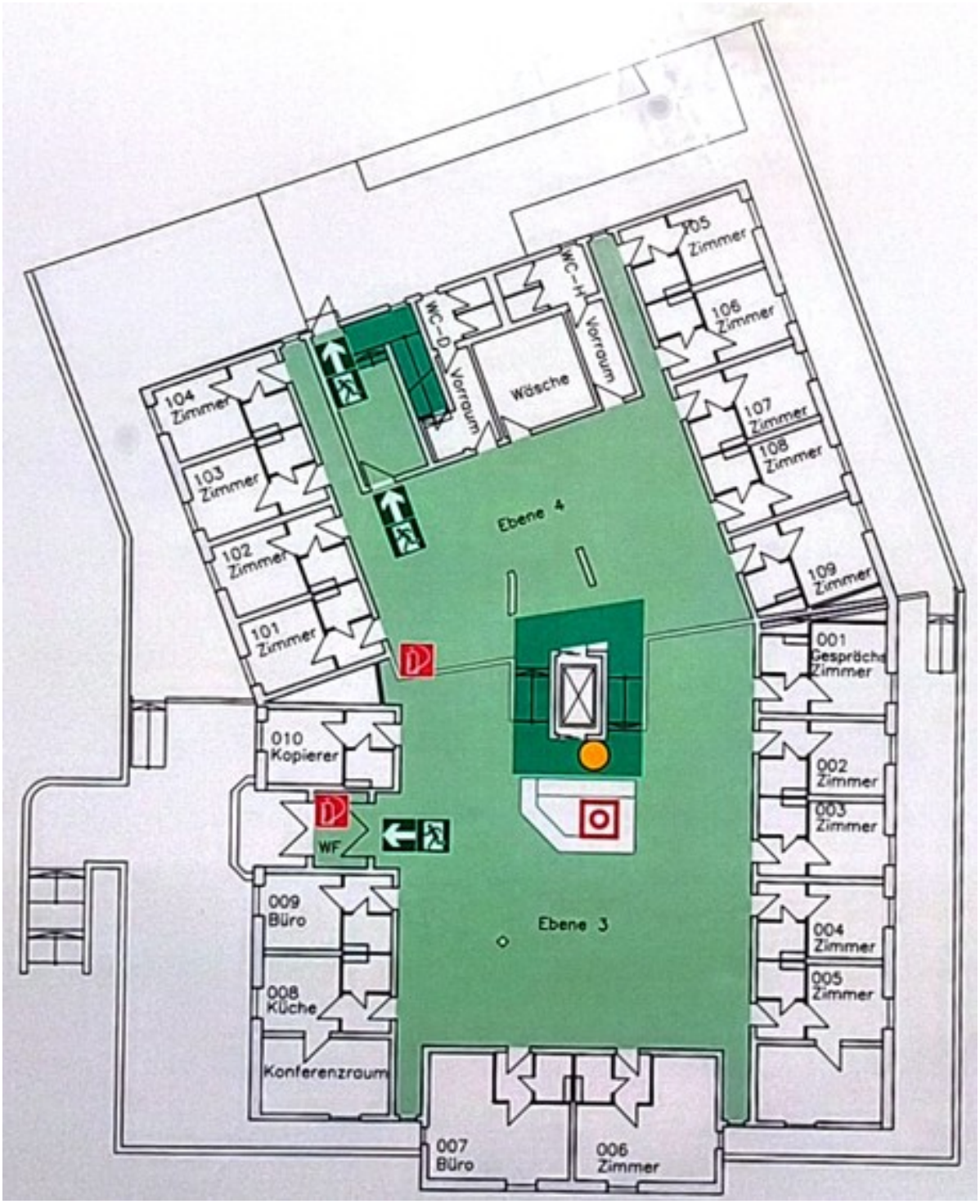

Рисунок Б.1 – План першого поверху

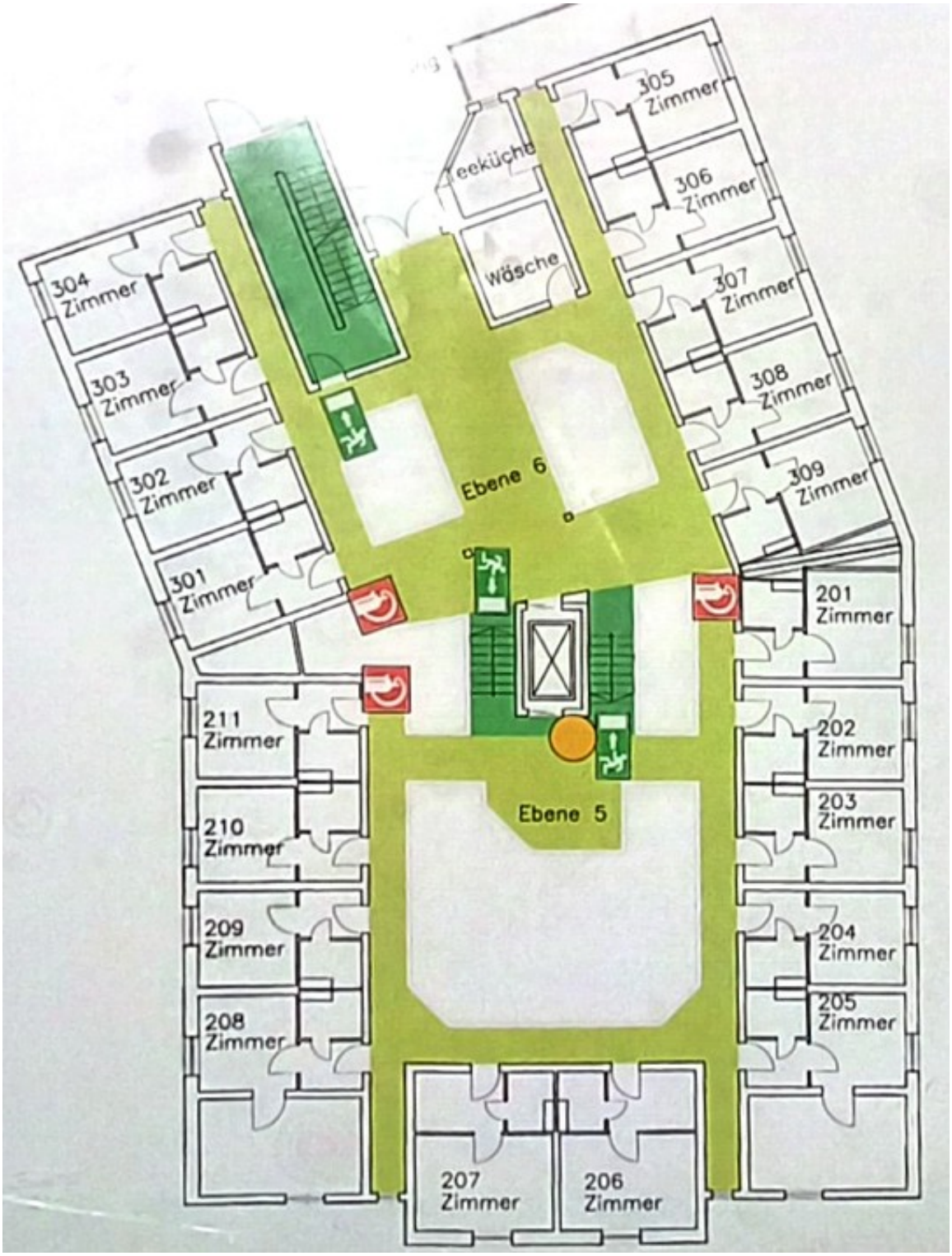

Рисунок Б.2 – План другого та третього поверхів

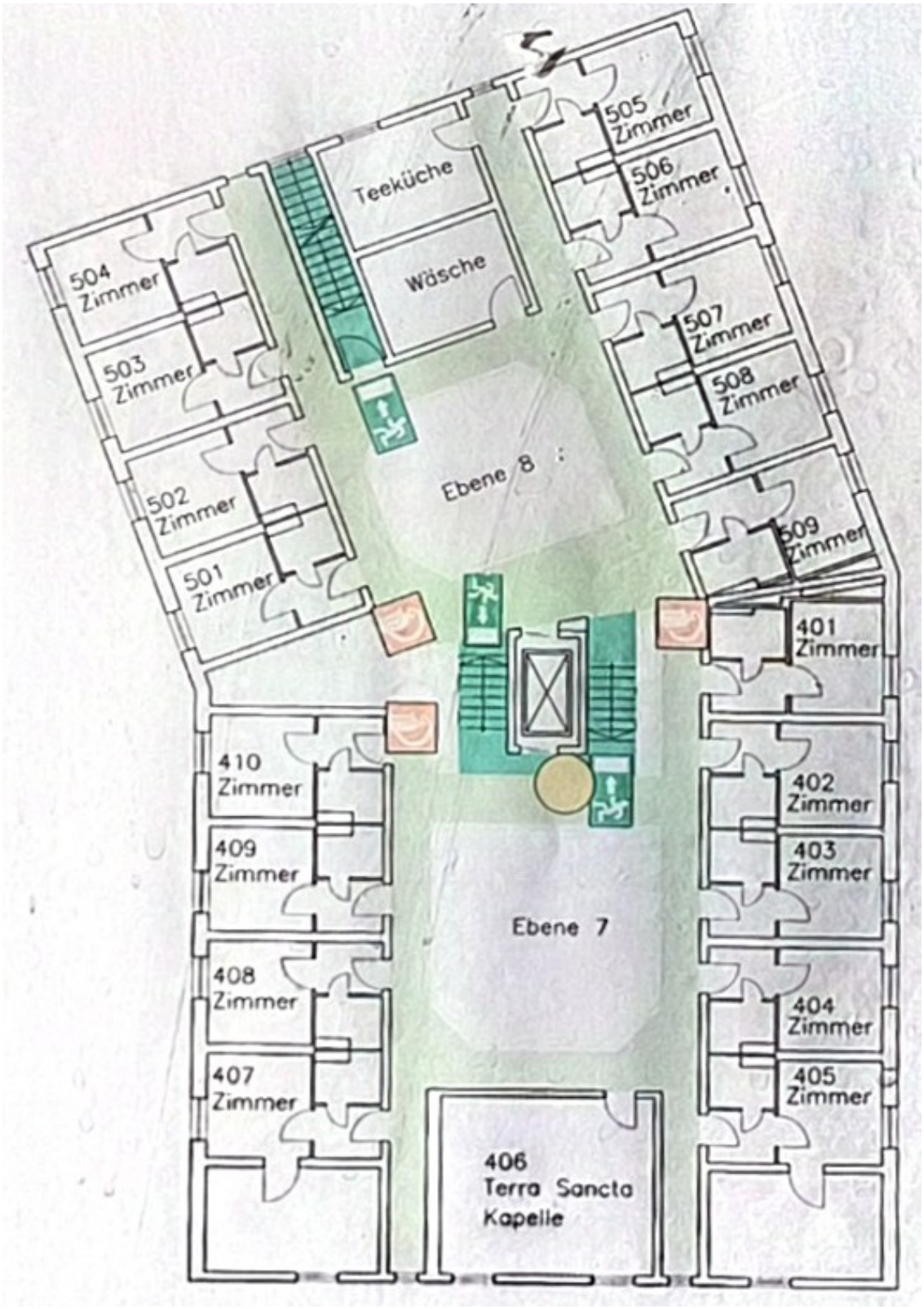

Рисунок Б.3 – План четвертого та п’ятого поверхів

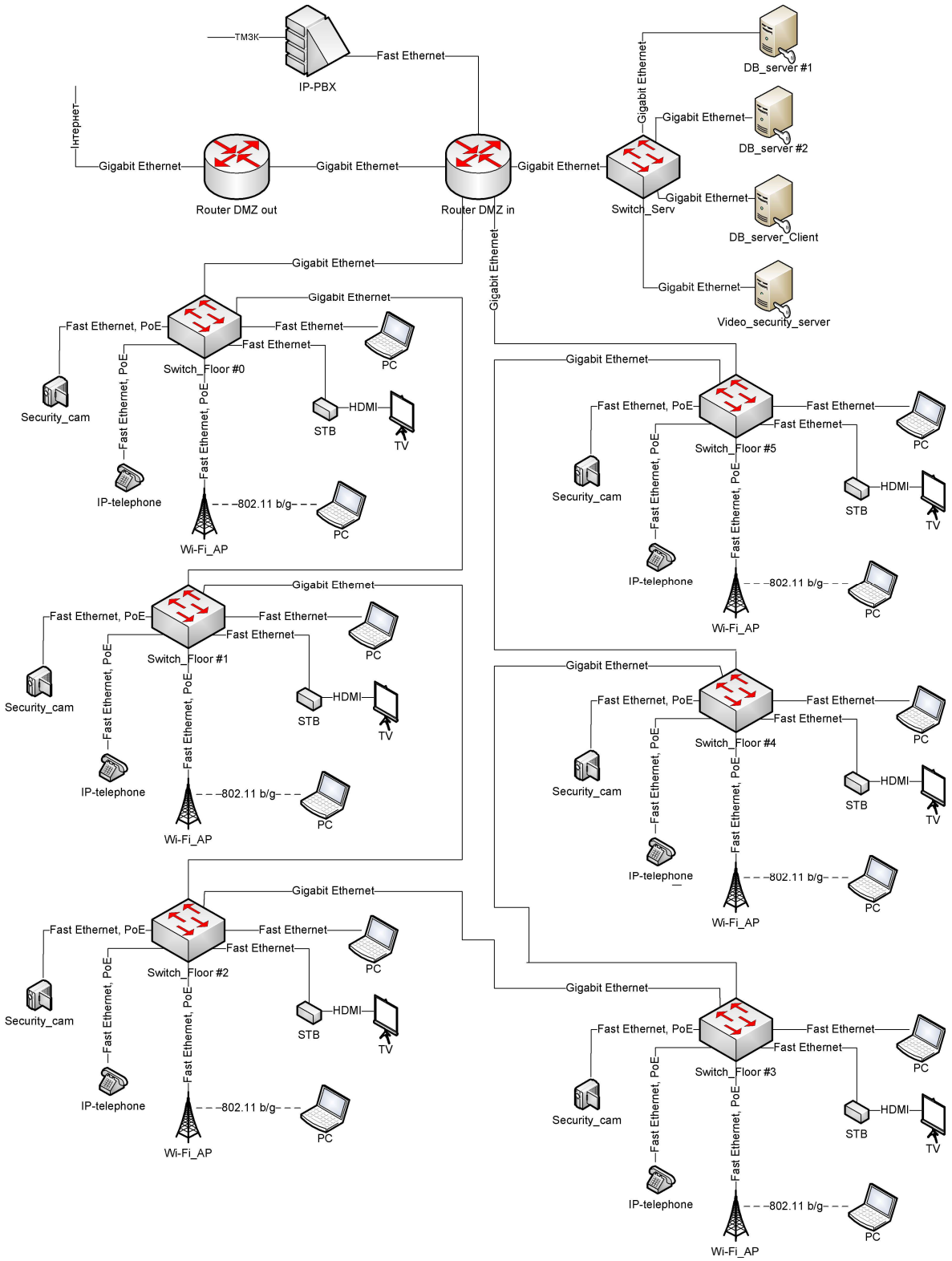

Рисунок Б.4 – Структурна схема мережі

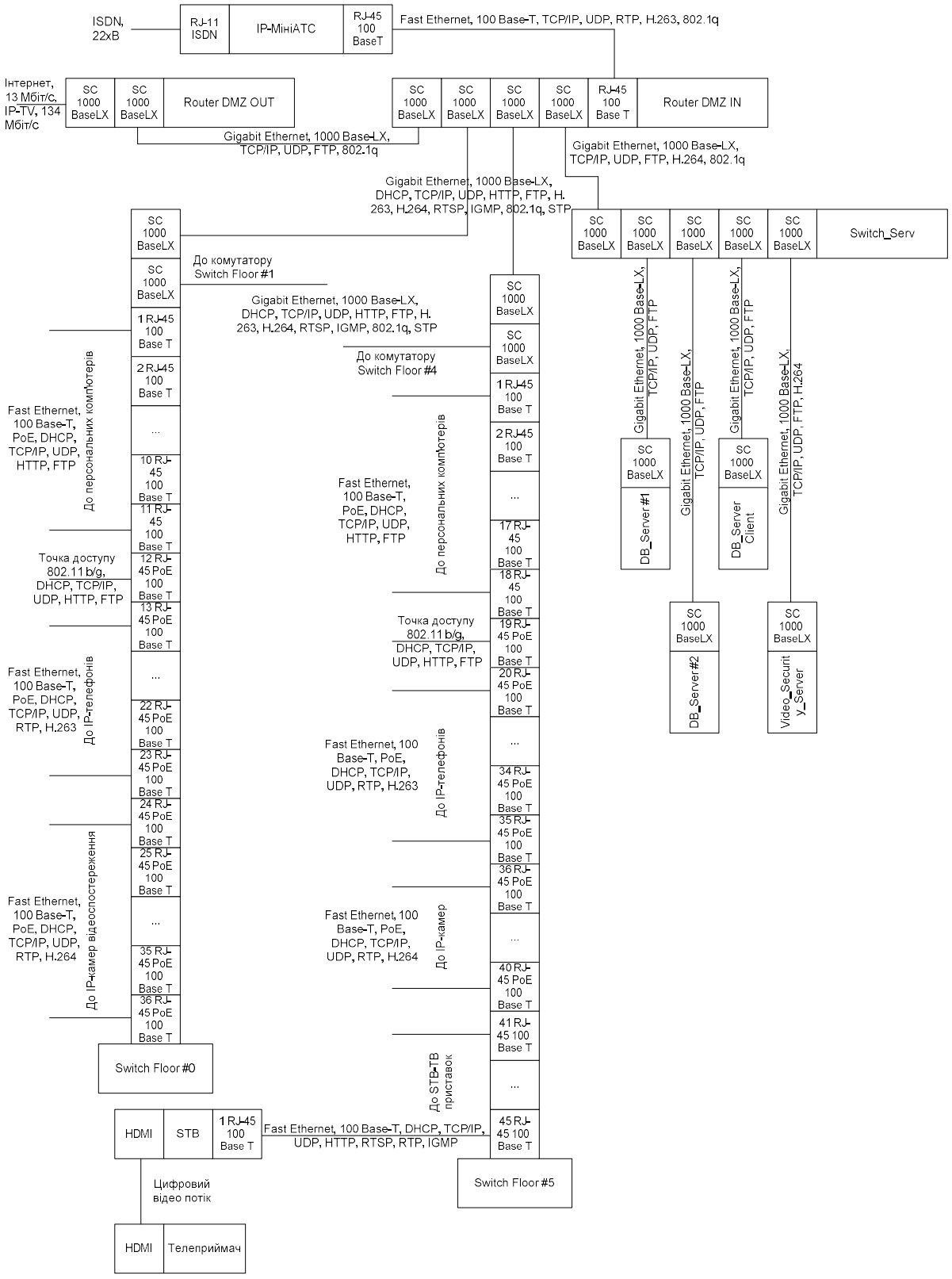

Рисунок Б.5 – Функціональна схема мережі

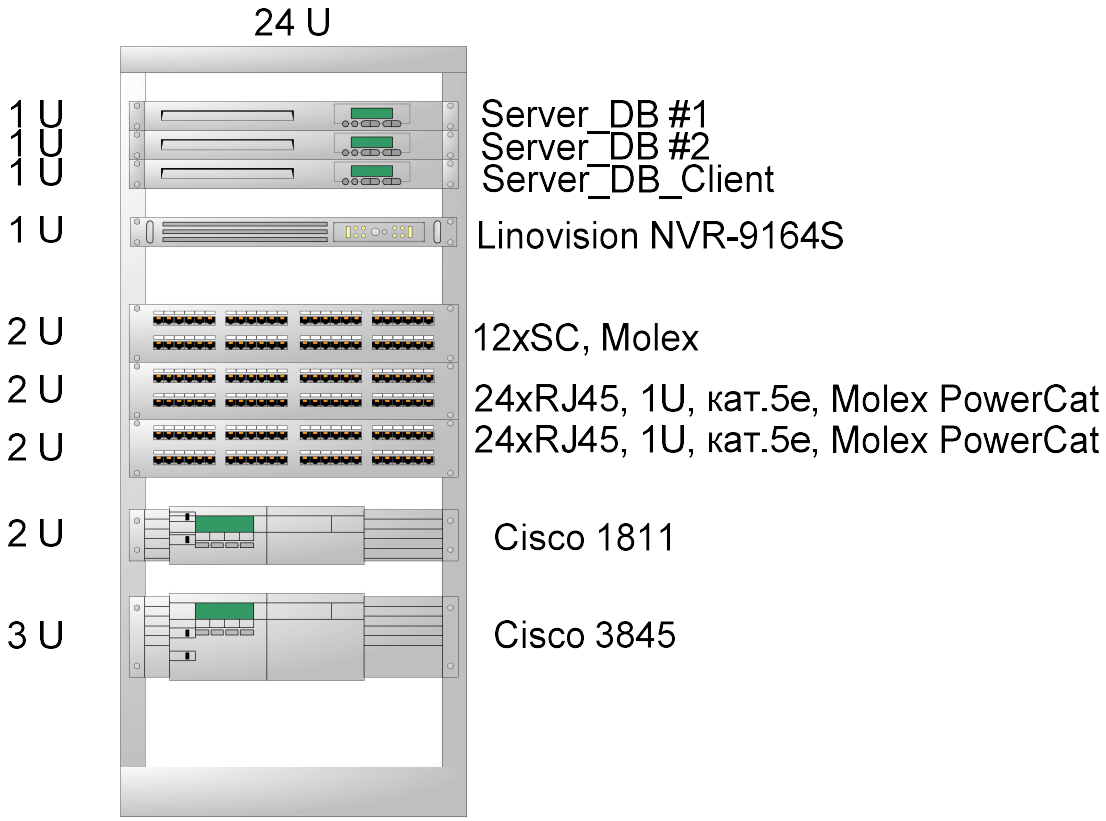

Рисунок Б.6 – Схема розміщення обладнання

Рисунок Б.7 – Схема з’єднань