Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»
(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем
(назва відділення)

Циклова комісія комп'ютерної інженерії
(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра
(освітній ступінь)

на тему: **Розробка проєкту комп'ютерної мережі ПП «УК «ЖИТЛОФОНД»**

Виконав: студент VII курсу, групи КІб-703

Спеціальності **123 Комп'ютерна інженерія**
(шифр і назва спеціальності)

_____ Павло ВІЦЕНТИЙ
(ім'я та прізвище)

Керівник Володимир ШТОКАЛО
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2026

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітній ступінь бакалавр
Освітньо-професійна програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
Галузь знань: 12 Інформаційні технології

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"18" травня 2026 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Віцентому Павлу Романовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи **Розробка проєкту комп'ютерної мережі ПП «УК «ЖИТЛОФОНД»**

керівник роботи Штокало Володимир Ярославович
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 18.05.2026р №4/9-252.

2. Строк подання студентом роботи: 22 червня 2026 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Безпека життєдіяльності, основи охорони праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): План приміщень. Логічна топологія. Фізична топологія. Таблиця IP-адрес. Таблиця техніко-економічних показників. Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Ірина ЛЕЩИК методист, викладач		
Безпека життєдіяльності, основи охорони праці	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	18.05	
2	Збір і узагальнення інформації	21.05	
3	Написання першого розділу	25.05	
4	Розробка технічного та робочого проекту	1.06	
5	Написання спеціального розділу	8.06	
6	Розрахунок економічної частини	11.06	
7	Написання розділу охорони праці	12.06	
8	Виконання графічної частини	14.06	
9	Оформлення проекту	18.06	
10	Погодження нормоконтролю	19.06	
11	Попередній захист роботи	22.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 18 травня 2026 року

Студент _____ Павло ВІЦЕНТИЙ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Володимир ШТОКАЛО
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Віцентий П. Р. Розробка проєкту комп'ютерної мережі ПП «УК «ЖИТЛОФОНД»: кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. 118 с.

У кваліфікаційній роботі розроблено та обґрунтовано проєкт корпоративної інформаційно-обчислювальної мережі для ПП «УК «ЖИТЛОФОНД» із використанням сучасного мережевого обладнання DrayTek, серверних рішень Synology та систем відеоспостереження TVT. У роботі виконано проєктування мережевої інфраструктури з логічною сегментацією на основі VLAN, реалізовано апаратну L3-маршрутизацію, відмовостійке підключення до мережі Інтернет за технологією Dual WAN, безшовну бездротову мережу Wi-Fi та централізовану систему зберігання даних із резервним копіюванням і захистом від втрати інформації. Також розроблено систему мережевої та фізичної безпеки, що включає розмежування доступу, міжмережевий екран і ізольовану мережу відеоспостереження. Результати роботи підтверджують технічну та економічну доцільність впровадження запропонованої мережевої інфраструктури, яка відповідає сучасним вимогам продуктивності, масштабованості, відмовостійкості та інформаційної безпеки.

Ключові слова: корпоративна мережа, VLAN, L3-маршрутизація, DrayTek, Synology, NAS, Dual WAN, Wi-Fi Mesh, інформаційна безпека, відеоспостереження.

ANNOTATION

Pavlo VITSENTYI. Computer Network Project Development for PJSC «Property Management Company «ZHYTLOFOND»: qualification work for obtaining a Bachelor's degree in Computer Engineering. Ternopil: SSS «TPC TNTU», 2026. 118 p

In this qualification thesis, a project for a corporate information and computing network for the private enterprise "Management Company 'ZHYTLOFOND'" has been developed and substantiated, utilizing modern DrayTek network equipment, Synology server solutions, and TVT video surveillance systems. The thesis presents the design of a network infrastructure with logical segmentation based on VLANs, and implements hardware-based L3 routing, a fault-tolerant Internet connection via Dual WAN technology, a seamless Wi-Fi wireless network, and a centralized data storage system with data backup and loss protection. Additionally, a network and physical security system has been developed, which includes access control, a firewall, and an isolated video surveillance network. The results of the work confirm the technical and economic feasibility of implementing the proposed network infrastructure, which meets modern requirements for performance, scalability, fault tolerance, and information security.

Keywords: corporate network, VLAN, L3 routing, DrayTek, Synology, NAS, Dual WAN, Wi-Fi Mesh, information security, video surveillance.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

ДБЖ- джерело безперебійного живлення;

ІКС – інформаційно-комунікаційна система;

ІС – інформаційні ситеми

ІТ – інформаційні технології;

КМ – комп’ютерна мережа;

ЛОМ- локальна обчислювальна мережа;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ПП – приватне підприємство;

СКС – структурована кабельна система;

ТО – технічне обслуговування;

УК – управлінська компанія;

PoE – Power over Ethernet.

ВСТУП

У сучасних умовах діяльність підприємств, що займаються обслуговуванням житлового фонду, дедалі більше залежить від ефективного використання ІТ. Керуючі компанії, житлово-експлуатаційні організації та підприємства з обслуговування будинків щоденно працюють із великим обсягом інформації: зверненнями мешканців, аварійними заявками, абонентськими даними, фінансовими документами, договорами, технічною документацією, актами виконаних робіт, планами ремонтів та службовою кореспонденцією. Для якісного виконання цих завдань необхідна надійна комп'ютерна мережа, яка забезпечує швидкий обмін даними між підрозділами, доступ до спільних ресурсів і стабільну роботу ІС.

Особливе значення комп'ютерні мережі мають для диспетчерських та аварійно-ремонтних служб. Саме ці підрозділи забезпечують приймання, реєстрацію та координацію виконання заявок мешканців, у тому числі аварійних. Стабільна робота мережі дозволяє швидко передавати інформацію між диспетчерським центром, технічними службами, головним інженером, абонентським відділом і керівництвом підприємства. Це скорочує час реагування на аварійні ситуації, підвищує контроль за виконанням робіт і покращує якість обслуговування житлового фонду.

Не менш важливою є роль комп'ютерної мережі у фінансовій та адміністративній діяльності підприємства. Бухгалтерія, головний бухгалтер, абонентський відділ, юрисконсульт і керівництво працюють із фінансовими, персональними та службовими даними, які потребують захисту, резервного копіювання та розмежування доступу. Тому проєктування комп'ютерної мережі повинно враховувати не лише потребу в підключенні робочих місць, а й вимоги до інформаційної безпеки, логічної сегментації мережі, контролю доступу, захисту від несанкціонованих підключень і збереження важливої інформації.

Актуальність розробки проєкту комп’ютерної мережі для ПП «УК «ЖИТЛОФОНД» зумовлена необхідністю створення сучасної, безпечної та масштабованої мережевої інфраструктури, здатної забезпечити ефективну роботу всіх структурних підрозділів підприємства. Її впровадження сприяє підвищенню оперативності роботи, покращенню якості обслуговування мешканців, захисту службової інформації, зменшенню витрат на адміністрування та створенню умов для подальшої цифровізації підприємства.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування об’єкта проєктування

Об’єктом проєктування є локальна комп’ютерна мережа адміністративно-технічного приміщення ПП «УК «ЖИТЛОФОНД».

Оскільки підприємство виконує функції керуючої компанії у сфері житлово-комунального господарства, його щоденна робота пов’язана з обробкою звернень громадян, веденням абонентського обліку, фінансових документів, технічної документації, аварійних заявок, договорів, актів виконаних робіт та внутрішньої службової інформації. Для ефективної роботи цих процесів необхідна надійна комп’ютерна мережа, яка об’єднає робочі місця працівників у єдину інфраструктуру.

1.1.2 Призначення комп’ютерної мережі

Комп’ютерна мережа ПП «УК «ЖИТЛОФОНД» призначена не лише для фізичного з’єднання комп’ютерів, а й для забезпечення повноцінної цифрової інфраструктури підприємства. Вона є основою для роботи інформаційних систем, електронного документообігу, диспетчеризації, фінансового обліку, технічного супроводу житлового фонду та безпечної взаємодії всіх структурних підрозділів.

Упровадження комп’ютерної мережі забезпечить:

- підвищення швидкості обробки звернень громадян;
- скорочення часу передавання заявок між підрозділами;
- підвищення якості роботи диспетчерського центру;
- централізацію зберігання службової інформації;
- підвищення рівня захисту даних;
- зручне використання мережевих принтерів і спільних ресурсів;

- можливість підключення відеоспостереження;
- спрощення адміністрування комп’ютерів і мережевого обладнання;
- підготовку підприємства до подальшої цифровізації.

1.1.3 Вимоги до комп’ютерної мережі ПП «УК «ЖИТЛОФОНД»

1.1.3.1 Загальні вимоги до КМ

Комп’ютерна мережа підприємства повинна відповідати таким вимогам:

1. Надійність: мережа має забезпечувати стабільну роботу основних підрозділів підприємства, особливо диспетчерського центру, аварійно-ремонтної служби, бухгалтерії та абонентського відділу.

2. Продуктивність: пропускна здатність мережі повинна бути достатньою для роботи офісних програм, електронного документообігу, доступу до баз даних, мережевих принтерів.

3. Безпека: необхідно передбачити розмежування доступу між підрозділами, захист від несанкціонованого підключення, використання паролів, мережевих політик, міжмережевого екрана та резервного копіювання важливих даних.

4. Масштабованість: мережа повинна мати резерв портів і можливість підключення нових робочих місць, додаткових точок доступу, камер відеоспостереження та іншого обладнання.

5. Керованість: мережеве обладнання має бути зосереджене в телекомунікаційній кімнаті, що забезпечить зручне адміністрування, контроль стану мережі та швидке усунення несправностей.

6. Сегментація: для підвищення безпеки та зручності адміністрування доцільно розділити мережу на логічні сегменти: адміністративний,

фінансовий, клієнтський, технічний, IT-сегмент, гостьовий Wi-Fi, відеоспостереження та службові системи [5].

1.1.3.2 Вимоги до СКС

Для побудови горизонтальної кабельної системи необхідно використовувати мідний кабель типу вита пара категорії не нижче Cat.6. Для підключення обладнання з підтримкою швидкостей вище 1 Гбіт/с або для створення запасу на майбутнє допускається використання кабелю Cat.6A.

Горизонтальні кабельні лінії повинні прокладатися від телекомунікаційної кімнати до інформаційних розеток у приміщеннях підприємства.

Вимоги:

- у кожному приміщенні має бути передбачений щонайменше один резервний інформаційний порт RJ-45;
- для мережевих принтерів, багатофункціональних пристроїв, камер і точок Wi-Fi передбачити окремі лінії;
- кабельні лінії повинні мати маркування з обох боків;
- кабелі повинні завершуватися на патч-панелях у телекомунікаційній шафі;
- кабелі повинні завершуватися зовнішніми інформаційними розетками RJ-45 на робочих місцях;
- прокладання кабелю повинно виконуватися в кабель-каналах, лотках, гофротрубах або інших захищених трасах;
- силові та слабкострумові кабелі необхідно прокладати окремо з дотриманням безпечної відстані або з фізичним розділенням;
- усі кабельні лінії, розетки, патч-панелі та порти комутаторів повинні бути промарковані за єдиною системою [6].

1.1.4 Вимоги до технічної і проєктної документації

Документація на проєктовану комп'ютерну мережу повинна забезпечувати повне й однозначне відображення прийнятих технічних рішень, структури мережі, складу обладнання, параметрів кабельної системи, логічної організації мережевих сегментів, вимог до інформаційної безпеки, електроживлення, монтажу, тестування та подальшої експлуатації. Проєктна документація має бути достатньою для виконання монтажних робіт, налаштування активного мережевого обладнання, перевірки працездатності мережі, її приймання в експлуатацію та подальшого адміністрування IT-відділом підприємства.

До складу документації повинна входити пояснювальна записка, у якій необхідно подати загальну характеристику підприємства, призначення комп'ютерної мережі, обґрунтування необхідності її створення, опис організаційної структури підприємства, перелік підрозділів і приміщень, що підлягають підключенню, а також основні технічні рішення щодо побудови мережі. У пояснювальній записці слід навести прийняту топологію мережі, принцип централізованої комутації через телекомунікаційну кімнату, обґрунтування вибору структурованої кабельної системи, активного мережевого обладнання, технологій Ethernet, Wi-Fi, VLAN, відеоспостереження та засобів захисту інформації.

Графічна частина документації повинна містити план приміщень із нанесеними робочими місцями, інформаційними розетками, точками підключення мережевих принтерів, камер відеоспостереження, точок бездротового доступу та іншого мережевого обладнання. На плані необхідно відобразити розташування телекомунікаційної кімнати, комутаційної шафи, основних кабельних трас, місць проходу кабелю між приміщеннями, а також умовні позначення всіх елементів мережевої інфраструктури. Усі позначення на планах повинні бути уніфікованими й відповідати прийнятій системі маркування.

У складі документації необхідно передбачити логічну схему мережі, у якій слід описати поділ мережі на функціональні сегменти. Для підрозділів підприємства доцільно передбачити окремі логічні сегменти або VLAN: адміністративний, фінансовий, клієнтський, технічний, диспетчерський, IT-сегмент, сегмент серверного та мережевого обладнання, сегмент відеоспостереження та гостьовий Wi-Fi. У логічній схемі необхідно зазначити правила взаємодії між сегментами, порядок маршрутизації, обмеження доступу, а також принципи захисту критичних підрозділів, зокрема бухгалтерії, абонентського відділу, диспетчерського центру та IT-відділу.

Документація повинна містити таблицю IP-адресації, у якій зазначаються діапазони адрес для кожного мережевого сегмента, адреси шлюзів, серверів, мережевого обладнання, принтерів, IP-камер, точок доступу та інших пристроїв зі статичною адресацією. Окремо слід визначити діапазони адрес, що видаються DHCP-сервером, а також адреси, зарезервовані для службового обладнання. Таблиця IP-адресації має бути побудована так, щоб забезпечити зручність адміністрування, можливість масштабування мережі та швидку ідентифікацію пристроїв за належністю до відповідного підрозділу або VLAN.

Обов’язковою частиною документації має бути таблиця комутації портів. У ній необхідно вказати відповідність між номером порту на патч-панелі, номером порту комутатора, номером інформаційної розетки, приміщенням, робочим місцем, типом підключеного обладнання та відповідним VLAN. Така таблиця повинна використовуватися під час монтажу, налагодження, експлуатації та пошуку несправностей у мережі. Усі порти патч-панелей, комутаторів, розеток і кабельних ліній повинні мати унікальне маркування, яке збігається з позначеннями в документації.

Окремо має бути розроблена специфікація обладнання та матеріалів. У ній необхідно вказати найменування, основні технічні характеристики, кількість і призначення кожної позиції: телекомунікаційної шафи, патч-панелей, кабелю типу вита пара, інформаційних розеток, патч-кордів,

кабельних органайзерів, комутаторів, PoE-комутаторів, маршрутизатора або міжмережевого екрана, точок доступу Wi-Fi, джерел безперебійного живлення, сервера або NAS, IP-камер, відеореєстратора та допоміжних монтажних матеріалів. Специфікація повинна бути достатньо деталізованою для закупівлі обладнання та перевірки його відповідності вимогам проєкту.

Документація повинна містити схему розміщення обладнання в телекомунікаційній шафі. На ній необхідно показати порядок встановлення патч-панелей, комутаторів, маршрутизатора або міжмережевого екрана, UPS, кабельних органайзерів, сервера або мережевого сховища, а також інших пристроїв. Така схема потрібна для правильного монтажу, забезпечення охолодження обладнання, зручної комутації, технічного обслуговування та подальшого розширення мережі.

Проєктна документація повинна містити розділ з інформаційної безпеки. У ньому необхідно описати принципи розмежування доступу між підрозділами, правила міжмережевої взаємодії, використання VLAN, політики паролів, обмеження адміністративного доступу до мережевого обладнання, порядок використання VPN, захист бездротової мережі, ізоляцію гостьового Wi-Fi, резервне копіювання конфігурацій та журналювання подій. Окрему увагу слід приділити захисту фінансових, персональних, юридичних і диспетчерських даних, оскільки саме ці категорії інформації є критичними для діяльності підприємства.

У документації також необхідно передбачити розділ з резервного копіювання та відновлення. У ньому слід визначити перелік даних, які підлягають резервному копіюванню, періодичність створення копій, місця зберігання резервних копій, відповідальних осіб, порядок перевірки резервних копій і процедуру відновлення роботи після збою. До резервного копіювання мають належати службові документи, бухгалтерські дані, абонентські бази, юридичні матеріали, технічна документація, конфігурації мережевого обладнання та інші критично важливі ресурси.

Обов’язковим є розділ з тестування та приймання комп’ютерної мережі. У ньому потрібно визначити перелік перевірок, які виконуються після монтажу: тестування кабельних ліній, перевірка правильності маркування, перевірка працездатності інформаційних розеток, доступу до Інтернету, роботи VLAN, Wi-Fi, відеоспостереження, мережевих принтерів, резервного живлення та правил доступу між сегментами. Результати тестування повинні оформлюватися протоколами або актами, які підтверджують відповідність реалізованої мережі проєктним рішенням.

Проєктна документація повинна містити інструкції з експлуатації та адміністрування мережі. У них необхідно описати порядок підключення нових робочих місць, внесення змін до таблиці комутації, створення нових облікових записів, адміністрування VLAN, оновлення мережевого обладнання, резервного копіювання конфігурацій, моніторингу стану мережі та реагування на несправності. Такі інструкції потрібні для IT-відділу підприємства і дозволяють підтримувати мережу в актуальному та працездатному стані.

Усі документи повинні мати єдину систему нумерації, назви, дати створення, версії, відомості про розробника та погодження із замовником. У разі внесення змін до мережевої інфраструктури документація повинна оновлюватися, а попередні версії зберігатися для історії змін. Актуальність документації є важливою умовою безпечної експлуатації комп’ютерної мережі, оскільки невідповідність фактичної конфігурації мережі проєктним матеріалам ускладнює адміністрування, пошук несправностей і контроль доступу.

Документація повинна надаватися замовнику в паперовому та електронному вигляді. Електронна версія повинна містити редаговані файли схем, таблиць і текстових документів, а також копії у форматі PDF для перегляду й архівного зберігання. Усі електронні файли повинні мати зрозумілі назви, структуру каталогів і відповідати затвердженому складу проєктної документації. Це забезпечить можливість подальшого оновлення,

супроводу та розвитку комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» [1]; [9]; [5].

1.1.5 Техніко-економічні показники проєктованої КМ

Техніко-економічні показники проєктованої комп'ютерної мережі характеризують ефективність прийнятих технічних рішень, доцільність використання обраного обладнання, рівень надійності, масштабованості, безпеки та економічної обґрунтованості створення мережевої інфраструктури.

Техніко-економічна ефективність проєкту досягається за рахунок раціонального вибору топології, централізованого розміщення обладнання, використання стандартної кабельної системи, резервування портів, логічної сегментації мережі, впровадження засобів захисту та можливості подальшого масштабування. Такий підхід забезпечує баланс між вартістю реалізації, технічною надійністю, зручністю експлуатації та потребами підприємства.

Економічна доцільність проєкту полягає в тому, що впровадження єдиної комп'ютерної мережі дозволяє централізувати доступ до інформаційних ресурсів, зменшити дублювання обладнання, спростити обслуговування робочих місць, скоротити час обміну інформацією між підрозділами та підвищити швидкість обробки звернень громадян. Завдяки використанню мережевих принтерів, спільних файлових ресурсів, централізованого резервного копіювання та єдиної точки адміністрування зменшуються експлуатаційні витрати підприємства.

Важливим економічним показником є співвідношення вартості обладнання та функціональних можливостей мережі. Для підприємства такого типу доцільно використовувати керовані комутатори середнього класу з підтримкою VLAN, PoE для точок доступу та камер, маршрутизатор або міжмережевий екран із базовими функціями захисту, а також кабельну систему Cat.6. Такий підхід дозволяє не переплачувати за надлишкові

можливості, але забезпечує достатній рівень продуктивності, безпеки та масштабованості.

Наведені у таблиці 1.1 техніко-економічні показники є проєктними та можуть уточнюватися чи коригуватися на етапі вибору конкретного обладнання, визначення фактичної кількості робочих місць, погодження провайдерів Інтернету, розрахунку Wi-Fi-покриття та остаточного формування специфікації. Основним принципом вибору технічних характеристик є забезпечення балансу між продуктивністю, надійністю, інформаційною безпекою, масштабованістю та економічною доцільністю впровадження комп'ютерної мережі.

Таблиця 1.1 – Проєктні техніко-економічні показники КМ

Показник	Проєктне значення
1	2
Тип мережі	Локальна комп'ютерна мережа підприємства
Топології мережі	Гібридна топологія: дротова частина будується за принципом «зірка» з центральним вузлом у телекомунікаційній кімнаті; бездротовий сегмент реалізується через точки доступу Wi-Fi; логічний поділ мережі виконується за допомогою VLAN
Центральний вузол мережі	Телекомунікаційна кімната з телекомунікаційною шафою
Тип кабельної системи	СКС на основі витої пари Cat.6
Резерв на модернізацію кабельної системи	Можливість використання Cat.6A для магістральних або перспективних високошвидкісних підключень
Основна технологія дротової мережі	Ethernet 1000BASE-T

Продовження таблиці 1.1

1	2
Швидкість підключення робочих місць	1 Гбіт/с
Швидкість підключення сервера або NAS	1 Гбіт/с, бажано 2×1 Гбіт/с з агрегацією каналів або 10 Гбіт/с за потреби
Рівень комутації	Для маршрутизації між VLAN — L2+ або L3-комутатор
Швидкість магістральних з’єднань	1–10 Гбіт/с залежно від обраного обладнання
Логічна сегментація мережі VLAN	ADMIN: адміністрація, ACCOUNTING: бухгалтерія, CLIENT_SERVICE: клієнтський блок, TECHNICAL: технічний блок, DISPATCH: диспетчерський сегмент, IT: IT-сегмент, SERVERS: серверне обладнання, VIDEO_REC: відеоспостереження, GUEST_WIFI: гостьовий Wi-Fi
Підтримка PoE	PoE / PoE+ для точок доступу Wi-Fi та IP-камер
Рекомендований стандарт Wi-Fi	Wi-Fi 6 / IEEE 802.11ax
Практична швидкість для користувача Wi-Fi	Орієнтовно 300–500 Мбіт/с залежно від відстані, перешкод і кількості клієнтів
Частотні діапазони Wi-Fi	2,4 ГГц і 5 ГГц
Захист Wi-Fi	WPA2/WPA3, окремі SSID для службової та гостьової мереж
Кількість провайдерів Інтернету	Рекомендовано 2: основний дротовий провайдер і резервний провайдер

Продовження таблиці 1.1

1	2
Підключення до Інтернету	Через маршрутизатор або міжмережевий екран
Тип підключення основного провайдера	Оптичне підключення Ethernet / GPON / FTTx
Швидкість основного каналу Інтернету	Рекомендовано не менше 500 Мбіт/с, оптимально — 1 Гбіт/с
Тип підключення резервного провайдера	Другий дротовий канал або мобільний LTE/5G-резерв
Швидкість резервного каналу Інтернету	50–100 Мбіт/с для підтримки критичних сервісів у разі відмови основного каналу
Відеоспостереження	IP-камери з підключенням до окремого VLAN
Швидкість IP-камер	1 Гбіт/с
Резервне живлення	UPS
Орієнтовний час автономної роботи UPS	15–30 хвилин для підтримки роботи критичного обладнання або коректного завершення процесів
Економічна пропозиція	850 тис. грн.

1.1.6 Стадії та етапи розробки проєкту комп’ютерної мережі

Розробка проєкту комп’ютерної мережі ПП «УК «ЖИТЛОФОНД» повинна виконуватися поетапно, з послідовним переходом від аналізу вихідних даних до формування технічних рішень, підготовки проєктної документації, монтажу, налаштування, тестування та введення мережі в експлуатацію (див. рис. 1.1). Такий підхід дозволяє забезпечити відповідність мережі функціональним потребам підприємства, вимогам надійності, інформаційної безпеки, масштабованості та зручності адміністрування.

Рисунок 1.1 – Стадії та етапи розробки проєкту комп'ютерної мережі

У таблиці 1.2 наведено послідовність робіт на кожному з етапів [17].

Таблиця 1.2 - Послідовність робіт на етапах розробки КМ

Етап	Послідовність робіт
1	2
Передпроєктне обстеження об'єкта	Аналізується план приміщення, структура ПП, склад підрозділів і характер інформаційних потоків. Визначаються кількість користувачів, робочих місць, мережевих пристроїв, критичні зони та перспективи розширення мережі.
Формування технічних вимог до мережі	Уточнюються функції майбутньої мережі: доступ до Інтернету, спільних ресурсів, Wi-Fi, відеоспостереження, резервного копіювання та адміністрування. Визначаються вимоги до швидкодії, безпеки, надійності та масштабованості.

Продовження таблиці 1.2

1	2
Розробка фізичної структури мережі	Визначається топологія мережі, місця розміщення розеток RJ-45, точок Wi-Fi, мережевих принтерів, камер відеоспостереження та іншого обладнання. Основою побудови приймається централізована схема з комутацією в телекомунікаційній кімнаті.
Проєктування кабельної інфраструктури	Розробляються кабельні траси від телекомунікаційної кімнати до робочих місць і мережевих пристроїв. Визначаються тип кабелю, спосіб прокладання, маркування кабелів, розеток, патч-панелей і портів комутаторів.
Розробка логічної структури мережі	Формується логічна модель мережі з поділом на функціональні сегменти або VLAN для адміністративного, фінансового, клієнтського, технічного, IT-сегмента, відеоспостереження та гостьового Wi-Fi. Визначаються IP-адресація, шлюзи, правила взаємодії між сегментами.
Проєктування системи інформаційної безпеки	Визначаються заходи захисту мережі та службових даних: розмежування доступу між підрозділами, правила міжмережевої взаємодії, захист адміністративних інтерфейсів, ізоляція гостьового Wi-Fi, журналювання подій і контроль доступу до критичних ресурсів.
Підбір обладнання та матеріалів	Виконується вибір комутаторів, маршрутизатора або міжмережевого екрана, патч-панелей, кабелю, розеток, точок Wi-Fi, UPS, серверного або мережевого сховища, камер і монтажних матеріалів. Обладнання підбирається з урахуванням кількості портів, підтримки VLAN, PoE, моніторингу та резерву для розвитку.

Продовження таблиці 1.2

1	2
Підготовка комплекту проєктної документації	Формуються пояснювальна записка, плани розміщення розеток і кабельних трас, структурна та логічна схеми мережі, таблиці IP-адресації й комутації, відомість кабельних ліній, схема телекомунікаційної шафи, специфікація обладнання та вимоги до експлуатації.
Монтаж і налагодження мережі	Після затвердження проєкту виконуються монтаж кабельних трас, встановлення розеток, телекомунікаційної шафи, патч-панелей, комутаторів, маршрутизатора, точок Wi-Fi та іншого обладнання. Далі налаштовуються VLAN, IP-адресація, доступ до Інтернету, Wi-Fi, правила безпеки та базовий моніторинг.
Тестування та приймання мережі	Перевіряється працездатність кабельних ліній, розеток, VLAN, доступу до Інтернету, Wi-Fi, відеоспостереження, резервного живлення та правил доступу між сегментами. Результати перевірок оформлюються актами приймання.
Введення в експлуатацію та супровід	Замовнику передається готова КМ й комплект документації. ІТ-відділ забезпечує подальший моніторинг, технічне обслуговування, резервне копіювання конфігурацій, ведення журналу змін і актуалізацію документації.

1.1.7 Вимоги до тестування та приймання мережі

Після монтажу мережі необхідно виконати деталізоване тестування функціонування ІКС для введення її в експлуатацію та складання акту приймання.

Перевірці підлягають:

- цілісність кабельних ліній;
- правильність обтискання та розведення пар;
- відповідність категорії кабельної системи;
- працездатність кожної інформаційної розетки;
- правильність маркування;
- доступність мережевих сервісів;
- швидкість підключення робочих місць;
- робота VLAN;
- доступ до Інтернету;
- робота Wi-Fi;
- робота камер відеоспостереження;
- робота резервного живлення;
- коректність правил міжмережевого доступу.

Результати тестування повинні бути оформлені актом або протоколом випробувань.

1.2 Постановка задачі на розробку проєкту. Характеристика підприємства, для якого створюється проєкт мережі

ПП «УК «ЖИТЛОФОНД» є керуючою компанією, діяльність якої пов’язана з обслуговуванням житлового фонду, організацією аварійно-ремонтних робіт, прийманням звернень громадян, веденням абонентського обліку, фінансово-бухгалтерським супроводом, юридичною підтримкою та технічною експлуатацією об’єктів житлово-комунального господарства.

Адміністративно-технічна структуру підприємства відображена на рисунку 1.2.

Організаційним центром підприємства є директор, якому підпорядковуються основні структурні напрями. Для забезпечення документообігу, приймання відвідувачів і координації роботи керівництва передбачено приймальню.

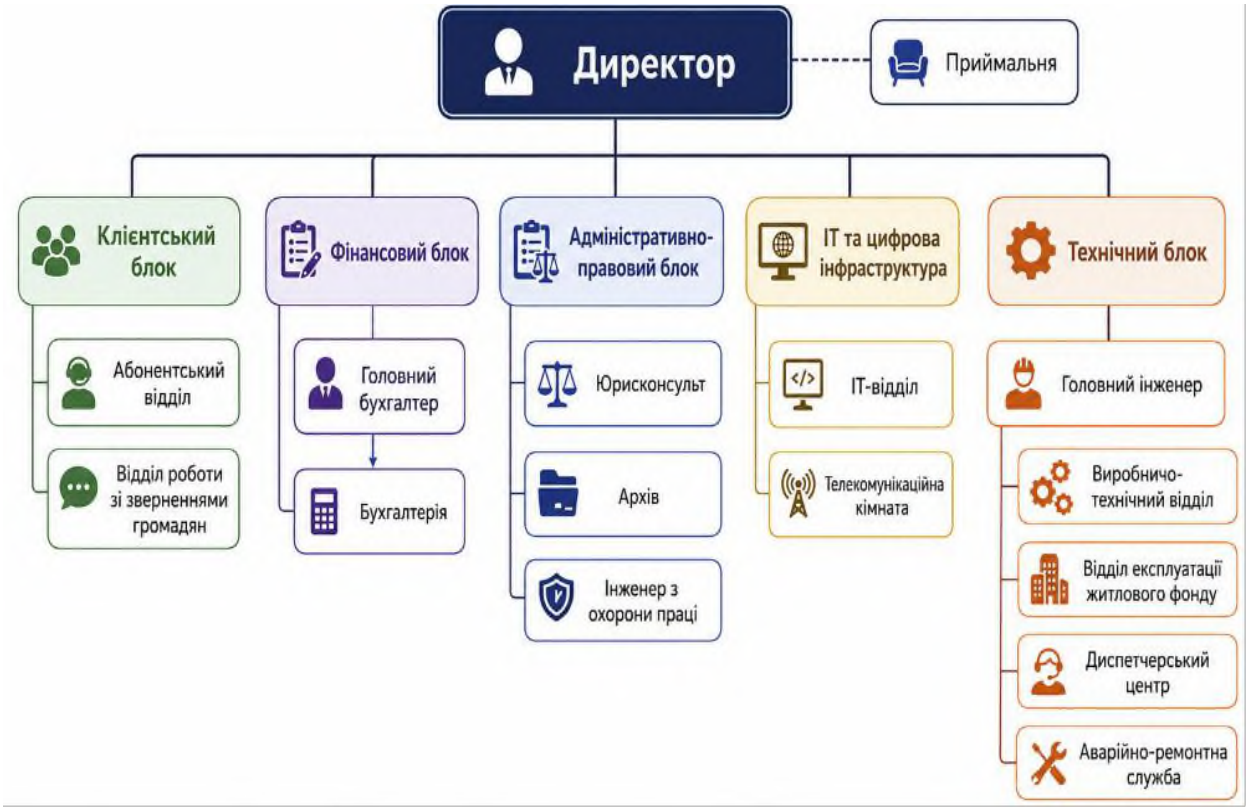

Рисунок 1.2 – Блок-схема структури ПП «УК «ЖИТЛОФОНД»

Клієнтський блок включає абонентський відділ та відділ роботи зі зверненнями громадян. Ці підрозділи забезпечують приймання мешканців, обробку звернень, консультації, реєстрацію заяв, роботу з абонентською інформацією та взаємодію з іншими службами підприємства.

Фінансовий блок складається з головного бухгалтера та бухгалтерії. Основними функціями цього напряму є фінансовий облік, нарахування платежів, ведення звітності, облік господарських операцій, робота з платіжними документами та взаємодія з банківськими й контролюючими установами.

Адміністративно-правовий блок включає юрисконсульта, архів та інженера з охорони праці. Ці підрозділи забезпечують юридичний супровід діяльності підприємства, зберігання документації, контроль дотримання вимог охорони праці та ведення службових документів.

IT-блок представлений IT-відділом та телекомунікаційною кімнатою. IT-відділ відповідає за підтримку користувачів, адміністрування

комп’ютерної техніки, роботу програмного забезпечення, доступ до інформаційних систем та технічний супровід цифрових сервісів. Телекомунікаційна кімната призначена для розміщення активного й пасивного мережевого обладнання: комутаційної шафи, патч-панелей, маршрутизатора, комутаторів, джерела безперебійного живлення та іншого обладнання комп’ютерної мережі.

Технічний блок очолює головний інженер. До нього належать виробничо-технічний відділ, відділ експлуатації житлового фонду, диспетчерський центр та аварійно-ремонтна служба. Ці підрозділи забезпечують ТО житлового фонду, планування ремонтних робіт, обробку аварійних заявок, координацію виїзних бригад і контроль виконання робіт.

Найбільша кількість робочих місць і мережевих підключень очікується в абонентському відділі, бухгалтерії, диспетчерському центрі, виробничо-технічному відділі та відділі експлуатації житлового фонду. Саме ці підрозділи активно працюють із базами даних, заявками, документами, електронною поштою, офісною технікою та внутрішніми інформаційними ресурсами.

Для директора, приймальні, головного бухгалтера, юрисконсульта, головного інженера та інженера з охорони праці необхідно передбачити індивідуальні робочі місця з доступом до локальної мережі, Інтернету, офісної техніки та службових інформаційних систем.

Для ІТ-відділу необхідно передбачити розширені можливості адміністрування мережі, доступ до телекомунікаційної кімнати, засобів моніторингу, серверного та комутаційного обладнання.

Телекомунікаційна кімната повинна бути центральним вузлом мережевої інфраструктури підприємства. У ній доцільно розмістити комутаційну шафу, патч-панелі, керовані комутатори, маршрутизатор, обладнання доступу до Інтернету, джерело безперебійного живлення та, за потреби, сервер або мережеве сховище [16].

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Логічна топологія мережі визначає спосіб взаємодії пристроїв, передачі даних між вузлами та організацію інформаційних потоків незалежно від фізичного розташування обладнання. На відміну від фізичної топології, яка описує фактичне розміщення кабелів і пристроїв, логічна архітектура відображає структуру маршрутизації трафіку, адресацію та правила взаємодії між окремими сегментами. Для ПП «УК «ЖИТЛОФОНД» обрано логічний тип мережі на основі технології Ethernet із сегментацією за допомогою віртуальних локальних мереж VLAN відповідно до міжнародного стандарту IEEE 802.1Q. Такий підхід дозволяє розділити єдину фізичну інфраструктуру на кілька незалежних логічних сегментів згідно з функціональною структурою підприємства.

Логічна структура мережі передбачає створення окремих віртуальних мереж для адміністрації, бухгалтерського підрозділу, абонентського відділу, технічного персоналу, диспетчерської служби, IT-відділу, серверного обладнання, системи відеоспостереження та гостьової бездротової мережі. Кожна VLAN утворює окремий широкомовний домен, що дозволяє суттєво обмежити розповсюдження службового трафіку та підвищити загальний рівень інформаційної безпеки. Для реалізації цієї сегментації використовується стандарт IEEE 802.1Q, який забезпечує маркування Ethernet-кадрів спеціальними тегами та дозволяє передавати трафік кількох логічних мереж через одні й ті самі фізичні канали зв'язку. Використання цього стандарту забезпечує повну сумісність обладнання різних виробників і є загальноприйнятим рішенням для побудови надійних корпоративних мереж.

Ця логічна архітектура розгортається поверх гібридної фізичної топології, яка поєднує дротовий сегмент типу «зірка» та бездротовий сегмент Wi-Fi 6 на базі точок доступу стандарту IEEE 802.11ax. Основою фізичної

мережі є центральний комутатор рівня L2+, до якого за допомогою структурованої кабельної системи підключаються всі робочі станції, сервери, принтери та інше обладнання. Така класична організація гарантує простоту адміністрування, високу надійності та можливість швидкої локалізації несправностей. При цьому бездротовий сегмент повністю інтегрується в загальну мережеву інфраструктуру та підтримує передачу трафіку різних VLAN через механізм тегування. Це дозволяє користувачам бездротової мережі працювати в тих самих логічних сегментах, що й користувачам дротової мережі, без порушення політик безпеки та розмежування доступу. Поєднання дротової топології та бездротового сегмента формує гнучку гібридну систему, де логічна структура залишається єдиною незалежно від способу підключення кінцевих пристроїв.

Основною перевагою обраної логічної структури є високий рівень інформаційної безпеки, оскільки забезпечується повна ізоляція критичних зон підприємства. Наприклад, працівники абонентського відділу чи гості у бездротовій мережі не мають прямого доступу до мережевих ресурсів бухгалтерії, а система відеоспостереження повністю відокремлена від загального користувацького сегмента. Взаємодія між окремими віртуальними мережами здійснюється централізовано через маршрутизатор DrayTek Vigor2865ax із обов'язковим застосуванням правил міжмережевого екрана та політик доступу. Крім того, розподіл пристроїв за функціональними сегментами зменшує кількість широкомовних пакетів, знижує навантаження на комутатори та підвищує продуктивність мережі, що особливо важливо для сегмента відеоспостереження, який генерує значні обсяги трафіку.

Обрана логічна архітектура також забезпечує відмінну масштабованість та можливість подальшого розвитку підприємства без суттєвої модернізації фізичної інфраструктури. У разі створення нових підрозділів або впровадження додаткових інформаційних систем адміністратору достатньо програмно створити нову VLAN на наявному обладнанні та налаштувати відповідні правила маршрутизації й доступу. Таким чином, використання

логічної Ethernet-мережі з VLAN-сегментацією за стандартом IEEE 802.1Q поверх гібридної топології є найбільш доцільним технічним рішенням для ПП «УК «ЖИТЛОФОНД», оскільки воно гарантує високий рівень керованості, безпеки, продуктивності та гнучкості всієї мережевої інфраструктури [2].

Поділ мережі на функціональні сегменти задокументовано у таблиці 2.1.

Таблиця 2.1 – Поділ мережі на функціональні сегменти

Маркування пристроїв	Кількість мережевих пристроїв	Фізичне розташування	Функціональний сегмент	Адреса підмережі/ маска
1	2	3	4	5
WS_1	1	Інженер з охорони праці	VLAN 10 ADMIN	192.168.10.0 /24
WS_2	1	Юрисконсульт	VLAN 10 ADMIN	192.168.10.0 /24
WS_3; PR_1	2	Приймальня	VLAN 10 ADMIN	192.168.10.0 /24
WS_4	1	Директор	VLAN 10 ADMIN	192.168.10.0 /24
WS_5-WS_6; PR_2	3	Аварійно-ремонтна служба	VLAN 20 DISPATCH	192.168.20.0 /24
WS_7-WS_9; PR_3	4	Диспетчерський центр	VLAN 20 DISPATCH	192.168.20.0 /24
WC_1	1	Диспетчерський центр	VLAN 90 VIDEO_REC	192.168.90.0 /24

Продовження таблиці 2.1

1	2	3	4	5
WS_10-WS_11; PR_4	3	Відділ роботи зі зверненнями громадян	VLAN 20 DISPATCH	192.168.20.0 /24
WS_12	1	Головний бухгалтер	VLAN 30 ACCOUNTING	192.168.30.0 /24
WS_13-WS_15; PR_5	4	Бухгалтерія	VLAN 30 ACCOUNTING	192.168.30.0 /24
WC_2	1	Бухгалтерія	VLAN 90 VIDEO_REC	192.168.90.0 /24
WS_16-WS_17	2	IT-відділ	VLAN 40 IT	192.168.40.0 /24
S_1; SW_1; R_1	3	Теле-комунікаційна кімната	VLAN 50 SERVERS	192.168.50.0 /24
S_2	1	Теле-комунікаційна кімната	VLAN 90 VIDEO_REC	192.168.90.0 /24
WS_18-WS_20; PR_6; PT_1-PT_3	7	Абонентський відділ	VLAN 60 CLIENT_ SERVICE	192.168.60.0 /24
WC_3	1	Абонентський відділ	VLAN 90 VIDEO_REC	192.168.90.0 /24
AP_1-AP_3	3	Коридор	VLAN 70 GUEST_WIFI	192.168.70.0 /24

Продовження таблиці 2.1

1	2	3	4	5
WC_4-WC_5	2	Коридор	VLAN 90 VIDEO_REC	192.168.90.0 /24
WS_21-WS_22; PR_7	3	Відділ експлуатації житлового фонду	VLAN 80 TECHNICAL	192.168.80.0 /24
WS_23-WS_24; PR_8	3	Виробничо-технічний відділ	VLAN 80 TECHNICAL	192.168.80.0 /24
WS_25	1	Головний інженер	VLAN 80 TECHNICAL	192.168.80.0 /24

Комутацію портів комутатора задокументовано у таблиці 2.2.

Таблиця 2.2 – Комутація портів

Маркування пристроїв	Перелік портів	Вид порту	Функціональний сегмент
1	2	3	4
WS_1- WS_4	1-4	Access	VLAN 10 ADMIN
WS_5- WS_11	5-11	Access	VLAN 20 DISPATCH
WS_12- WS_15	12-15	Access	VLAN 30 ACCOUNTING
WS_16- WS_17	16-17	Access	VLAN 40 IT

Продовження таблиці 2.2

1	2	3	4
WS_18- WS_20	18-20	Access	VLAN 60 CLIENT_ SERVICE
WS_21- WS_25	21-25	Access	VLAN 80 TECHNICAL
PR_1	26	Access	VLAN 10 ADMIN
PR_2- PR_4	27-29	Access	VLAN 20 DISPATCH
PR_5	30	Access	VLAN 30 ACCOUNTING
PR_6	31	Access	VLAN 60 CLIENT_ SERVICE
PR_7- PR_8	32-33	Access	VLAN 80 TECHNICAL
AP_1-AP_3	34-36	Trunk	VLAN 70 GUEST_WIFI
WC_1- WC_5	37-41	Access	VLAN 90 VIDEO_REC
PT_1-PT_3	42-44	Access	VLAN 60 CLIENT_ SERVICE
R_1	48	Trunk	VLAN 50 SERVERS
S_1	49	Access	VLAN 50 SERVERS

Продовження таблиці 2.2

1	2	3	4
S_2	50	Access	VLAN 90 VIDEO_REC

2.2 Розробка схеми фізичного розташування кабелів та вузлів комп'ютерної мережі ПП «УК «ЖИТЛОФОНД»

Фізичний етап проєктування ЛОМ полягає в інтеграції розробленої логічної структури та гібридної топології безпосередньо в архітектурні межі наявного плану приміщення підприємства. Основним завданням є створення СКС та оптимальне розміщення комутаційних центрів, що гарантуватиме мінімальне затухання сигналу, захист від електромагнітних завад і простоту подальшого обслуговування.

2.2.1 Організація центрального комутаційного вузла

Основою фізичної структури мережі є центральний комутаційний вузол, який локалізовано в окремому, спеціально виділеному приміщенні — телекомунікаційній кімнаті, розташованій суміжно з ІТ-відділом. Таке розміщення є стратегічно виправданим, оскільки воно забезпечує обмежений допуск сторонніх осіб до ядра мережі та спрощує адміністрування для фахівців ІТ-служби.

У телекомунікаційній кімнаті монтується закрита комутаційна шафа (або стійка), всередині якої встановлюється центральний керований комутатор рівня L2+ (SW_1), магістральний маршрутизатор (R_1), що забезпечує зв'язок із мережею Інтернет та між-VLAN маршрутизацію, а також серверипідприємства (S_1- S_2). Сюди ж зводяться всі кабельні траси (горизонтальна підсистема СКС) від кінцевих пристроїв, які комутуються на патч-панелях для забезпечення гнучкості перекросування.

2.2.2 Обґрунтування вибору кабельної продукції

Для побудови горизонтальної підсистеми СКС обрано екранований чотирипарний кабель «кручена пара» типу F/UTP категорії 6 (Cat 6) з чистолінійними мідними жилами та оболонкою LSZH (Low Smoke Zero Halogen).

Вибір категорії 6 замість базової 5е є технологічно виправданим кроком, який створює довгостроковий інфраструктурний резерв для ПП «УК «ЖИТЛОФОНД». Кабель Cat 6 працює на вищій частоті (до 250 МГц) і має внутрішній пластиковий розділювач пар (хрестовину), що суттєво знижує рівень міжпарних наводок (NEXT). Це дозволяє стабільно підтримувати швидкість до 1 Гбіт/с на відстані до 100 метрів, а також забезпечує технічну спроможність передачі даних на швидкості до 10 Гбіт/с (10GBASE-T) на коротших дистанціях (до 37–55 метрів), що ідеально підходить для підключення серверного обладнання та високонавантажених точок доступу Wi-Fi 6.

Застосування загального екранування (F/UTP) захищає інформаційні канали від зовнішніх наведень від силової проводки, а оболонка LSZH забезпечує відповідність суворим вимогам пожежної безпеки, оскільки у разі загоряння вона не виділяє токсичного диму та шкідливих сполук газу-галогену [2].

2.2.3 Трасування кабельної системи (дротового сегменту «зірки»)

Кабельна інфраструктура проєктується за класичною топологією «зірка», де кожен кінцевий пристрій має виділену лінію зв'язку безпосередньо до комутатора в телекомунікаційній кімнаті. Магістральні кабельні канали прокладаються вздовж центрального коридору будівлі всередині підвісних стель або в спеціальних настінних пластикових коробах (кабель-каналах),

утворюючи потужний інформаційний шлейф. Від цього шлейфу виконуються відгалуження в кожне робоче приміщення.

Дротовим способом підключаються стаціонарні робочі станції (WS_1- WS_25), мережеві принтери (PR_1- PR_8), платіжні термінали (PT_1- PT_3), а також сервери (S_1- S_2) та IP-камери (WC_1–WC_5). Наприклад, кабельні лінії від робочих місць адміністрації (кабінети директора, приймальні, юрисконсульта), бухгалтерії, абонентського відділу та диспетчерського центру сходяться до єдиної точки комутації. Довжина кожної окремої лінії не перевищує технологічну межу в 90 метрів (для мідної крученої пари категорії 6), що повністю нівелює ризик критичного згасання сигналу та падіння швидкості.

2.2.4 Розгортання бездротового сегмента та системи відеоспостереження

Для організації бездротового сегмента мережі (VLAN 70) на плані приміщення визначено точки оптимального монтажу бездротових точок доступу стандарту Wi-Fi 6 (AP_1, AP_2, AP_3). Їхнє розташування в коридорній зоні та місцях найбільшого скупчення людей (наприклад, у відділі роботи зі зверненнями громадян та абонентському відділі) розраховане таким чином, щоб зони покриття радіосигналу частково перекривали одна одну. Це гарантує відсутність «мертвих зон» та забезпечує стабільний безшовний роумінг для мобільних пристроїв персоналу та гостей. Точки доступу монтуються на стелі та підключаються до центрального комутатора кабельними лініями з підтримкою технології PoE (Power over Ethernet), що виключає потребу в прокладанні додаткових силових кабелів живлення.

Аналогічно реалізовано фізичне розміщення елементів системи відеоспостереження (VLAN 90). Цифрові IP-камери (WC_1–WC_5) та локальний сервер відеореєстратора (S_2) інтегруються у спільні кабельні

траси. IP-камери також підключаються до центрального комутатора кабельними лініями з підтримкою технології PoE.

2.2.5 Логічна ізоляція на фізичному рівні

Незважаючи на те, що всі кабельні лінії від робочих станцій бухгалтерів (VLAN 20), диспетчерів (VLAN 40), камер відеонагляду та Wi-Fi точок прокладаються в межах одних і тих самих будівельних конструкцій та підключаються до одного фізичного комутатора SW_1, вони залишаються повністю ізольованими. Схема фізичного розташування розроблялася з урахуванням чіткої прив'язки кожного фізичного порту на патч-панелі та комутаторі до конкретного логічного ідентифікатора стандарту IEEE 802.1Q. Такий підхід дозволив створити надійне, фізично впорядковане та захищене середовище, яке відповідає всім архітектурним особливостям приміщення ПП «УК «ЖИТЛОФОНД» і вимогам сучасної IT-безпеки.

2.3 Обґрунтування вибору обладнання для мережі (активного та пасивного)

Обґрунтування вибору мережевого обладнання базується на фундаментальних архітектурних принципах побудови локальних обчислювальних мереж. Відповідно до класичного підходу, розробка специфікації «заліза» вимагає чіткого розподілу на активні компоненти, які безпосередньо беруть участь в обробці, комутації та маршрутизації інформаційних потоків за допомогою ПЗ, та пасивні елементи, які забезпечують створення стабільного фізичного середовища для передачі сигналу та механічного кріплення вузлів.

Вибір активного обладнання, зокрема маршрутизаторів та комутаторів, обґрунтовується на основі аналізу топології та інтенсивності мережевого трафіку. Ключовими критеріями для вибору комутаторів є їхня внутрішня

пропускна здатність, обсяг буферної пам'яті для зберігання пакетів під час перевантажень, сумісність із мережевими стандартами (такими як Ethernet) та можливість підтримки віртуальних локальних мереж VLAN [7].

Для комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» найбільш технічно та архітектурно обґрунтованим, на основі порівняння техніко-економічних характеристик із підібраних трьох пропозицій у таблиці 2.3 [13], є вибір керованого комутатора DrayTek VigorSwitch P2540x (див. рис. 2.1). Модель від DrayTek забезпечує максимальний рівень продуктивності для поточної архітектури. Комутатор має найвищу серед представлених кандидатів комутаційну здатність у 216 Гбіт/с та швидкість пересилання пакетів на рівні 160,7 Mpps, що гарантує безперебійну обробку щільних потоків даних без ризику виникнення затримок. Такий набір характеристик найкраще відповідає потребам підприємства: роботі Wi-Fi, NVR-сегмента, робочих місць, серверного або NAS-обладнання, логічній сегментації мережі та централізованому адмініструванню.

Рисунок 2.1 – Обраний комутатор DrayTek VigorSwitch P2540x

Ключовою перевагою DrayTek VigorSwitch P2540x є наявність 6 оптичних uplink-портів стандарту 10G SFP+, тоді як конкуренти від PLANET та Edge-Core пропонують лише по 2 або 4 порти такого класу. Цей надлишковий високошвидкісний потенціал є критично важливим для нашої топології, оскільки дозволяє безпосередньо підключити файл-сервер NAS Synology та магістральний маршрутизатор на швидкості 10 Гбіт/с, повністю ліквідуючи мережеві «вузькі місця» під час інтенсивного резервного

копіювання баз даних та трансляції потоків відеоспостереження. Додатковим аргументом виступає наявність розвинених L3-функцій, зокрема підтримки VLAN Route для 8 віртуальних мереж, що дозволяє розвантажити центральний маршрутизатор і здійснювати внутрішню комутацію між функціональними підрозділами безпосередньо на рівні комутатора ядра.

З точки зору бюджету потужності, інтегрований PoE-бюджет у 400 Вт для 48 портів є повністю збалансованим. Його абсолютно достатньо для одночасного стабільного живлення всіх передбачених проєктом стельових точок доступу Wi-Fi 6 та цифрових IP-камер, де споживання на один порт не перевищуватиме стандартні 15–30 Вт. На додачу, побудова ядра мережі на базі обладнання одного вендора (маршрутизатор DrayTek Vigor2865ax + комутатор VigorSwitch P2540x) дозволяє IT-відділу використовувати єдину програмну систему централізованого моніторингу та адміністрування VigorACS, суттєво спрощуючи налаштування політик безпеки, оновлення прошивок та загальну експлуатацію корпоративної мережі підприємства [19].

Таблиця 2.3 – Підбір керованого комутатора

Характеристика	DrayTek VigorSwitch P2540x / P2540xs	PLANET GS-5220-48P4X	Edge-Core ECS4510-52P
1	2	3	4
Клас пристрою	L2+ керований PoE-комутатор з окремими L3-функції.	L2+/L3 керований PoE-комутатор.	L2+ керований PoE-комутатор з окремими L3-функції.
Корпус / монтаж	1U, 19” rack	1U, 19” rack	1U, 19” rack
Оптичні / uplink-порти	6 × SFP+ 1G/10G.	4 × SFP+ 10GBASE-SR/LR.	2 × 10G SFP+ та 1 слот під dual-port 10G expansion module.

Продовження таблиці 2.3

1	2	3	4
Основні мідні порти	48 × RJ-45 10/100/1000 Мбіт/с BASE-T PoE+.	48 × RJ-45 10/100/1000 Мбіт/с BASE-T PoE+.	48 × RJ-45 10/100/1000 Мбіт/с BASE-T PoE+.
Консольний порт	1 × RS232-to-RJ45 serial console.	1 × RS232-to-RJ45 serial console.	1 × RS232-to-RJ45 serial console.; також USB Type-A storage port.
PoE-стандарт	IEEE 802.3af PoE та IEEE 802.3at PoE+.	IEEE 802.3af/ 802.3at PoE PSE.	IEEE 802.3af PoE та IEEE 802.3at PoE+.
Кількість PoE-портів	48 PoE+ портів.	48 PoE+ портів.	48 PoE+ портів.
PoE-бюджет	400 Вт.	400 Вт для GS-5220-48P4X; до 720 Вт для GS-5220-48PL4XR.	780 Вт.
Максимальна потужність PoE на порт	До 30 Вт на порт відповідно до IEEE 802.3at PoE+.	До 36 Вт на порт.	До 30 Вт на порт за стандартом.
Комутаційна здатність	216 Гбіт/с	176 Гбіт/с	176 Гбіт/с
Швидкість пересилання пакетів	160,7 Mpps.	130 Mpps	130,94 Mpps.
Таблиця MAC-адрес	16K записів	16K записів	16K записів
Буфер / пам’ять	16 Mbit	32 Mbit	16 Mbit
Jumbo Frame	До 12 KB	До 10 KB	До 12 KB
VLAN	До 512 VLAN	До 4K VLAN	До 4K VLAN
L3-функції	Static Route, VLAN Route, DHCP Server; до 512 routes, DHCP для 8 VLAN.	IPv4 OSPFv2, IPv4/IPv6 hardware static routing, до 128 VLAN	IPv4 Static Route та RIP v1/v2.

Продовження таблиці 2.3

1	2	3	4
Безпека	802.1X/MAC Authentication, ACL, IP Source Guard, DHCP Snooping, DAI, Storm Control, DoS Defense.	ACL L2-L4, 802.1X, MAC-based authentication, RADIUS/TACACS+, DHCP Snooping, IP Source Guard, DAI.	Port security, 802.1X, MAC authentication, DHCP Snooping, IP Source Guard, ACL, Private VLAN, DAI, SSH/SSL.
Керування	Web GUI, HTTP/HTTPS, Telnet, SSHv2, SNMP v1/v2c/v3, RMON, LLDP/LLDP-MED, sFlow, VigorACS/VigorConnect.	Console/Telnet CLI, Web, SNMP v1/v2c/v3, SSHv2, TLSv1.2, Syslog, Smart Discovery Utility, UNI-NMS.	Web management, CLI, Telnet, SNMP v1/v2c/v3, RMON, Syslog, SMTP notification, LLDP/LLDP-MED.
Ціна	46296 грн.	53578 грн.	40247 грн.

Маршрутизатори мережі обираються за критеріями швидкості обробки таблиць маршрутизації та щільності інтерфейсів для підключення магістральних ліній зв'язку [7]. Такий аналіз дозволяє мінімізувати затримки передачі даних і виключити утворення вузьких місць у місцях концентрації трафіку.

Для комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» найбільш найбільш технічно та архітектурно обґрунтованим, на основі порівняння техніко-економічних характеристик із підібраних трьох пропозицій у таблиці 2.4 [14], є вибір маршрутизатора DrayTek Vigor2865ax (див. рис. 2.2).

DrayTek Vigor2865ax є спеціалізованим бізнес-рішенням класу SMB (Small and Medium Business), яке ідеально закриває всі системні потреби підприємства. Він «з коробки» підтримує до 16 активних логічних сегментів VLAN із можливістю гнучкого налаштування міжмережевого екрана та політик доступу між ними, що дозволить, наприклад, надійно ізолювати

трафік системи відеоспостереження від гостьового Wi-Fi. Крім того, пристрій володіє потужним корпоративним VPN-сервером із підтримкою до 32 одночасних тунелів (включаючи сучасний та швидкий WireGuard, а також IPsec з апаратним прискоренням до 800 Мбіт/с), що забезпечить безпечне віддалене підключення для співробітників або технічного персоналу на виїздах.

Рисунок 2.2 – Обраний маршрутизатор DrayTek Vigor2865ax

Важливим фактором на користь DrayTek є інтеграція пристрою в загальну екосистему проєкту. Шлюз має вбудовані інструменти централізованого керування точками доступу та комутаторами (Central AP/Switch Management), а також сумісний із системою VigorACS 3. Оскільки в якості комутатора ядра вже обрано DrayTek VigorSwitch P2540x, побудова мережі на базі одного вендора дозволить адміністраторам ПП «УК «ЖИТЛОФОНД» здійснювати комплексний моніторинг інформаційних потоків, розгортати бездротові мережі та керувати безпекою всього підприємства з єдиної консолі управління, мінімізуючи витрати на обслуговування інфраструктури [20].

Таблиця 2.4 – Підбір маршрутизатора

Характеристика	DrayTek Vigor2865ax	ASUS RT-AX89X	NETGEAR XR1000-100EUS
Стандарт Wi-Fi	Wi-Fi 6 (IEEE 802.11ax), сумісність з 802.11a/b/g/n/ac/ax	Wi-Fi 6 (802.11ax), Wi-Fi 5, Wi-Fi 4, 802.11a/b/g	Wi-Fi 6 (802.11ax), зворотна сумісність з 802.11a/b/g/n/ac
Діапазони Wi-Fi	2,4 ГГц / 5 ГГц	2,4 ГГц / 5 ГГц	2,4 ГГц / 5 ГГц
Максимальна швидкість Wi-Fi	2,4 ГГц: до 574 Мбіт/с; 5 ГГц: до 2402 Мбіт/с	2,4 ГГц: до 1148 Мбіт/с; 5 ГГц: до 4804 Мбіт/с	2,4 ГГц: до 600 Мбіт/с; 5 ГГц: до 4,8 Гбіт/с
Конфігурація радіомодулів	2x2 MIMO / 2x2 MU-MIMO	2,4 ГГц: 4x4; 5 ГГц: 8x8	2,4 ГГц: 2x2; 5 ГГц: 4x4
WAN-порти	1 x RJ-11 xDSL WAN; 1 x 1GbE RJ-45 WAN/LAN	1 x 1GbE WAN; 1 x 10GbE RJ-45 WAN/LAN; 1 x 10G SFP+ WAN/LAN	1 x Gigabit Ethernet WAN
LAN-порти	5 x 1GbE RJ-45 LAN + 1 x 1GbE WAN/LAN	8 x 1GbE RJ-45 LAN; 1 x 10GbE RJ-45; 1 x SFP+	4 x Gigabit Ethernet LAN
Безпека	SPI firewall, content filtering, IP-based firewall policy, DoS/Spoofing defense, URL/DNS keyword filtering, VPN pass-through	AiProtection, WPA3/WPA2/WPA, Firewall, SSH, Let’s Encrypt, MAC-фільтрація, Guest Network	NETGEAR Armor, WPA3, 128-bit AES with PSK, Guest Network, automatic firmware update
Централізоване керування	Central AP Management, Central Switch Management, VigorACS 3, SNMP, Syslog, NetFlow/IPFIX	AiMesh, Web UI, ASUS Router App, System Log, config backup/restore, diagnostics	Nighthawk App, DumaOS 3.0 dashboard, firmware updates
Ціна	17555 грн.	18767 грн.	21013 грн.

Особливе місце в обґрунтуванні активних компонентів посідає бездротовий сегмент та системи збереження даних. Архітектура бездротових точок доступу повинна розраховуватися з урахуванням координації каналів для уникнення взаємних завад та забезпечення належної пропускної здатності середовища для багатьох мобільних клієнтів одночасно [7].

Для комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» найбільш технічно та архітектурно обґрунтованим, на основі порівняння техніко-економічних характеристик із підібраних трьох пропозицій у таблиці 2.5 [15], є вибір точки доступу DrayTek VigorAP 1060C (див. рис. 2.3).

Рисунок 2.3 – Обрана точка доступу DrayTek VigorAP 1060C

Ця модель є беззаперечним лідером за співвідношенням «ціна-продуктивність». За суттєво дешевшої вартості пристрій пропонує аналогічні, а в деяких аспектах і кращі характеристики.

Швидкість до 3.6 Гбіт/с та просторова конфігурація антен 4x4 MU-MIMO гарантують стабільне покриття та плавну роботу десятків бездротових гаджетів одночасно. Наявність порту 1 × 2.5GbE з підтримкою PoE+ (802.3at) дозволяє підключити пристрій до комутатора ядра на швидкості понад

1Гбіт/с, ліквідуючи будь-які затримки трафіку у навантажених зонах (наприклад, в абонентському відділі).

Точка доступу повністю підтримує сучасне шифрування WPA3, технологію побудови Mesh-мереж для безшовного роумінгу, а також повноцінне тегування 802.1Q VLAN. Це дозволяє безперешкодно транслювати через одну фізичну точку три ізольовані бездротові мережі (SSID): для адміністрації, технологічного персоналу та ізольовану гостьову мережу.

Головний плюс — безкоштовне централізоване керування. Оскільки маршрутизатор (Vigor2865ax) та комутатор ядра (VigorSwitch P2540x) у даному проєкті також належать до лінійки DrayTek, ці точки доступу автоматично підхоплюються та адмініструються безпосередньо з інтерфейсу маршрутизатора (через вбудовану утиліту Central AP Management) або безкоштовний софт VigorConnect. Тому не потрібно купувати жодних ліцензій чи додаткових апаратних контролерів [22].

Таблиця 2.5 – Підбір точки доступу

Характеристика	DrayTek VigorAP 1060C	Aruba AP-515 (Q9H62A)	EnGenius EWS377AP
Стандарт Wi-Fi	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Діапазони	2.4 / 5 ГГц	2.4 / 5 ГГц	2.4 / 5 ГГц
Швидкість	До 3.6 Гбіт/с	До 5.37 Гбіт/с	До 3.55 Гбіт/с
Просторові потоки	4x4 MU-MIMO	4x4:4 (5 ГГц), 2x2 (2.4 ГГц)	4x4:4 MU-MIMO
Порт Ethernet	1 × 2.5GbE PoE+	1 × 2.5GbE + 1 × 1GbE	1 × 2.5GbE PoE+
PoE	802.3af/at	802.3af/at/bt	802.3at
Підтримка WPA3	Так	Так	Так
Mesh	Так	Так	Так
Монтаж	Стіна/стеля	Стіна/стеля	Стіна/стеля
Ціна	20625 грн.	24999 грн.	25828 грн.

Що стосується систем збереження даних типу NAS та мережевих відеореєстраторів (NVR), їхній вибір базується на концепції мережевих систем зберігання, де ключовими факторами є швидкість мережевого інтерфейсу, надійність дискових масивів (RAID) та здатність процесора обробляти інтенсивні потоки вводу-виводу (I/O) під час паралельного запису критичних бекапів або важких медіаданих [7].

Для комп'ютерної мережі ПП «УК «ЖИТЛОФОНД», де мережеве сховище (NAS) одночасно виконуватиме роль центрального файл-сервера для колективної роботи та сервера резервного копіювання, найбільш технічно та архітектурно обґрунтованим, на основі порівняння техніко-економічних характеристик із підібраних трьох пропозицій у таблиці 2.6 [12], є вибір моделі Synology DS1825+ (див. рис. 2.4).

Рисунок 2.4 – Обраний NAS Synology DS1825+

Synology DS1825+ — це безальтернативний лідер за критерієм «ціна-продуктивність» для довгострокового проєкту. Переплата у 9 000 грн порівняно з Asustor повністю нівелюється наявністю ECC-пам'яті, процесором Ryzen, підтримкою мереж 10G/25G, величезним лімітом місткості (432 Тб) та безкоштовним професійним ПЗ для бекапів, що робить його найнадійнішим серцем для даних ПП «УК «ЖИТЛОФОНД».

Процесор AMD Ryzen V1500B (4 ядра / 8 потоків) оптимізований під високі навантаження вводу-виводу (I/O) та шифрування «на льоту». Об'єм ОЗП у 8 ГБ стандарту DDR4 ECC (із захистом від помилок та збоїв) гарантує

стабільність роботи баз даних та файлових систем без ризику пошкодження файлів.

Безкоштовний софт корпоративного рівня (Active Backup for Business): Synology надає готову екосистему для автоматичного резервного копіювання всієї мережі (ПК, серверів, баз даних) без купівлі ліцензій чи підписок. Це економить тисячі доларів на сторонньому софті (на кшталт Veeam чи Acronis).

Підтримка файлової системи Btrfs дозволяє створювати миттєві знімки даних (Snapshots), захищаючи підприємство від шифрувальників. Фірмовий RAID-масив SHR (Synology Hybrid RAID) дозволяє використовувати 8 відсіків із дисками різних об'ємів без втрати корисного простору, забезпечуючи відмовоустійкість (мережа працюватиме навіть при виході з ладу 1–2 дисків) та потенціал розширення ємності до вражаючих 432 Тб [23].

Таблиця 2.6 – Підбір NAS

Характеристика	Asustor AS6510T	Synology DS1825+	Netgear RN426
Відсіки	10	8	6
Процесор	Intel Atom C3538 4C 2.1GHz	AMD Ryzen V1500B 4C/8T 2.2GHz	Intel Atom C3000 Quad-Core
ОЗП	8 ГБ DDR4	8 ГБ DDR4 ECC	4 ГБ DDR4
Максимум ОЗП	32 ГБ	32 ГБ	32 ГБ
Мережа	2×10GbE + 2×1GbE	2×2.5GbE, до 25GbE	4×1GbE
M.2 NVMe	2	2	Немає
USB	2×USB 3.2	3×USB 3.2 Gen1	2×USB 3.0
RAID	JBOD,0,1,5,6,10	SHR,JBOD,0,1,5,6,10	X-RAID,0,1,5,6,10
Макс. ємність	160 ТБ	432 ТБ (з розширенням)	72 ТБ
Ціна	67599 грн.	76757 грн.	56760 грн.

У контексті побудови систем безпеки, вибір кінцевих цифрових пристроїв, таких як IP-камери та IP-відеореєстратори, безпосередньо

зав'язаний на мережеву інфраструктуру. Інтеграція таких медіапристроїв вимагає обов'язкової підтримки мережевих протоколів приорітизації трафіку QoS (Quality of Service) для чутливих до затримок відеопотоків, а також використання технології PoE стандартами IEEE 802.3af/at, що дозволяє передавати живлення та дані по одному кабелю. Вибір самих камер обґрунтовується необхідною роздільною здатністю та параметрами стиснення потоку (кодеками) для раціонального використання пропускної здатності каналів зв'язку, тоді як IP-відеореєстратор підбирається за сумарною вхідною пропускною здатністю (Inbound Bandwidth) та кількістю підтримуваних каналів, щоб уникнути втрати пакетів відеопотоку на етапі збереження в архів [8].

Для комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» найбільш технічно та архітектурно обґрунтованим, на основі порівняння техніко-економічних характеристик із підібраних трьох пропозицій у таблиці 2.7 [10], є вибір моделі TVT TD-3316H2-B2-B (див. рис. 2.5).

Рисунок 2.5 – Обраний IP-відеореєстратор TVT TD-3316H2-B2-B

TVT TD-3316H2-B2-B демонструє найкращий показник «ціна-продуктивність» для корпоративного використання. Завдяки наявності двох гігабітних мережевих портів, підтримці ультрависокої роздільної здатності 16 Мп та потужному вбудованому ШІ, цей реєстратор забезпечує максимальну відмовоустійкість, безпеку та ідеально інтегрується у розроблену нами логічну структуру мережі підприємства [10]

Таблиця 2.7 – Підбір IP-відеореєстратора

Характеристика	TVT TD-3316H2-B2-B	Provision-ISR NVR12-16400FAN	Dahua DH-XVR5216AN-I3/T
Тип	IP NVR	IP NVR	Penta-brid XVR
Канали	16 IP	16 IP	16 аналогових + до 24 IP
Макс. роздільна здатність	16 МП	до 12 МП	до 6 МП IP / 5 МП аналог
Пропускна здатність	192 Мбіт/с	400 Мбіт/с	128 Мбіт/с
Кодеки	H.265+/H.265/H.264	H.265+/H.265/H.264	H.265+/H.265/H.264
Відеовиходи	HDMI 4K, VGA	HDMI, VGA	HDMI 4K, VGA
Накопичувачі	2×SATA до 10 ТБ	2×SATA	2×SATA до 16 ТБ
Мережа	2×RJ45 1GbE	1×RJ45 1GbE	1×RJ45 1GbE
AI-функції	Face, LPR, VCA	VCA	WizSense, SMD+, Face Recognition
Ціна	14940 грн.	13200 грн.	12956 грн.

Для комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» найбільш технічно та архітектурно обґрунтованим та далекоглядним вибором на основі порівняння техніко-економічних характеристик із підібраних трьох пропозицій у таблиці 2.8 [11], є вибір моделі TVT TD-9584SL-C(D/PE/AW2) (див. рис. 2.6). Купуючи цю модель, ПП «УК «ЖИТЛОФОНД» економить на кожній камері понад 200 грн, отримуючи натомість повноцінну роздільну здатність 4K (8 Мп), кращу нічну оптику, розширену підтримку карт пам'яті та ідеальну сумісність із обраним ядром системи відеонагляду TVT.

Рисунок 2.6 – Обрана IP-камера TVT TD-9584SL-C(D/PE/AW2)

Таблиця 2.8 – Підбір IP-камери

Характеристика	Provision-ISR DV-340SRN-28	Dahua DH-IPC-HDW2449T-S-PRO-BE	TVT TD-9584SL-C(D/PE/AW2)
Роздільна здатність	4 МП	4 МП	8 МП
Об’єктив	2.8 мм	2.8 мм	2.8 мм
Сенсор	1/3" CMOS	1/2.9" CMOS	1/2.8" CMOS
Підсвічування	LED до 25 м	Full Color LED	White LED
Нічний режим	24/7 Full Color	Full Color	Full Color
Стиснення	H.265+/H.264+	H.265+/H.264+	H.265+/H.264+
Аналітика	Людина/авто, лінія	SMD Plus AI	Людина/транспорт
Аудіо	Вбудований мікрофон	Вбудований мікрофон	Вбудований мікрофон
microSD	до 256 ГБ	до 256 ГБ	до 512 ГБ
PoE	Так	Так	Так
Захист	IP67	IP67	IP67
Ціна	5940 грн.	5985 грн.	5744 грн.

Персональні комп'ютери користувачів та мережеві принтери не вносилися до переліку обладнання для закупівлі, оскільки вони вже перебувають на балансі підприємства та повністю задовольняють експлуатаційні вимоги щодо продуктивності, що дозволило уникнути додаткових капіталовкладень і спрямувати бюджет проєкту на забезпечення максимальної надійності мережевого ядра, серверного пулу та системи безпеки.

Обґрунтування вибору пасивного обладнання здійснюється на основі електричних, механічних та експлуатаційних параметрів, що забезпечують довговічність СКС. Під час вибору кабельної продукції (такої як кручена пара чи оптоволокно) необхідно враховувати вимоги до смуги пропускання та відстаней, на які передається сигнал. Наприклад, вибір екранованого кабелю

типу FTP категорії 6 регламентується необхідністю роботи мережі на гігабітних швидкостях у середовищі з наявністю значних зовнішніх електромагнітних завад. Вибір комутаційних патч-панелей, крос-модулів, горизонтальних організаторів та конструктиву підлогових шаф обґрунтовується їхньою категорійною відповідністю кабелю, потребами щільності портів та зручності кабельного менеджменту для запобігання критичним радіусам вигину провідників.

Спільна інтеграція активного та пасивного обладнання підпорядковується концепції ієрархічної побудови мереж. Застосування підходу вимагає, щоб пасивні елементи (патч-панелі) розміщувалися у безпосередній близькості до активних пристроїв (комутаторів ядра чи доступу) через кабельні організатори для забезпечення найменшої довжини сполучних патч-кордів [8]. Крім того, активне обладнання вимагає обов'язкового розрахунку сумарного тепловиділення та потужності споживання електроенергії, що є базою для вибору пасивних елементів охолодження (вентиляторних модулів шафи) та ДБЖ. Таким чином, системний вибір обладнання гарантує відмовоустійкість та масштабованість IT-інфраструктури підприємства [7]; [8].

Розроблена специфікація обладнання та матеріалів задокументована у таблиці 2.9.

Таблиця 2.9 - Специфікація обладнання та матеріалів

№ п/п	Назва елемента	Позначення	Ціна, грн.	Кількість	Одиниці виміру
1	2	3	4	5	6
1	Комутатор DrayTek VigorSwitch P2540x	SW_1	46296	1	шт.
2	Маршрутизатор DrayTek Vigor2865ax	R_1	17555	1	шт.

Продовження таблиці 2.9

1	2	3	4	5	6
3	Точка доступу DrayTek VigorAP 1060C	AP_1-AP_3	20625	3	шт.
4	NAS Synology DS1825+	S_1	76757	1	шт.
5	IP-відеореєстратор TVT TD-3316H2-B2-B	S_2	14940	1	шт.
6	IP-камера TVT TD-9584SL-C(D/PE/AW2)	WC_1-WC_5	5744	5	шт.
7	Шафа серверна підлогова 42U глибина 675 мм чорний CMS UA-MGSE4266MB	-	38528	1	шт.
8	Вентиляторний блок в дах для шаф MGSE CMS UA-MGSE-F3MB	-	4165	1	шт.
9	Полиця консольна 300 мм 19" 1U черна CMS UA-SHC300B	-	477	2	шт.
10	Фільтр мережевий 19” на 8 розеток Clever AUE2250D3-08LMCPMB	-	1822	1	шт.

Продовження таблиці 2.9

1	2	3	4	5	6
11	Патч-панель екранована мережева RJ-45 19" 24 порта cat.6 1U FTP з органайзером 6PLDN-F24BK	-	3644	2	шт.
12	Кабельний організатор 19" 1U з кришкою EPN PLMN-060Z	-	555	2	шт.
13	ДБЖ Cover CORE 3K	-	41673	1	шт.
14	Кабель вита пара F/UTP категорія 6 4x2x0.54 бухта 305 м OK-Net	-	11246	4	шт.
15	Патч-корд S/FTP LSOH 0.5 м cat.6 сірий Premium Line 18642005L	-	143	44	шт.
16	Патч-корд S/FTP LSOH 3 м cat.6 сірий Premium Line 18642030L	-	309	41	шт.
17	Розетка настінна на 1 порт RJ-45 FTP cat.6 EPNew 6BX-S1WHA6	-	137	41	шт.

Продовження таблиці 2.9

1	2	3	4	5	6
18	DKC лоток перфорований 100х50 гарячого цинкування, метод Сендзіміру	-	175	122	м
19	Кабельний канал 15х10 мм білий серія LH Kopos LH 15X10_HD, 2м	-	37	33	шт.
20	Серверний жорсткий диск для систем відеоспостереження Lenovo ThinkSystem 4XB7A83970 2.5" 2.5ТБ SAS	-	14587	2	шт.
21	Серверний жорсткий диск для NAS систем Western Digital Blue SATA III 2TB	-	7799	2	шт.

2.4 Особливості монтування мережі та організація обладнання в телекомунікаційній шафі ПП «УК «ЖИТЛОФОНД»

Монтаж мережевої інфраструктури для ПП «УК «ЖИТЛОФОНД» виконується відповідно до суворих галузевих СКС. Фізична реалізація проєкту передбачає концентрацію всього активного та пасивного обладнання

всередині підлогової телекомунікаційної шафи 42U CMS UA-MGSE4266MB, встановленої в захищеній телекомунікаційній кімнаті.

Грамотна поюнітова архітектура шафи, зображена на рисунку 2.7, дозволяє розв'язати три головні технічні завдання: мінімізацію наведень, ефективне охолодження та зручність адміністрування.

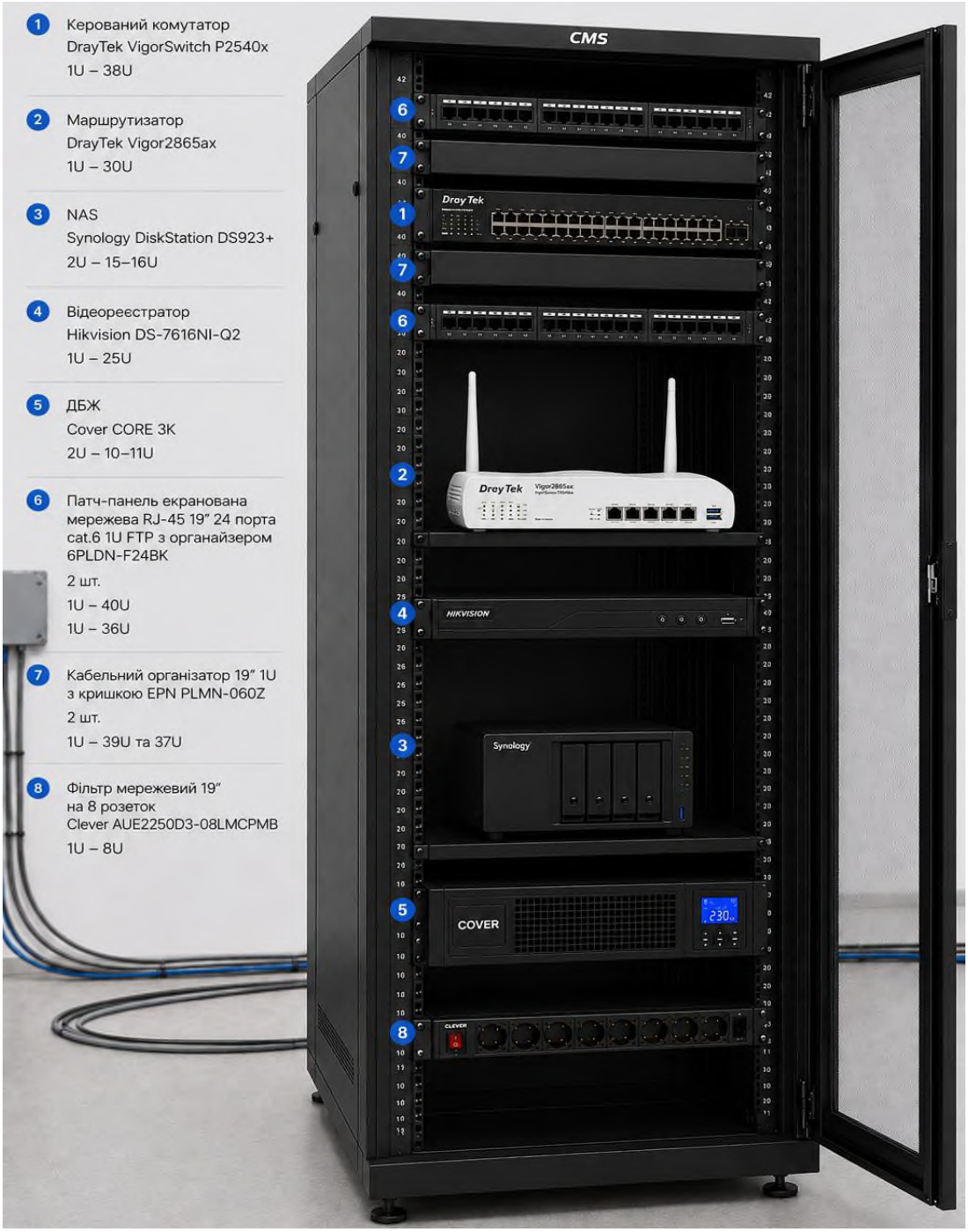

Рисунок 2.7 - Розміщення обладнання в шафі серверній підлоговій CMS UA-MGSE4266MB (42U)

Верхня частина шафи виділена під інтеграцію пасивних комутаційних елементів та головного комутатора мережі. Монтаж виконано за класичною індустріальною схемою «сендвіч», що є найбільш технічно грамотним рішенням для 48-портових систем: по центру, між двома патч-панелями, встановлено єдиний керований комутатор DrayTek VigorSwitch P2540x. Горизонтальні кабельні організатори з кришкою встановлені безпосередньо над і під комутатором.

Таке симетричне компонування дозволяє розділити комутаційне навантаження. Патч-корди від верхньої патч-панелі (40U) через верхній організатор (39U) опускаються в перші 24 порти комутатора. Патч-корди від нижньої патч-панелі (36U) через нижній організатор (37U) підіймаються у наступні 24 порти. Це повністю ліквідує проблему «кабельного хаосу», дозволяє використовувати ультракороткі патч-корди (30–50 см), забезпечує легкий доступ до будь-якого порту та залишає відкритою світлодіодну індикацію комутатора для діагностики лінків фахівцями IT-відділу.

Середня зона шафи використовується для пристроїв, які потребують регулярного автономного охолодження та чіткого логічного зв'язку з ядром мережі: маршрутизатор DrayTek Vigor2865ax (він виступає шлюзом безпеки, приймає зовнішні магістральні кабелі від провайдерів Інтернет та підключається окремим аплінком до комутатора), мережевий відеореєстратор Hikvision DS-7616NI-Q2 та стаціонарна поличка з NAS Synology DS923.

Розміщення NAS на рівні 15U та відеореєстратора на 25U забезпечує оптимальний теплообмін. Оскільки ці пристрої містять жорсткі диски (HDD), які працюють у режимі 24/7 та виділяють значну кількість тепла, значні технологічні проміжки між ними (31U–35U, 26U–29U, 16U–24U) запобігають перегріву та передчасному виходу дисків з ладу під дією гарячих повітряних потоків всередині шафи.

Нижній ярус телекомунікаційної шафи повністю відданий під важке силове обладнання: ДБЖ Cover CORE 3K потужністю 3 кВА, інтегрований разом із блоком розеток Clever PDU AUE2250D3 (на 8 розеток).

Монтаж ДБЖ на найнижчих рейках шафи є критично важливим з точки зору фізичної безпеки та архітектурного розрахунку. ДБЖ разом із внутрішніми свинцево-кислотними акумуляторами має найбільшу вагу серед усього набору обладнання. Його встановлення в самому низу зміщує центр ваги підлогової шафи до підлоги, гарантуючи стійкість конструкції та унеможливлюючи її випадкове перекидання під час монтажних робіт.

Крім того, перенесення блоку розеток Clever PDU вниз, безпосередньо до ДБЖ, дозволяє локалізувати всі силові кабелі живлення 220V в одній нижній зоні. Інформаційні слабострумові кабелі (FTP кручена пара) заходять у шафу зверху, а силові лінії підводяться знизу. Таке фізичне розділення інформаційних та силових трас повністю нівелює ризик виникнення низькочастотних електромагнітних завад і гарантує стабільну роботу мережі на швидкості 1 Гбіт/с без втрати пакетів.

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів

У проєктованій мережі ПП «УК «ЖИТЛОФОНД» серверна інфраструктура розгортається за децентралізованою схемою розподілу ресурсів, де кожна програмна роль підпорядкована окремому спеціалізованому апаратному вузлу. Сервер S_1 - центральне мережеве сховище Synology DS1825+ функціонує під управлінням фірмової операційної системи Synology DiskStation Manager (DSM), тоді як відеосервер S_2 - мережевий відеореєстратор TVT TD-3316H2-B2-B працює на базі закритих мікропрограм Embedded Linux. Такий вибір операційних систем та прикладного програмного забезпечення обґрунтовано критеріями відмовостійкості, кібербезпеки, відсутності витрат на ліцензування та відповідності фундаментальним архітектурним концепціям побудови клієнт-серверних систем [7].

Основою центрального серверного вузла підприємства є операційна система Synology DSM, яка побудована на базі модифікованого ядра Linux, що гарантує високу стабільність обробки мережевих запитів. Важливим архітектурним чинником вибору цієї ОС є інтеграція на рівні ядра підтримки новітньої файлової системи Btrfs, яка реалізує технологію Copy-on-Write (CoW). Використання сучасних файлових систем із підтримкою самовідновлення метаданих та миттєвих знімків (Snapshots) дозволяє надійно захистити критичні корпоративні дані й бази даних бухгалтерії від випадкового видалення або пошкодження шкідливим програмним забезпеченням [8]. Крім того, ОС DSM є пропрієтарним мікрокодом, оптимізованим під роботу оперативної пам'яті з корекцією помилок DDR4 ECC та ефективне керування пулом жорстких дисків у відмовостійкому масиві SHR (Synology Hybrid RAID), що забезпечує безперервність бізнес-процесів компанії.

Для реалізації ролі файл-сервера в середовищі ОС DSM розгортається програмний комплекс Synology Drive Server та служби мережевого доступу за протоколом SMB 3.0. Згідно з концепціями організації мережевого обміну даних, ефективний файл-сервер повинен мінімізувати затримки при обробці операцій вводу-виводу (I/O) та забезпечувати безпечний багатокористувацький доступ [7]. Протокол SMB v3 підтримує механізми шифрування трафіку «на льоту» та технологію SMB Multichannel, що гарантує максимальну швидкість передачі великих об'ємів даних і сумісність із наявним парком операційних систем Windows на робочих місцях без необхідності придбання додаткових клієнтських ліцензій доступу (CAL). Для захисту цифрових активів додатково впроваджується пакет Synology Active Backup for Business, який безліцензійно реалізує технологію глобальної дедуплікації на рівні блоків, що аналізує резервні копії з усіх робочих станцій, відсікає ідентичні системні файли й заощаджує до 50–60% простору на накопичувачах NAS.

Окреме місце в серверній інфраструктурі посідає IP-відеореєстратор TVT, який логічно виступає у ролі виділеного мережевого відеосервера та функціонує під управлінням спеціалізованої вбудованої операційної системи класу Embedded Linux. Використання мікропрограмних ОС замкненого циклу (Firmware) має суттєві переваги над універсальними платформами в розрізі кіберзахисту [8]. Оскільки Embedded Linux у реєстраторі TVT позбавлена графічних оболонок загального призначення, зайвих системних служб та можливості інсталяції стороннього програмного коду, вона має мінімальну площу цифрової атаки, що робить відеосервер практично невразливим до поширених мережевих вірусів чи цільових атак програм-вимагачів, які зазвичай орієнтовані на компрометацію вразливостей в універсальних ОС.

Архітектура Embedded Linux оптимізована на рівні компіляції ядра для виконання однієї пріоритетної задачі — обслуговування високошвидкісного потокового введення-виведення медіаданих у реальному часі. Робота з мультимедійним трафіком потребує суворого планування ресурсів процесора та буферної пам'яті для запобігання втрати мережевих пакетів [7]. Вбудована ОС відеосервера TVT забезпечує пряму взаємодію з апаратними кодеками стиснення H.265+ та файловою системою жорстких дисків без додаткових програмних прошарків, що гарантує абсолютну стабільність пристрою при максимальному навантаженні мережевих інтерфейсів, виключає зависання та забезпечує цілісність записуваного відеоархіву у виділеному сегменті системи безпеки (VLAN 90) [7]; [8].

Для забезпечення стовідсоткової сумісності та стабільної взаємодії з серверним пулом на робочих станціях користувачів ПП «УК «ЖИТЛОФОНД» розгорнуто операційні системи сімейства Windows 11 Pro. Вибір професійних редакцій клієнтських ОС обґрунтовано наявністю повноцінного програмного стека для роботи з сучасними мережевими протоколами прикладного рівня, зокрема з SMB v3 (Server Message Block), який є базовим для обміну даними з файл-сервером Synology DS1825+. Корпоративні версії десктопних ОС підтримують розширені функції безпеки, такі як автентифікація на основі

шифрування NTLMv2/Kerberos та ізоляція трафіку, що дозволяє мережевим інтерфейсам комп'ютерів коректно взаємодіяти з тегованими віртуальними мережами (VLAN 10, 20, 30, 40), налаштованими на комутаторі DrayTek [8].

Крім того, вибір професійних лінійок Windows забезпечує безперешкодну роботу служб фонового резервного копіювання за допомогою технології миттєвих знімків томів VSS (Volume Shadow Copy Service). Ця служба є критично важливою для функціонування сервера бекапів, оскільки вона дозволяє агенту програми Synology Active Backup for Business виконувати повне копіювання файлової системи комп'ютера (Bare-Metal Backup) безпосередньо під час робочого процесу користувача, не блокуючи доступ до відкритих документів та баз даних. Така програмна однорідність клієнтської частини мінімізує накладні витрати процесорного часу на перетворення форматів даних, оптимізує черги мережевих запитів до NAS та гарантує захищеність і високу швидкість відновлення будь-якого робочого місця адміністрації чи бухгалтерії з централізованого архіву [7]; [8].

2.6 Тестування та налагодження спроєктованої мережі

Етап тестування та налагодження є критично важливою фінальною фазою впровадження мережевої інфраструктури ПП «УК «ЖИТЛОФОНД», яка гарантує відповідність реальних експлуатаційних характеристик заявленим проєктним вимогам. Цей процес виконується ієрархічно, починаючи від сертифікації фізичного рівня СКС і закінчуючи тестуванням прикладних серверних служб та політик корпоративної безпеки.

Першим кроком є апаратне тестування мідної горизонтальної підсистеми, яка налічує 41 лінію екранованого кабелю FTP Cat.6. Для цього використовується професійний кабельний аналізатор (наприклад, класу Fluke Networks), який виконує сертифікацію кожної лінії на відповідність індустріальним стандартам TIA/EIA-568. Під час перевірки вимірюються такі критичні показники, як правильність розшивки пар, рівень перехресних

наведень на ближньому кінці, зворотні втрати та загасання сигналу. Успішне проходження цих тестів гарантує, що кабельна траса здатна стабільно передавати дані на гігабітних швидкостях. Оскільки точки доступу та IP-камери живляться безпосередньо через мережевий кабель, додатково проводиться стрес-тест бюджету потужності PoE+. Комутатор DrayTek VigorSwitch P2540x навантажується одночасним підключенням усього периферійного обладнання, після чого вимірюється падіння напруги на найвіддаленіших розетках для підтвердження стабільності електроживлення під максимальним навантаженням [8].

Після підтвердження фізичної цілісності мережі розпочинається програмне налагодження активного обладнання з акцентом на перевірці сегментації та маршрутизації на базі шлюзу DrayTek Vigor2865ax. Для тестування ізоляції VLAN штучно генерується трафік між різними віртуальними мережами та перевіряється спрацювання списків контролю доступу (ACL). Наприклад, робочі станції з абонентського відділу не повинні мати логічного доступу до адміністрації, а IP-камери ізольованого сегмента (VLAN 90) не повинні мати прямого виходу в глобальну мережу Інтернет. Паралельно, за допомогою системи централізованого управління VigorACS, проводиться радіопланування та налагодження бездротового роумінгу. Інженери вимірюють рівень сигналу Wi-Fi 6 у різних частинах будівлі та перевіряють безшовне перемикання терміналів між точками доступу VigorAP 1060C без розривів з'єднання чи втрати мережевих пакетів.

На фінальному етапі тестується працездатність серверного пулу та систем збереження даних в умовах пікових навантажень підприємства. За допомогою спеціалізованих утиліт імітується одночасне звернення десятків користувачів до файл-сервера Synology DS1825+ за протоколом SMB 3.0, що дозволяє перевірити пропускну здатність інтерфейсів та стабільність відгуку дискового масиву SHR. Для перевірки відмовоустійкості проводяться контрольовані збої: імітується відключення електроенергії для тестування переходу на резервне живлення від ДБЖ Cover CORE 3K, а також штучно

вилучається один із жорстких дисків із NAS або відеореєстратора TVT для підтвердження здатності масивів продовжувати роботу без втрати даних. Завершується процес стрес-тестом системи відеонагляду, під час якого всі камери перемикаються в режим максимального бітрейту для перевірки здатності відеосервера декодувати потоки без пропуску кадрів та коректно обробляти аналітичні події розпізнавання облич [7].

Комплексне тестування дозволяє виявити та усунути приховані архітектурні чи конфігураційні конфлікти ще до введення мережі в комерційну експлуатацію. Успішне проходження всіх етапів налагодження гарантує, що спроєктована ІТ-інфраструктура ПП «УК «ЖИТЛОФОНД» функціонуватиме стабільно, безпечно та з високим рівнем відмовоустійкості з першого дня роботи.

Тестування працездатності мережі інструментами DrayTek

Побудова мережі на єдиній екосистемі DrayTek (маршрутизатор Vigor2865ax, комутатор VigorSwitch P2540x, точки доступу VigorAP 1060C) дозволяє використовувати фірмові програмні та апаратні інструменти для глибокого тестування, моніторингу та пошуку несправностей без необхідності купівлі стороннього комерційного ПЗ.

Програмний комплекс DrayTek VigorConnect — це безкоштовне програмне забезпечення від DrayTek для централізованого управління мережею (NMS), яке ідеально підходить для підприємств класу SMB (підтримує до 100 вузлів). Дозволяє розгорнути його на сервері Synology (через віртуальну машину або Docker) або на комп'ютері адміністратора.

Можливості для тестування:

1. Автоматична топологія (Auto Topology): ПЗ автоматично малює фізичну та логічну карту мережі (див. рис. 2.8). Це дозволяє візуально перевірити, чи правильно підключені всі точки доступу та комутатори.

2. Моніторинг навантаження: Тестування пропускної здатності портів та утилізації процесора/пам'яті на комутаторі в реальному часі.

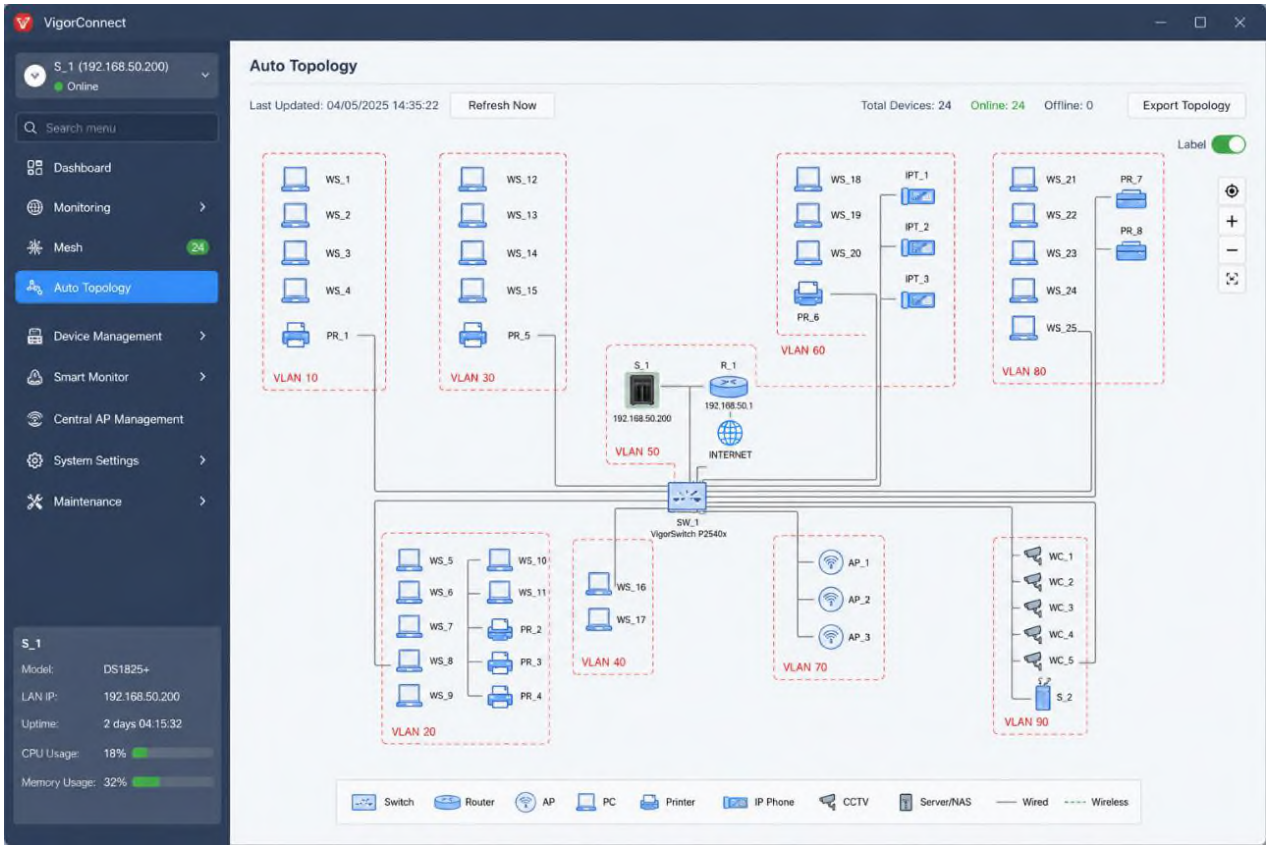

Рисунок 2.8 - Автоматична топологія в ПЗ DrayTek VigorConnect

3. Тестування PoE: Дозволяє бачити поточне споживання енергії (у Ватах) кожною камерою TVT та точкою доступу, щоб переконатися, що бюджет PoE (400 Вт для комутатора) не перевищено.

4. Система сповіщень (Alarms): Дозволяє протестувати відмовостійкість. Наприклад, можна фізично відключити резервний інтернет-канал або одну точку доступу і перевірити, чи система миттєво згенерує тривожне сповіщення.

Вбудовані інструменти діагностики (Diagnostics)

Як маршрутизатор Vigor2865ax, так і комутатор VigorSwitch P2540x мають потужне вбудоване меню Diagnostics у своїх веб-інтерфейсах.

1. Ping / Traceroute: Базові інструменти для перевірки зв'язку. Дозволяють безпосередньо з інтерфейсу комутатора «пінгувати» IP-адреси камер (VLAN 90) або серверів (VLAN 50), щоб переконатися, що L3-маршрутизація налаштована правильно і пакети проходять між відділами.

2. Data Flow Monitor (на маршрутизаторі): Дозволяє в реальному часі бачити, які саме пристрої споживають найбільше інтернет-трафіку і через який із двох WAN-каналів він іде. Це чудово підходить для тестування балансування навантаження (Load Balancing).

3. ARP Cache Table: Допомагає швидко знайти IP-адреси підключених пристроїв за їхніми MAC-адресами та переконатися, що ізоляція VLAN працює (наприклад, що гостьові пристрої не отримують адреси корпоративної мережі).

Port Mirroring (Віддзеркалення портів) для глибокого тестування

Якщо для тестування інформаційної безпеки або пошуку складних мережевих петель вам потрібен глибокий аналіз пакетів (наприклад, за допомогою популярної програми Wireshark), комутатор VigorSwitch P2540x підтримує функцію Port Mirroring.

Можна налаштувати комутатор так, щоб він копіював весь трафік, який проходить через магістральний оптичний порт 10G (зв'язок із сервером), і відправляв цю копію на звичайний мідний порт, до якого підключено ноутбук адміністратора з увімкненим сніфером. Це дозволяє аналізувати пакети на низькому рівні без розриву зв'язку для користувачів.

Перевірка безшовного Wi-Fi (AP Discovery та Station List)

Для тестування роботи Mesh-мережі на трьох точках VigorAP 1060C використовується меню маршрутизатора Central AP Management.

1. Station List: Показує рівень сигналу (RSSI) кожного підключеного смартфона чи ноутбука.

2. Тестування роумінгу: Можна взяти смартфон, увімкнути безперервний ping до локального сервера і пересуватися офісом. В інтерфейсі Central AP Management в реальному часі можна бачити, як клієнт «перестрибує» з однієї точки доступу на іншу без втрати пакетів [18]; [21]; [24].

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з інсталяції та налаштування активного комутаційного обладнання

3.1.1 Обґрунтування вибору архітектури міжвіртуальної маршрутизації в мережі ПП «УК «ЖИТЛОФОНД»

Для мережі ПП «УК «ЖИТЛОФОНД» технічно найбільш правильним і продуктивним рішенням є налаштування внутрішньої маршрутизації на комутаторі ядра (DrayTek VigorSwitch P2540x), тоді як маршрутизатор (DrayTek Vigor2865ax) слід розвантажити і залишити йому виключно роботу з Інтернетом (NAT, Firewall).

Головним аргументом на користь перенесення маршрутизації на комутатор є пропускна здатність та уникнення мережевого «вузького місця». Згідно з технічними характеристиками, шлюз Vigor2865ax має лише мідні гігабітні порти (1GbE). Якщо налаштували зв'язок між віртуальними мережами (VLAN) на ньому, весь міжвідомчий трафік мусив би йти до маршрутизатора і повертатися назад по одному кабелю. Наприклад, під час нічного резервного копіювання ПК адміністрації (VLAN 10) на файл-сервер Synology швидкість впиралася б у цей 1 Гбіт/с, повністю зводячи нанівець перевагу дорогих 10-гігабітних (10G SFP+) портів між комутатором та NAS-сервером.

Натомість комутатор VigorSwitch P2540x є пристроєм рівня L2+ і підтримує апаратну маршрутизацію (VLAN Route). Виконуючи маршрутизацію між підрозділами безпосередньо на його спеціалізованих мікросхемах (ASIC), ми досягаємо пересилання пакетів на швидкості шини (Wire-Speed), використовуючи весь потенціал комутаційної матриці у 216 Гбіт/с. Відповідно, комп'ютери з різних VLAN зможуть звертатися до сервера

або обмінюватися документами без мілісекундних затримок, минаючи маршрутизатор.

Водночас центральний процесор маршрутизатора Vigor2865ax повністю звільняється від рутинної внутрішньої переадресації. Це дозволяє йому зосередити всі обчислювальні ресурси на глибокому аналізі зовнішніх пакетів (SPI Firewall), боротьбі з DDoS-атаками та криптографічному шифруванні віддалених підключень співробітників по тунелях WireGuard чи IPsec.

З точки зору реалізації, такий гібридний підхід є золотим стандартом мережевої інженерії. Комутатор VigorSwitch отримує IP-адреси у кожній VLAN і виступає шлюзом за замовчуванням (Default Gateway) для всіх ПК, камер та серверів. Права доступу між відділами гнучко обмежуються безпосередньо на ньому за допомогою списків контролю доступу (ACL). Далі на комутаторі прописується один статичний маршрут (Static Route 0.0.0.0/0), який спрямовує весь невідомий трафік — тобто запити в Інтернет — на IP-адресу маршрутизатора Vigor2865ax.

3.1.2 Конфігурування центрального комутаційного вузла

Використання дев'яти окремих віртуальних мереж дозволяє надійно ізолювати потоки даних, підвищити загальний рівень кібербезпеки та утилізувати повну швидкість комутаційної матриці пристрою без залучення обчислювальних потужностей зовнішнього маршрутизатора. Усі етапи налаштування виконуються виключно через графічний веб-інтерфейс (Web GUI) для мінімізації синтаксичних помилок та прискорення введення системи в експлуатацію.

Етап 1: Первинне підключення та авторизація:

1. Підключити робочу станцію (ПК або ноутбук) за допомогою патч-корду до будь-якого мідного порту комутатора (від 1 до 48).

2. Налаштувати на мережевому адаптері ПК статичну IP-адресу з підмережі комутатора, наприклад, 192.168.1.2 з маскою 255.255.255.0.

3. Відкрити веб-браузер та ввести заводську IP-адресу комутатора: 192.168.1.224.

4. На сторінці авторизації (див. рис. 3.1) ввести стандартні облікові дані (логін: admin, пароль: admin).

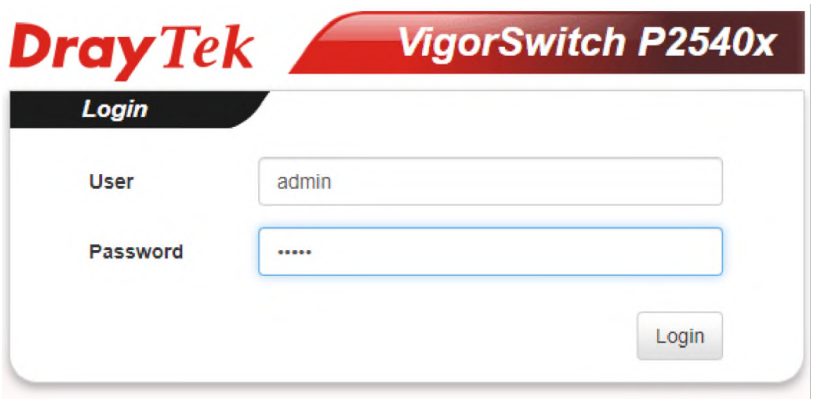

Рисунок 3.1 – Сторінка авторизації

5. Система автоматично запропонує змінити заводський пароль. Задати новий складний пароль для облікового запису адміністратора. Після чого відкриється головне вікно конфігурування (див. рис. 3.2).

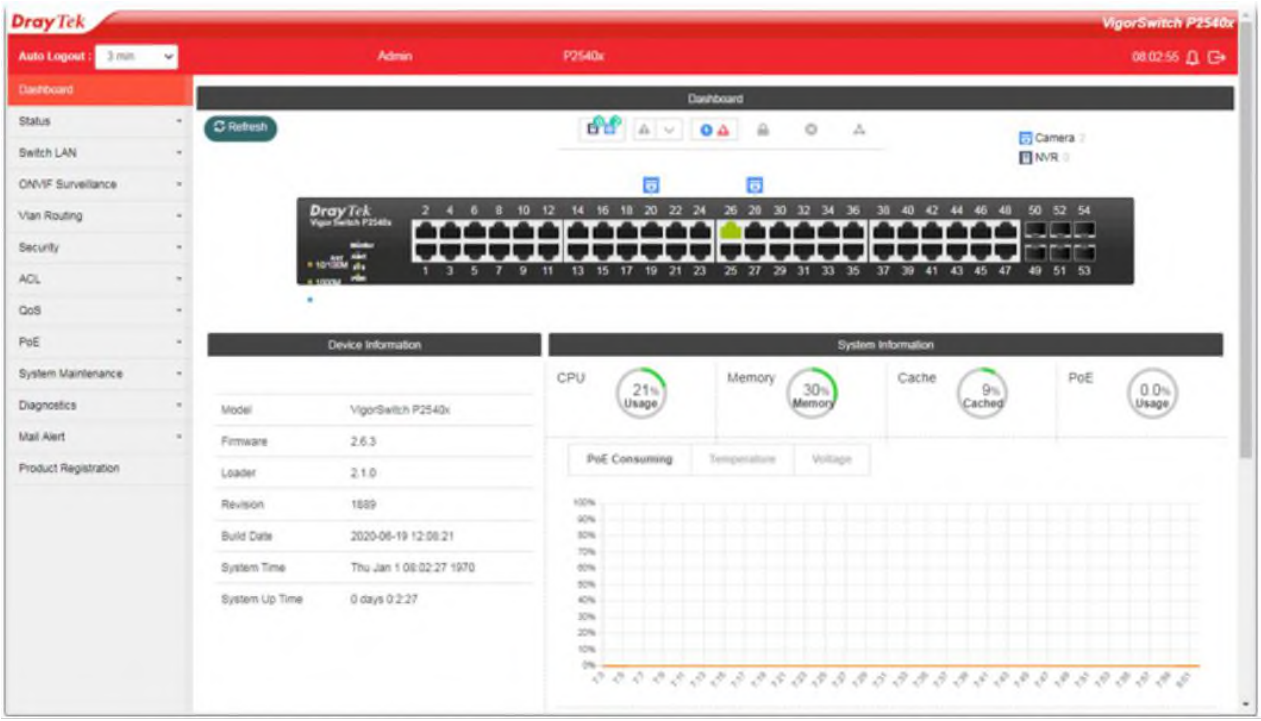

Рисунок 3.2 – Головне вікно конфігурування

Етап 2: Створення віртуальних локальних мереж (VLAN):

За допомогою послідовного додавання через кнопку Add створюються дев'ять обов'язкових віртуальних мереж із чіткою прив'язкою ідентифікаторів та назв. Адміністратор вносить у конфігурацію такі записи: VLAN 10 з назвою ADMIN, VLAN 20 з назвою DISPATCH, VLAN 30 з назвою ACCOUNTING, VLAN 40 з назвою IT, VLAN 50 з назвою SERVERS, VLAN 60 з назвою CLIENT_SERVICE, VLAN 70 з назвою GUEST_WIFI, VLAN 80 з назвою TECHNICAL та VLAN 90 з назвою VIDEO_REC.

1. У лівому навігаційному меню перейти до розділу Switch LAN.
2. Відкрити підрозділ VLAN Management та обрати вкладку Create VLAN.
3. Натиснути кнопку Add для створення нової віртуальної мережі.
4. У полі VLAN ID ввести числовий ідентифікатор для кожної підмережі (10, 20, 30, 40, 50, 60, 70, 80 і 90).
5. У полі VLAN Name ввести назви усіх підмереж.
6. Зберегти налаштування кнопкою Apply та повторити процедуру для всіх необхідних підмереж (див. рис. 3.3).

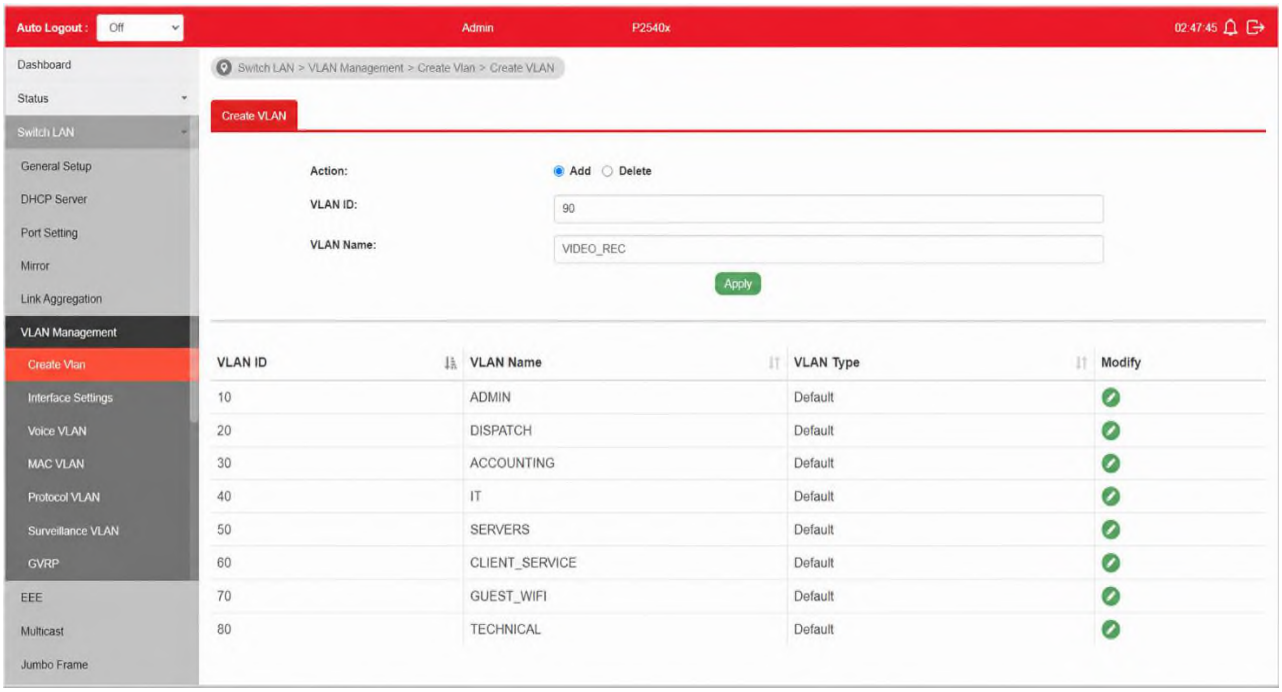

Рисунок 3.3 – Сторінка створення підмереж

Етап 3: Налаштування маршрутизації між VLAN (L3-інтерфейси):

Оскільки комутатор виконуватиме роль ядра мережі, йому необхідно призначити IP-адреси в кожній створеній VLAN. Ці адреси стануть «основними шлюзами» (Default Gateway) для кінцевих пристроїв у відповідних відділах.

1. Перейти до розділу Routing > Interface Settings.
2. Натиснути Add, щоб створити новий IP-інтерфейс.
3. Зі списку вибрати раніше створений VLAN ID (наприклад, 90 для VIDEO_REC).
4. У полі IP Address ввести першу адресу цієї підмережі (192.168.90.1), а в полі Subnet Mask — 255.255.255.0.
5. Зберегти зміни (Apply). Повторити дію для всіх підмереж. Тепер комутатор автоматично маршрутизуватиме трафік між відділами на апаратному рівні (див. рис. 3.4).

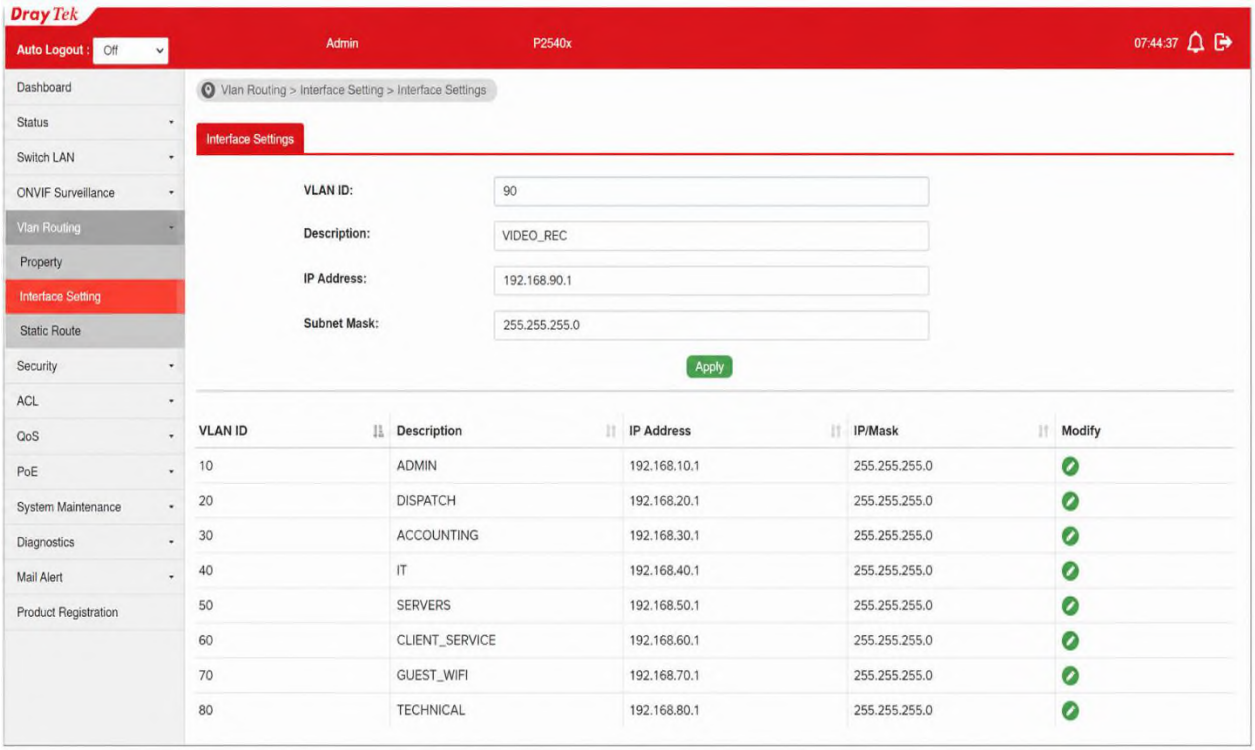

Рисунок 3.4 – Сторінка налаштування маршрутизації між VLAN

Етап 4: Конфігурація інтерфейсів (Access та Trunk порти):

Після створення VLAN необхідно розподілити фізичні порти комутатора відповідно до типу обладнання, яке до них підключатиметься.

1. Перейти до розділу Switch LAN > VLAN Management > Interface Settings.
2. Вибрати порти, до яких підключаються кінцеві пристрої (ПК користувачів, принтери, IP-камери, NAS).
3. Змінити параметр Port Type для цих портів на Access.
4. У полі PVID (Port VLAN ID) вкажіть ідентифікатор тієї мережі, до якої належить пристрій.
5. Вибрати магістральні порти (оптичні uplink-порти SFP+ для підключення до маршрутизатора Vigor2865ax та мідні порти для точок доступу VigorAP).
6. Змінити параметр Port Type на Trunk. Це дозволить пропускати через ці порти тегований трафік одразу кількох VLAN (див. рис. 3.5).
7. Збережіть внесені зміни кнопкою Apply.

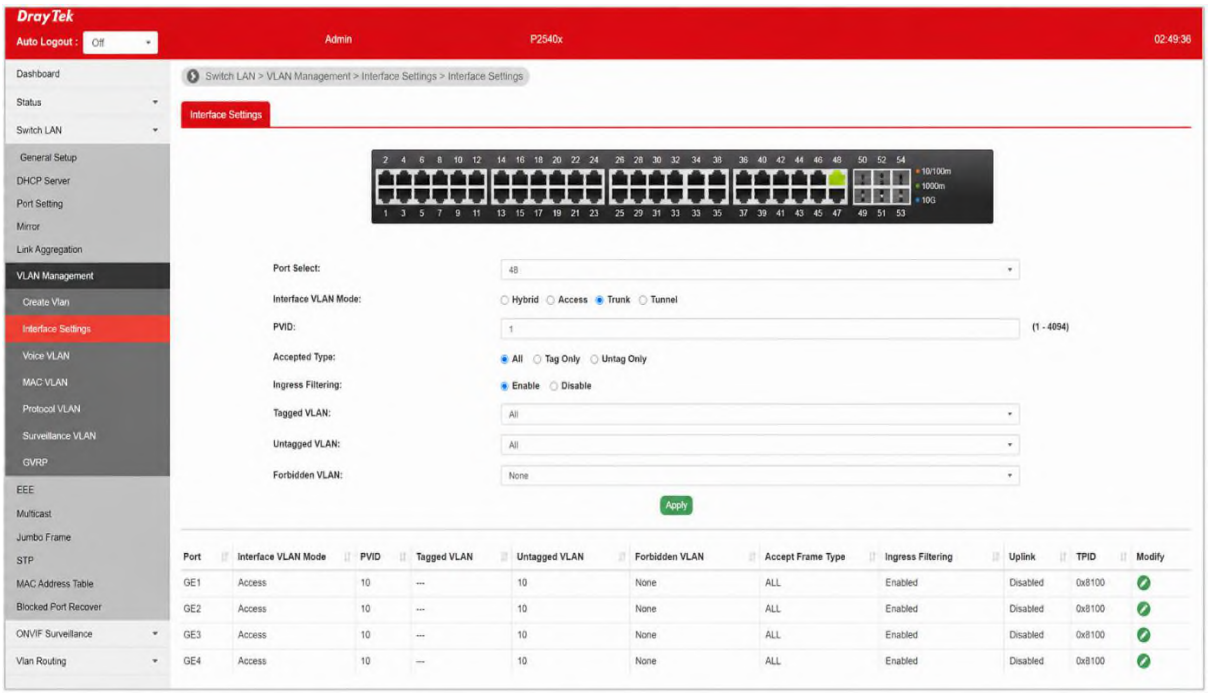

Рисунок 3.5 – Сторінка конфігурації інтерфейсів

Етап 5: Керування живленням (PoE):

Комутатор VigorSwitch P2540x підтримує подачу живлення на кінцеві пристрої. Цей функціонал необхідно для подачі напруги на IP-камери TVT та бездротові точки доступу DrayTek.

1. Перейти до головного меню PoE та відкрити розділ Port Setup.
2. У таблиці портів переконайтеся, що в колонці State для портів із підключеними камерами та точками доступу встановлено значення Enable.
3. За потреби, для критично важливих пристроїв (наприклад, центральних точок доступу або камер) можна підвищити пріоритет живлення у колонці Priority, змінивши його з Low на High або Critical. Це гарантує безперебійне живлення цих пристроїв у разі перевищення загального PoE-бюджету (див. рис. 3.6).
4. Натисніть Apply для застосування налаштувань.

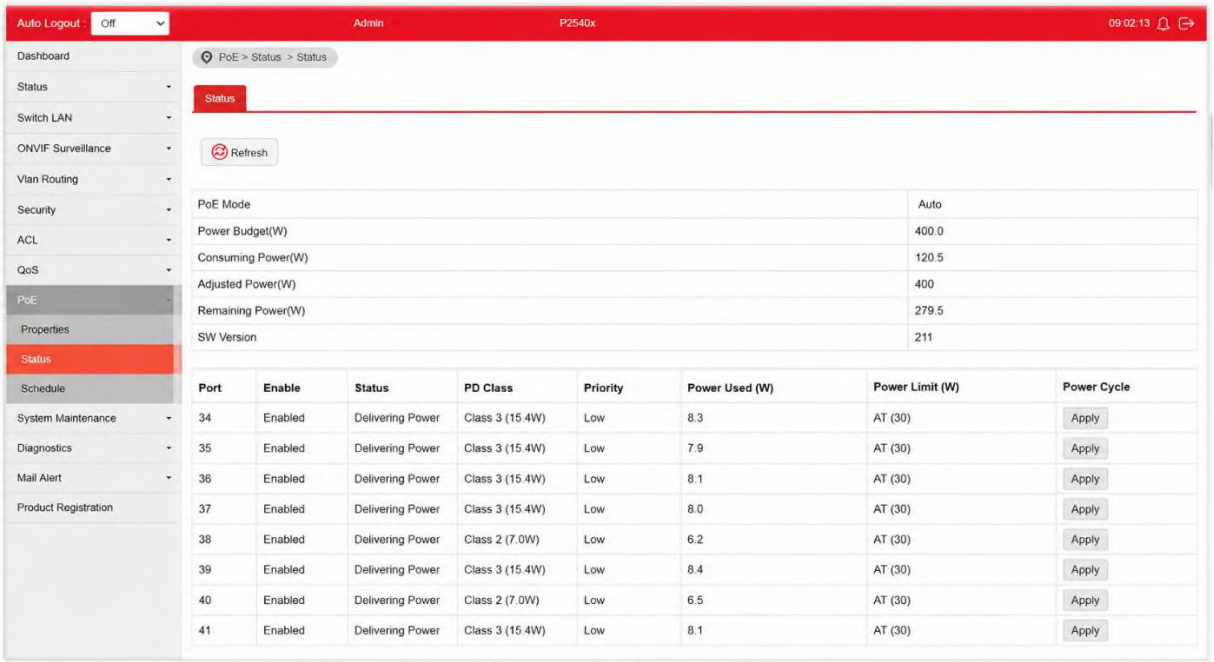

Рисунок 3.6 – Сторінка конфігурації PoE

Етап 6: Налаштування доступу в Інтернет (Static Route):

Щоб трафік, який не належить до внутрішніх відділів (наприклад, запити до веб-сайтів), успішно виходив в Інтернет, комутатору потрібно вказати шлях до головного маршрутизатора Vigor2865ax.

1. Перейти до розділу VLAN Routing > IPv4 Static Route.

2. Натиснути Add для додавання нового маршруту.

3. У полі Destination Address ввести 0.0.0.0, а в полі Subnet Mask також 0.0.0.0 (це означає «будь-який невідомий напрямок»).

4. У полі Next Hop (або Gateway) ввести IP-адресу маршрутизатора Vigor2865ax (192.168.50.254) (див. рис. 3.7).

5. Натиснути Apply.

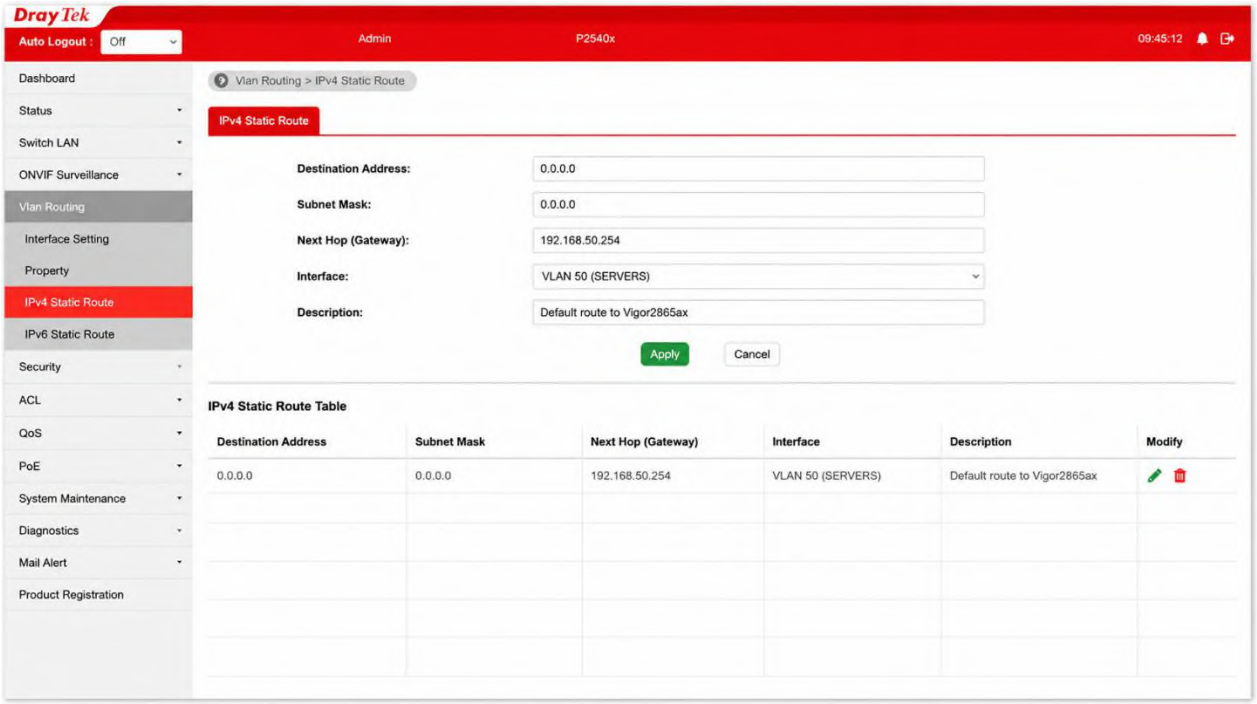

Рисунок 3.7 – Сторінка налаштування доступу в Інтернет

Етап 7: Збереження та резервне копіювання конфігурації:

Усі внесені через веб-інтерфейс зміни застосовуються в оперативній пам'яті (Running Config). Щоб вони не зникли після перезавантаження комутатора, їх обов'язково потрібно зберегти у незалежну пам'ять.

1. У верхньому правому куті веб-інтерфейсу натиснути іконку дискети або кнопку Save для фіксації налаштувань у Startup Config.

2. Для створення резервної копії налаштувань перейти до розділу System Maintenance > Configuration Backup.

3. Натиснути кнопку Backup, щоб завантажити файл із поточною конфігурацією на комп'ютер. Цей файл дозволить швидко відновити роботу мережі у разі апаратної заміни комутатора [18].

3.1.3 Конфігурування двох інтернет-каналів (основного та резервного) на маршрутизаторі DrayTek Vigor2865ax

Перед початком налаштування інтернет-каналів необхідно отримати доступ до панелі керування маршрутизатора через веб-інтерфейс.

Етап 1: Первинне підключення та авторизація:

1. Підключити робочу станцію (ПК або ноутбук) за допомогою патч-корду до будь-якого локального мідного порту маршрутизатора (інтерфейси LAN від 1 до 4).

2. Переконатися, що мережевий адаптер ПК налаштований на автоматичне отримання IP-адреси (DHCP клієнт), або задати статичну адресу з діапазону заводської підмережі, наприклад, 192.168.1.100 з маскою 255.255.255.0.

3. Відкрити веб-браузер і ввести стандартну заводську IP-адресу маршрутизатора: 192.168.1.1.

4. На сторінці авторизації, що відкрилася, ввести стандартні облікові дані адміністратора за замовчуванням (у полі Username ввести admin, у полі Password ввести admin).

5. Під час першого входу створити новий надійний адміністративний пароль, підтвердити його та зберегти зміни для захисту пристрою.

Етап 2: Активація фізичних портів (WAN1 та WAN2):

Спершу необхідно увімкнути порти, до яких підключені кабелі від інтернет-провайдерів, та задати їхню логіку роботи.

1. У лівому навігаційному меню сторінки конфігурування перейти до розділу WAN та відкрити підрозділ General Setup.

2. У таблиці натиснути на інтерфейс WAN1.

3. У полі Enable вибрати Yes, щоб активувати порт.

4. У полі Active Mode обрати логіку роботи каналу: Always On — якщо цей канал має працювати постійно (основний канал або для балансування навантаження) чи Backup — якщо цей канал має вмикатися лише тоді, коли зникає зв'язок на основному (у цьому режимі з'являться додаткові поля для вибору умови активації, наприклад, When WAN1 is disconnected) (див. рис. 3.8).

5. Натиснути OK для збереження.

6. Повторити ті ж дії (пункти 2–5) для інтерфейсу WAN2, куди підключено другого провайдера.

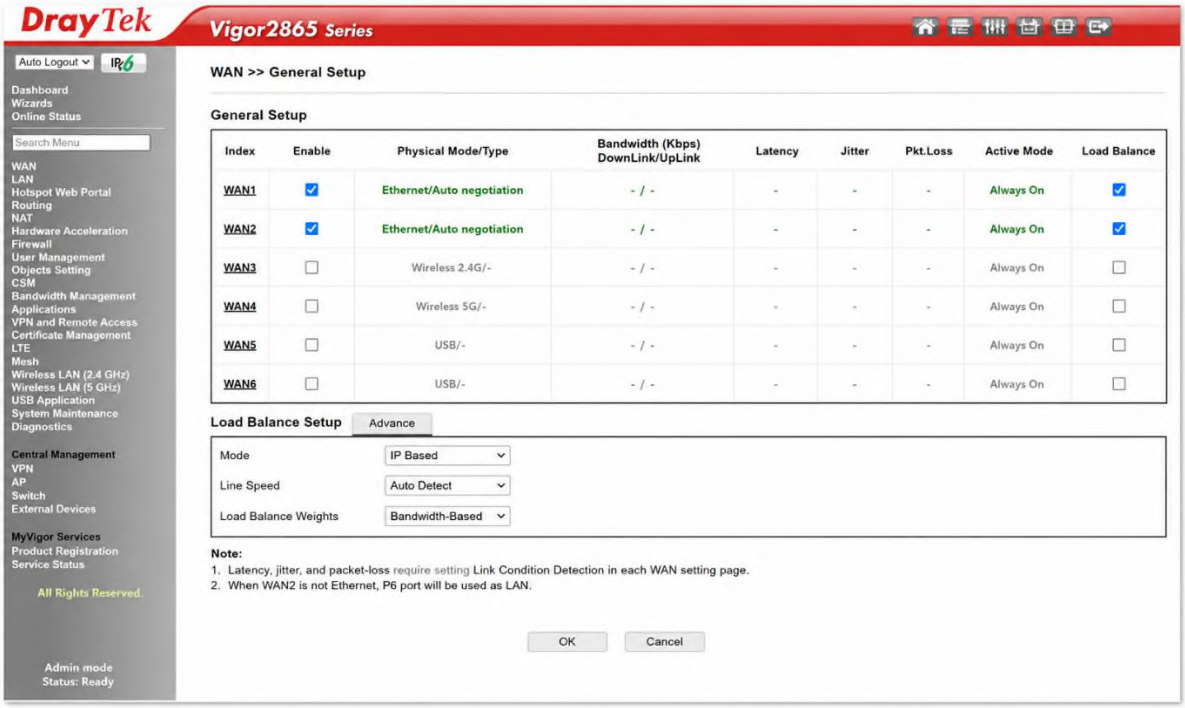

Рисунок 3.8 – Сторінка налаштування балансування WAN1 та WAN2

Етап 3: Налаштування доступу до Інтернету:

Після активації портів необхідно прописати налаштування, які надав кожен із провайдерів (тип підключення, логіни/паролі або статичні IP).

1. Перейти до розділу WAN > Internet Access.

2. Для інтерфейсу WAN1 у випадному списку Access Mode обрати тип підключення (Dynamic IP). Увімкнути Enable і обрати Obtain an IP address automatically (див. рис. 3.9).

3. Натиснути OK внизу сторінки для збереження та перезавантаження інтерфейсу.

4. Повторити пункти 2–5 для інтерфейсу WAN2 з даними від другого провайдера [21].

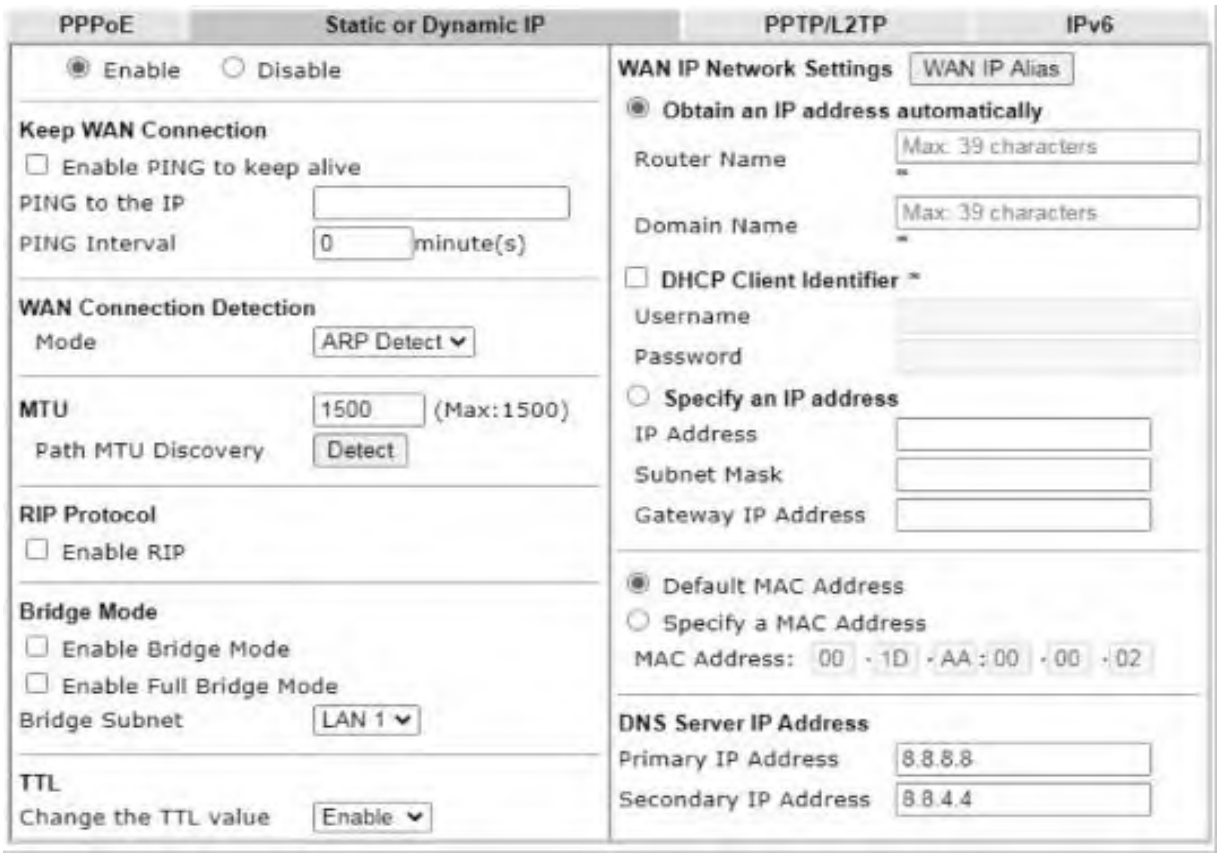

Рисунок 3.9 – Сторінка налаштування підключення до провайдера

3.1.4 Конфігурування безшовної Wi-Fi мережі на основі точок доступу DrayTek VigorAP 1060C

Для створення єдиної безшовної Wi-Fi мережі (де пристрої автоматично та непомітно перемикаються між трьома точками під час переміщення по коридорах приміщень) найкраще використати вбудовану технологію Mesh,

призначивши одну точку «Головною» (Mesh Root), а дві інші — «Підлеглими» (Mesh Node).

Такий підхід дозволяє налаштувати бездротову мережу лише один раз на головному пристрої, після чого налаштування (SSID, паролі та параметри роумінгу) автоматично синхронізуються на інші точки.

Етап 1: Підготовка та вхід до головної точки:

1. Підключити першу точку доступу (яка буде головною) кабелем до комутатора VigorSwitch P2540x (порт із подачею живлення PoE). Дві інші точки також увімкнути у відповідні порти комутатора.

2. Дізнатися IP-адресу першої точки (її можна подивитися в таблиці DHCP на маршрутизаторі Vigor2865ax).

3. Відкрити браузер і ввести цю IP-адресу.

4. Увійти у веб-інтерфейс, використовуючи стандартні облікові дані (логін: admin, пароль: admin). Змінити пароль на безпечний при першому вході.

Етап 2: Налаштування загальної Wi-Fi мережі (SSID та пароль)

Перед створенням групи потрібно задати назву мережі, яка буде спільною для всього офісу.

1. У лівому меню сторінки конфігурування перейти до Wireless LAN (2.4GHz) > General Setup.

2. У полі SSID ввести назву корпоративної мережі (Zhitlofond_Corp).

3. Натиснути OK, щоб зберегти.

4. Перейти до Wireless LAN (2.4GHz) > Security.

5. Обрати режим безпеки WPA2/PSK (або WPA2/WPA3) та ввести надійний пароль у поле Pass Phrase. Натиснути OK.

6. Повторити ці ж дії для діапазону 5 ГГц у меню Wireless LAN (5GHz) (див. рис. 3.10).

Етап 3: Активація безшовного перемикання:

Щоб смартфони та ноутбуки не «трималися» за далеку точку доступу до останнього, необхідно увімкнути протоколи швидкого роумінгу.

1. Перейти до меню Wireless LAN > Roaming.

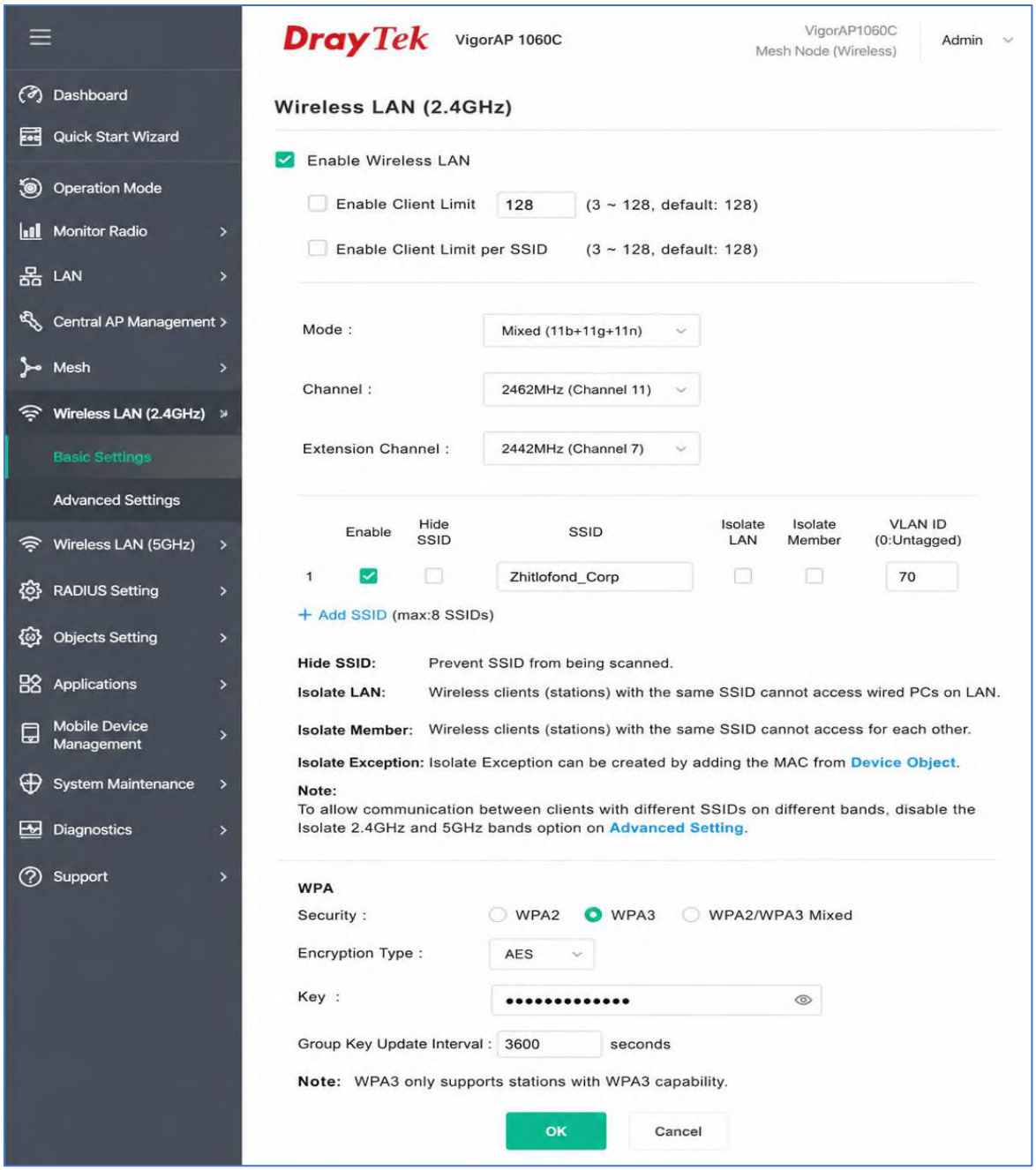

Рисунок 3.10 – Сторінка налаштування Wi-Fi мережі (SSID та пароль)

2. Увімкнути функцію Fast Roaming (це активує стандарти 802.11r/k/v, які дозволяють пристроям перемикатися між точками за мілісекунди без обриву зв'язку, наприклад, під час відеодзвінка).

3. Увімкнути AP-Assisted Client Roaming. Вказати поріг Strict Minimum RSSI (наприклад, -75 dBm). Це змусить точку доступу примусово відключати

клієнта, якщо сигнал стає занадто слабким, змушуючи його миттєво підключитися до ближчої точки доступу. Натиснути OK (див. рис. 3.11).

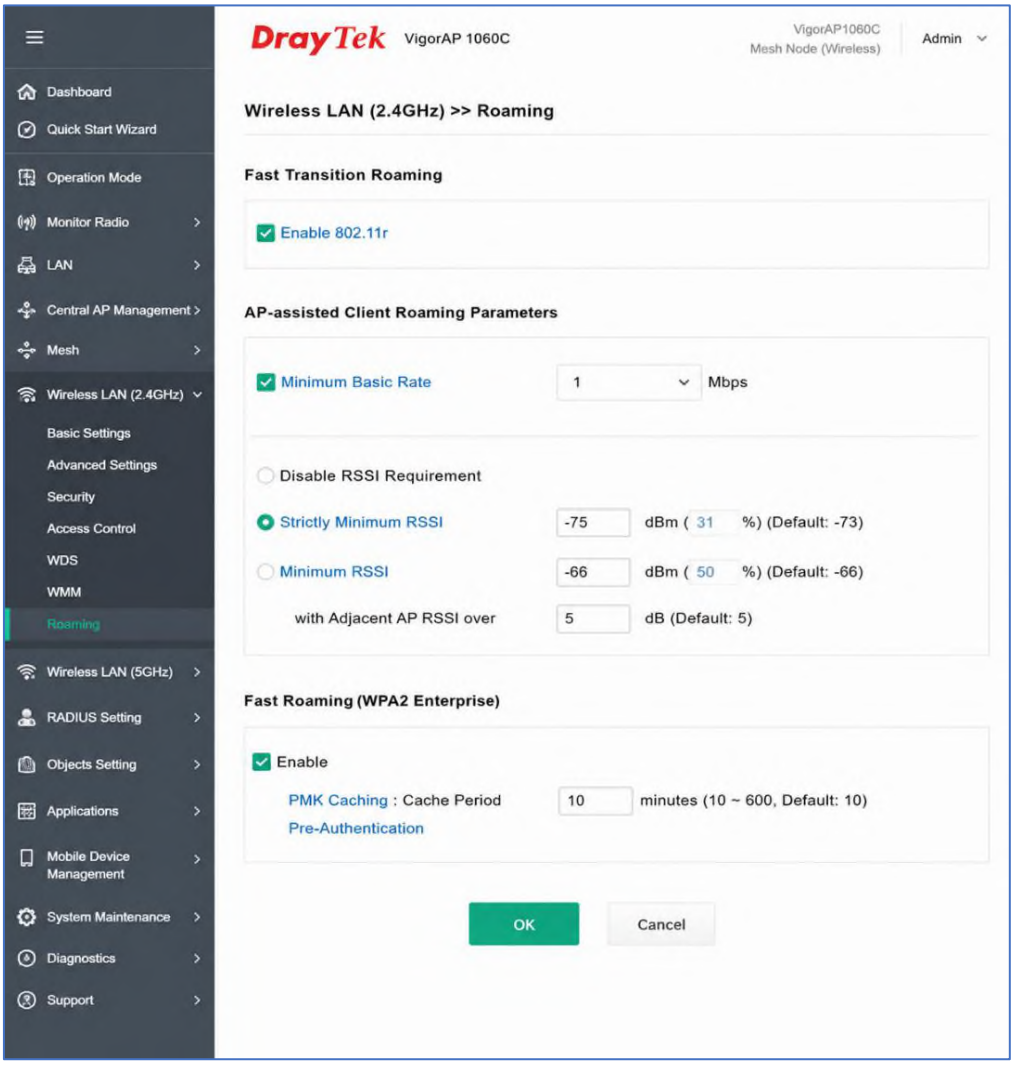

Рисунок 3.11 – Сторінка активації безшовного перемикання

Крок 4: Створення Mesh-групи та додавання інших точок:

Тепер необхідно «підпорядкувати» дві інші точки доступу до головної.

1. Перейти до головного меню Mesh > Mesh Setup.
2. Переконатися, що параметр Enable Mesh активовано (див. рис. 3.12).
3. У полі Mesh Mode обрати Mesh Root (Головний вузол).
4. Натиснути кнопку Search (Пошук), щоб просканувати мережу на наявність інших точок VigorAP 1060C.

5. У таблиці з'являться дві інші точки доступу. Виділити їх галочками.

6. Ввести адміністративний пароль від цих точок (або Device PIN-код, якщо вони не налаштовані) і натиснути Add to Mesh Group.

7.

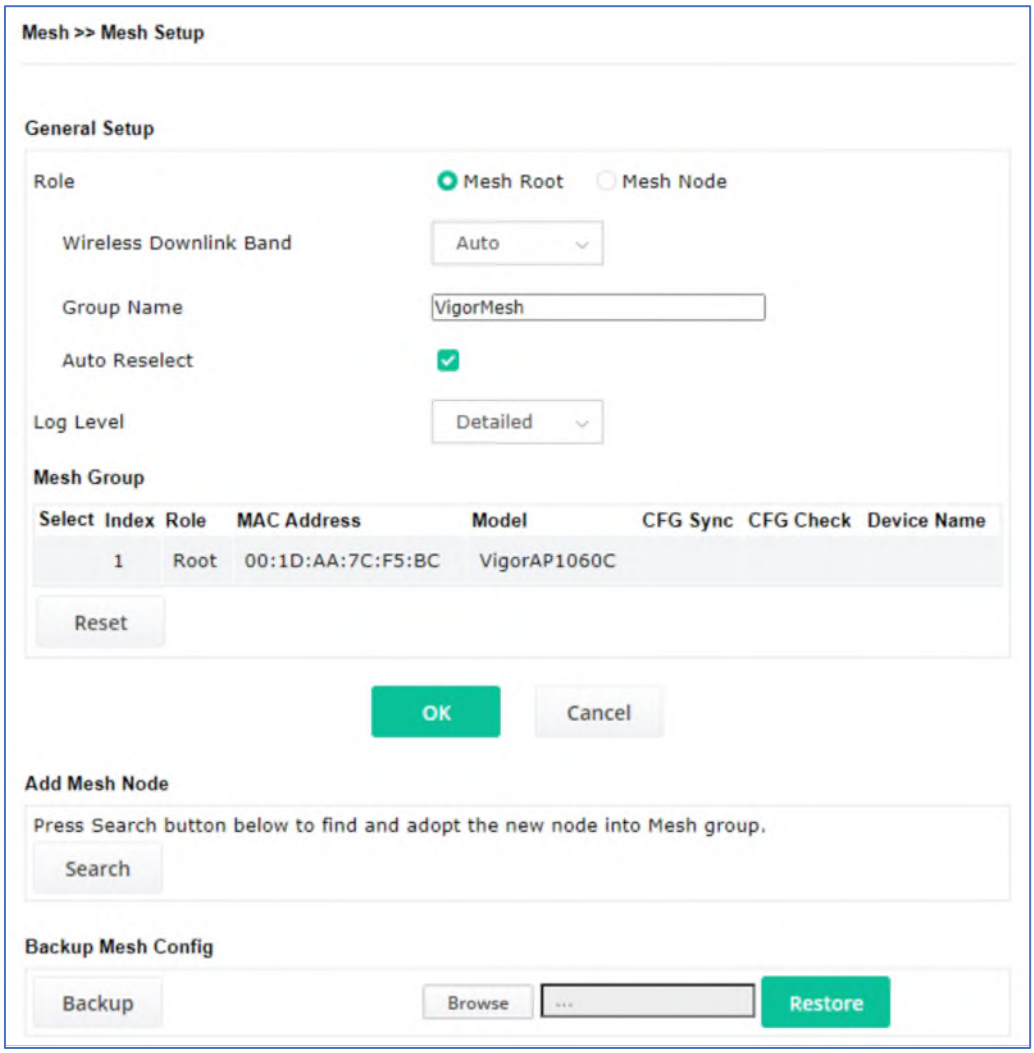

Рисунок 3.12 – Сторінка створення Mesh-групи та додавання інших точок

Етап 5: Перевірка статусу та синхронізація:

Після додавання підлеглих точок (Mesh Nodes) вони автоматично завантажать усі налаштування з головної точки.

1. Перейти до розділу Mesh > Mesh Status.

2. Відобразиться деревоподібна схема (топологія) бездротової мережі (див. рис. 3.13).

3. Переконатися, що всі три точки (Mesh Root та дві Mesh Node) мають статус Connected (Підключено).

4. Оскільки точки підключені до комутатора кабелями, система автоматично використає Ethernet Uplink (дротовий зв'язок) для обміну даними між собою, що гарантує максимальну швидкість без втрат по Wi-Fi, а сам радіоефір працюватиме як єдина безшовна мережа [24].

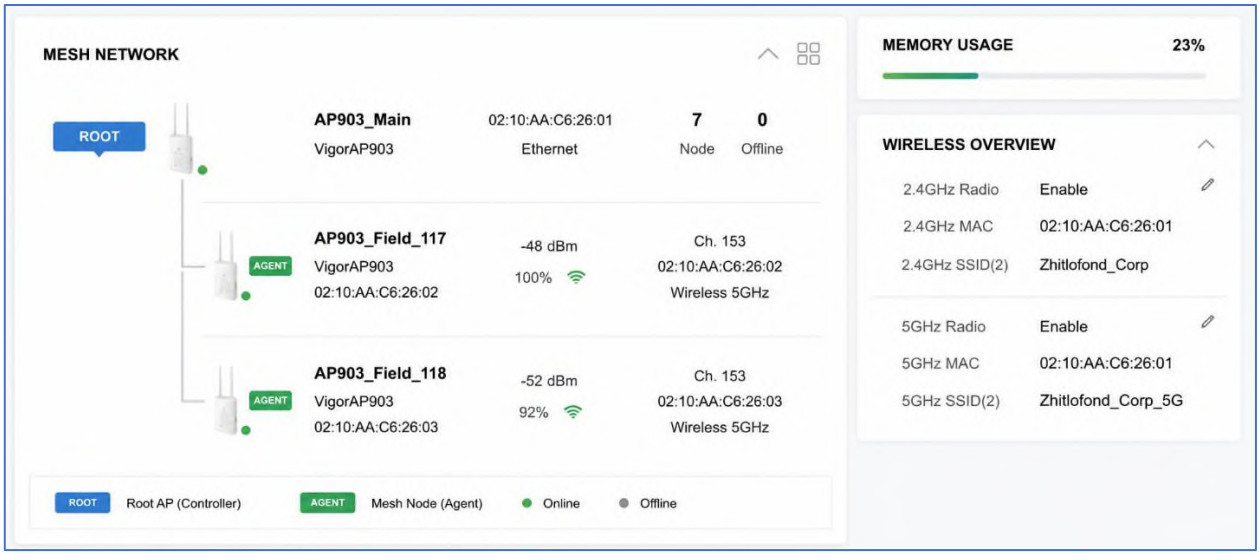

Рисунок 3.13 – Схема (топологія) бездротової мережі

3.2 Інструкція з конфігурування Synology DS1825+ (сервера S_1), як файлового сервера та системи бекапів

Для перетворення NAS Synology на надійний файловий сервер та систему бекапів після первинної ініціалізації пристрою та встановлення операційної системи DiskStation Manager (DSM) необхідно виконати такі дії:

Етап 1: Мережеві налаштування:

Оскільки Synology DS1825+ виступає в ролі ядра зберігання даних (VLAN 50 SERVERS), йому необхідна статична IP-адреса.

1. Увійти у веб-інтерфейс DSM через браузер (наприклад, за адресою http://find.synology.com або по поточній DHCP-адресі).

2. Відкрити панель керування (Control Panel) > Мережа (Network) > вкладка Мережевий інтерфейс (Network Interface).

3. Вибрати підключений LAN-порт (наприклад, LAN 1 або 10G-інтерфейс) і натиснути Редагувати (Edit).

4. Вибрати пункт Використовувати конфігурацію вручну (Use manual configuration).

5. Ввести заздалегідь визначені параметри:

IP-адреса: 192.168.50.200

Маска підмережі: 255.255.255.0

Шлюз (Gateway): 192.168.50.1 (див. рис. 3.14)

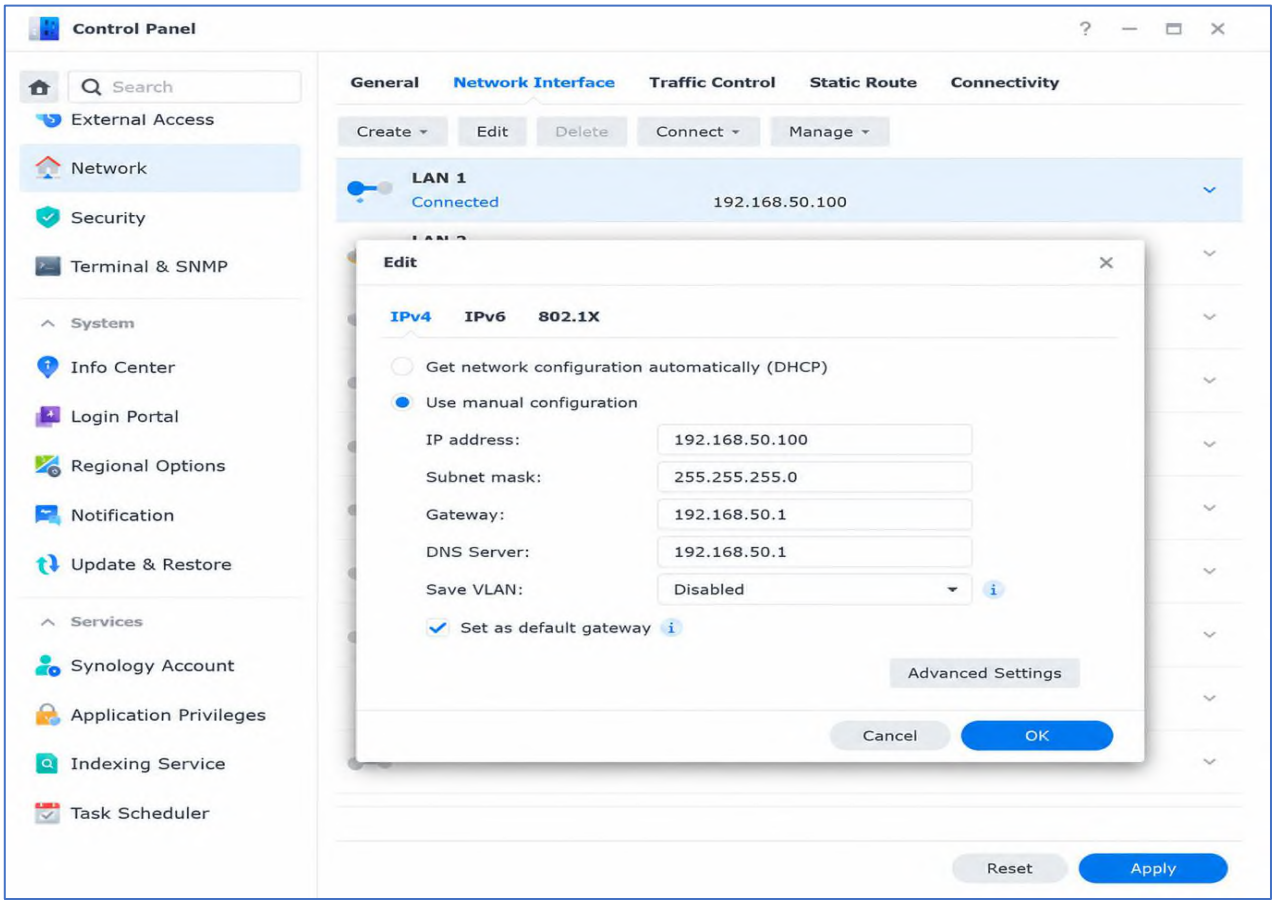

Рисунок 3.14 – Налаштування параметрів мережі сервера S_1

6. Натиснути OK. Підключення до інтерфейсу перерветься. Увійти знову за новою статичною адресою 192.168.50.200.

Етап 2: Створення простору для зберігання (Storage Pool & Volume):

Перш ніж створювати папки, необхідно об'єднати фізичні жорсткі диски в логічний масив (RAID).

1. Відкрити Диспетчер зберігання (Storage Manager) з головного меню.

2. Перейти до розділу Сховище (Storage) і натиснути Створити (Create) > Пул зберігання (Storage Pool).

3. Обрати тип RAID (для 2-дискового NAS оптимальним балансом між надійністю та об'ємом є RAID 1, що витримує вихід з ладу одного з дисків).

4. Вибрати жорсткі диски, які увійдуть до пулу, і дотримуватись вказівок майстра для форматування.

5. Після створення пулу натиснути Створити (Create) > Том (Volume).

6. Обрати створений пул зберігання і як файлову систему обов'язково вказати Btrfs (вона підтримує знімки (snapshots) для захисту від вірусів-шифрувальників) (див. рис. 3.15).

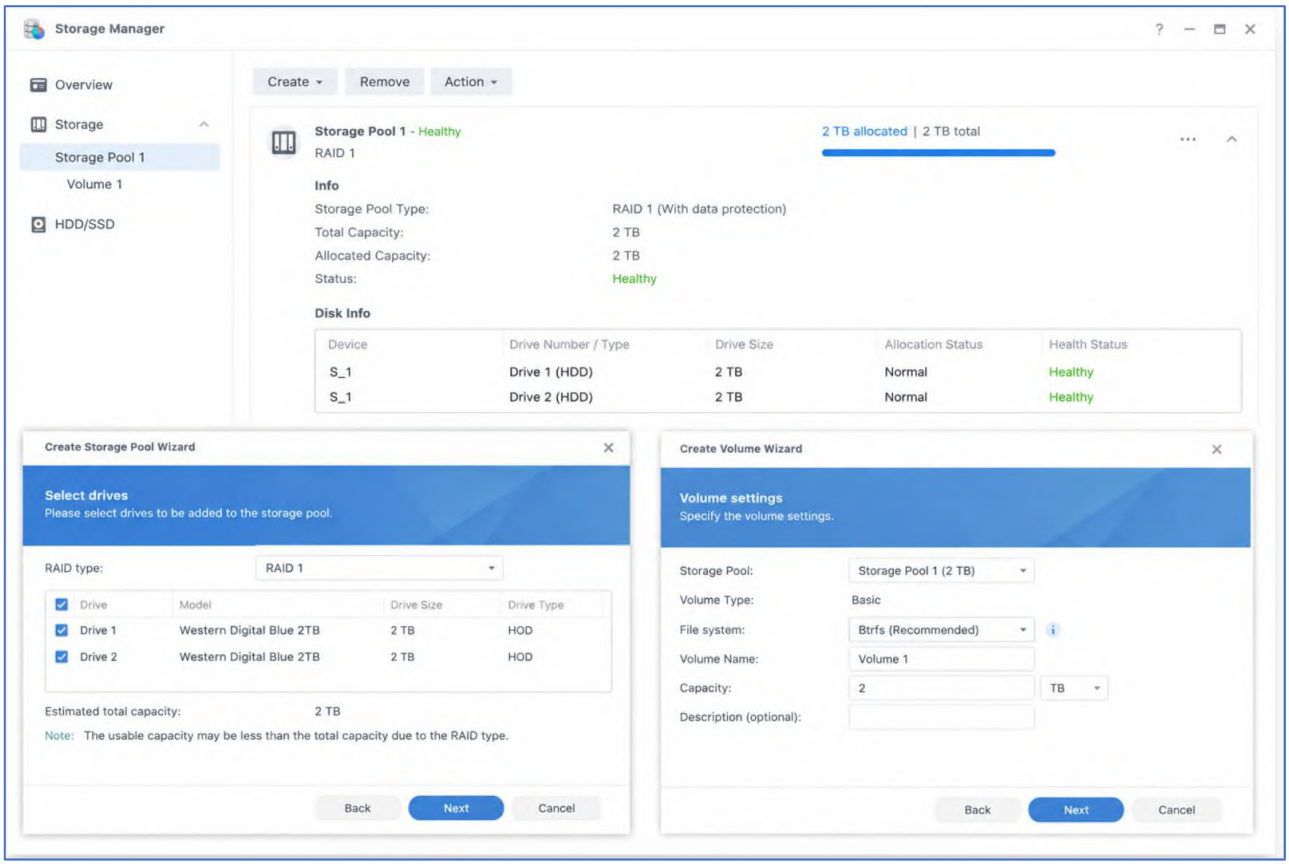

Рисунок 3.15 – Створення простору для зберігання на S_1

Етап 3: Налаштування файлового сервера (Спільні папки):

1. Відкрити Панель керування (Control Panel) > Спільна папка (Shared Folder).

2. Натиснути Створити (Create). Створіть необхідні папки для кожного відділу, наприклад:

Ім'я: Accounting_Share (для VLAN 30)

Ім'я: IT_Admin (для VLAN 40)

3. Під час створення папки обов'язково встановити галочку Увімкнути контрольні суми даних для розширеної цілісності (Enable data checksum for advanced data integrity) (доступно тільки на Btrfs).

4. Після створення папки відкриється вікно дозволів. Надати відповідні права доступу (Читання/Запис або Тільки читання) для груп або конкретних користувачів.

5. Для підключення до папок з Windows-ПК користувачі можуть використовувати провідник: \\192.168.50.200\Accounting_Share.

Етап 4: Налаштування сервера резервного копіювання:

Synology має потужні безкоштовні інструменти для бекапів, зокрема Active Backup for Business, який дозволяє централізовано створювати резервні копії комп'ютерів та серверів.

1. Відкрити Центр пакунків (Package Center).

2. Знайти і встановити додаток Active Backup for Business.

3. Запустити додаток і пройти безкоштовну активацію через обліковий запис Synology (необхідний доступ в інтернет).

4. У додатку перейти до розділу ПК (PC) або Фізичний сервер (Physical Server) і згенерувати інсталяційний файл агента.

5. Встановити цього агента на комп'ютери бухгалтерів чи інші важливі ПК.

6. Після підключення ПК до NAS, в Active Backup for Business створити Завдання (Task) для регулярного бекапування цих пристроїв (наприклад, щодня о 23:00) за технологією інкрементного копіювання.

Етап 5: Налаштування захисту від шифрувальників (Snapshot Replication)

Для захисту самих файлових папок на NAS від випадкового видалення або атак програм-вимагачів:

1. Встановити додаток Snapshot Replication із Центру пакунків.

2. Запустити його, перейти до розділу Знімки (Snapshots).

3. Вибрати спільні папки (наприклад, Accounting_Share) і натиснути Налаштування (Settings).

4. Налаштувати розклад (наприклад, робити знімок кожні 4 години) та політику зберігання (наприклад, зберігати останні 30 знімків). Це дозволить миттєво відкотити вміст папки у разі пошкодження файлів [25]; [26].

3.3 Інструкція з конфігурування системи відеонагляду TVT

Ця інструкція описує процес налаштування 16-канального мережевого відеореєстратора (S_2) TVT TD-3316H2-B2-B та підключення до нього купольних IP-камер TVT TD-9584SL-C-& у виділеному захищеному сегменті мережі (VLAN 90 VIDEO_REC).

Етап 1: Мережеві налаштування відеореєстратора:

Оскільки NVR є центральним сервером для камер, йому необхідно призначити статичну IP-адресу з виділеної підмережі відеоспостереження.

1. Підключити NVR кабелем до порту комутатора DrayTek, налаштованого як Access VLAN 90. Підключити монітор (через HDMI) та мишу до NVR.

2. Увімкнути реєстратор і дочекатися завантаження. При першому запуску система запропонує створити пароль адміністратора. Створити надійний пароль та графічний ключ для швидкого доступу.

3. Клацнути правою кнопкою миші на головному екрані та обрати Головне меню (Main Menu).

4. Перейти до розділу Мережа (Network) > TCP/IP.

5. Зняти галочку з отримати IP-адресу автоматично (Obtain an IP address automatically / DHCP).

6. Ввести заздалегідь визначені параметри для мережі:

IP-адреса (IP Address): 192.168.90.200

Маска підмережі (Subnet Mask): 255.255.255.0

Шлюз (Default Gateway): 192.168.90.1 (див. рис. 3.16).

Рисунок 3.16 – Сторінка налаштування параметрів відеосервера

7. Натиснути Застосувати (Apply) для збереження налаштувань.

Етап 2: Налаштування IP-камер TVT:

Камери підключаються до портів комутатора DrayTek, які налаштовані як Access VLAN 90 з активованою функцією PoE для подачі живлення.

1. Камери TVT за замовчуванням зазвичай мають IP-адресу 192.168.226.201 або отримують її по DHCP. Найкраще налаштовувати їх через утиліту IP Tool на комп'ютері, тимчасово підключеному до VLAN 90.

2. Підключити ПК до порту комутатора (Access VLAN 90) і задати йому статичну адресу (наприклад, 192.168.90.2).

3. Запустити утиліту TVT IP Tool (зазвичай йде на диску в комплекті або завантажується з сайту виробника).

4. Утиліта знайде всі підключені камери. Виділити першу камеру.

5. Змінити її IP-адресу на статичну з виділеного діапазону (192.168.90.101, маска 255.255.255.0, шлюз 192.168.90.1).

6. Повторити процедуру для всіх інших камер, призначаючи їм унікальні адреси (192.168.90.102, 192.168.90.103, 192.168.90.104, 192.168.90.105).

7. Зайти через веб-браузер на IP-адресу кожної камери, авторизуватись (зазвичай admin/123456) і змінити стандартний пароль на безпечний. Це обов'язкова вимога для корпоративної безпеки.

Етап 3: Додавання камер до відеореєстратора:

Після того, як камери отримали правильні IP-адреси, їх потрібно прописати в NVR.

1. На реєстраторі (через підключений монітор або веб-інтерфейс за адресою 192.168.90.200) відкрити Головне меню > Камера (Camera) > Додати камеру (Add Camera).

2. Натиснути кнопку Швидке додавання (Quick Add) або Пошук (Search).

3. NVR просканує мережу VLAN 90 і знайде всі камери (від .101 до .105).

4. Виділити потрібні камери галочками і натиснути Додати (Add) (див. рис. 3.17):

5. Система запропонує ввести логін і пароль від камер (ті, що задані на Етапі 2, пункт 7). Ввести їх.

6. Статус камер у списку має змінитися на «Підключено» (або з'явиться зелений індикатор), і з’явиться зображення на екрані.

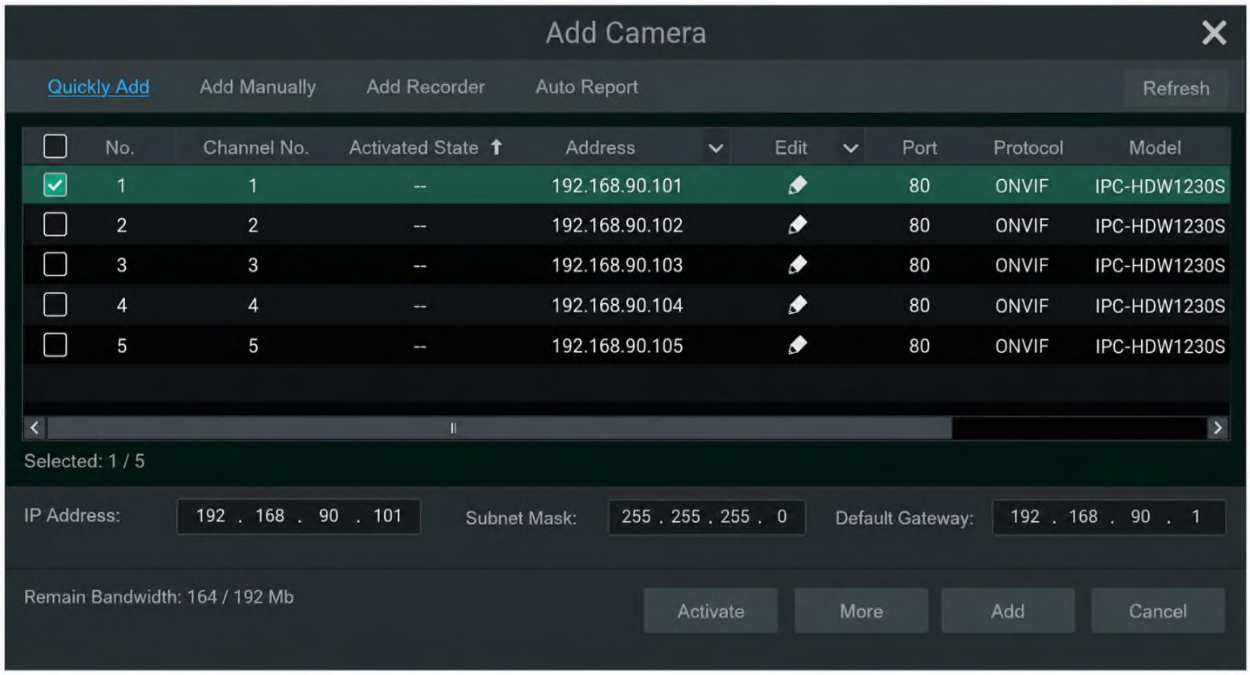

Рисунок 3.17 – Сторінка додавання камер

Етап 4: Налаштування запису та якості:

1. Перейти до Головне меню > Запис (Record) > Налаштування запису (Record Settings).

2. Вибрати канал (камеру) або всі канали відразу.

3. Встановити розклад запису (найчастіше це Постійний запис (Continuous) 24/7 або запис За рухом (Motion) для економії місця). Натиснути Застосувати.

4. Перейти до Головне меню > Камера (Camera) > Кодування (Encoding) / Відео (Video).

5. Для кожної камери налаштувати параметри основного потоку (Main Stream), який пишеться на диск:

Роздільна здатність: 8MP.

Частота кадрів (FPS): зазвичай достатньо 15-20 кадрів в секунду.

Тип бітрейту: Змінний (VBR).

Відеокодек: Обов'язково H.265 або H.265+ (це суттєво зменшить розмір відеоархіву порівняно зі старим H.264).

6. Натиснути Застосувати [27].

3.4 Інструкція з тестування працездатності мережі інструментами DrayTek

Тест №1: Перевірка маршрутизації між відділами (Inter-VLAN Routing):

Мета: Переконатися, що пристрої з різних віртуальних мереж «бачать» один одного (наприклад, Бухгалтерія має доступ до Сервера).

1. Увійти у веб-інтерфейс комутатора VigorSwitch P2540x.

2. Перейти до розділу Diagnostics > Ping.

3. У полі IP Address ввести адресу пристрою з іншого відділу (наприклад, 192.168.50.100 — IP-адреса сервера Synology S_1).

4. Натиснути кнопку Ping.

В результаті буде отримао 4 успішні відповіді (Reply from...). Якщо відповідей немає, перевірити налаштування L3-інтерфейсів та ACL (списки контролю доступу).

Тест №2: Перевірка безшовного роумінгу Wi-Fi (Mesh):

Мета: Переконатися, що клієнтські пристрої миттєво перемикаються між трьома точками доступу без обриву зв'язку.

1. Увійти у веб-інтерфейс маршрутизатора Vigor2865ax.

2. Перейти до Central AP Management > Station List. Буде відображено список усіх підключених Wi-Fi пристроїв та точки, до яких вони зараз під'єднані.

3. Підключити смартфон до корпоративного Wi-Fi і запустити безперервний пінг до будь-якого вузла (наприклад, через додаток PingTools до 8.8.8.8 або локального шлюзу 192.168.10.1).

4. Рухатись по офісу від однієї точки доступу до іншої.

В результаті в інтерфейсі Station List (після оновлення) смартфон змінюватиме прив'язку до різних точок (MAC-адреси AP). У додатку на смартфоні не повинно бути втрачених пакетів (максимум 1-2 стрибки затримки).

Тест №3: Перевірка балансування інтернет-каналів (Load Balancing):

Мета: Перевірити, що трафік дійсно розподіляється між двома провайдерами (WAN1 та WAN2).

1. Увійти у веб-інтерфейс маршрутизатора Vigor2865ax.
2. Перейти до Diagnostics > Data Flow Monitor.
3. Натиснути Enable, щоб запустити моніторинг у реальному часі.
4. На кількох комп'ютерах в офісі запустити завантаження великих файлів або тест швидкості (Speedtest).

В результаті у таблиці Data Flow Monitor відобразяться активні сесії. У колонці Interface має відображатися як WAN1, так і WAN2, що підтверджує коректний розподіл навантаження.

Тест №4: Перевірка навантаження PoE (Живлення камер та AP):

Мета: Переконатися, що комутатор має достатній запас потужності для всього обладнання.

1. Запустити програму VigorConnect (або зайти у веб-інтерфейс комутатора VigorSwitch P2540x у розділ PoE > Status).
2. Відкрити графік споживання енергії (PoE Power Consumption).

В результаті відобразиться поточне навантаження у Ватах. Переконатися, що загальне споживання всіх камер TVT та точок доступу не наближається до максимального ліміту комутатора (400 Вт). Бажано мати щонайменше 20% вільного запасу потужності [18]; [21].

3.5 Інструкція з конфігурування базового захисту мережі за допомогою фаєрвола

Налаштування та перевірка базового захисту мережі (Firewall) з метою обмежити доступ до критично важливих сегментів мережі (наприклад, серверів) ззовні та між ізольованими відділами:

1. Увійти у веб-інтерфейс маршрутизатора Vigor2865ax (або комутатора, якщо ACL налаштовуються на ньому).

2. Перейти до Firewall > Filter Setup. За замовчуванням увімкнено Default Data Filter, який дозволяє весь вихідний трафік.

3. Для створення нового правила натиснути на вільний індекс у таблиці (наприклад, 2).

4. Налаштувати правило, щоб блокувати небажаний трафік. Наприклад, щоб заборонити доступ з гостьової мережі Guest_WiFi (VLAN 70) до мережі серверів Servers (VLAN 50):

5. Увімкнути правило (Enable).

У полі Source (Джерело) вказати підмережу Guest_WiFi (192.168.70.0/24).

У полі Destination (Призначення) вказати підмережу Servers (192.168.50.0/24).

У полі Action (Дія) обрати Block або Drop.

6. Натиснути OK, щоб застосувати налаштування.

7. Перевірити дієвість правила, підключивши пристрій до гостьової мережі Wi-Fi (VLAN 70) та спробувавши пропінгувати адресу сервера (192.168.50.10). Запити мають блокуватися (повідомлення «Request timed out»), що підтверджує надійну роботу фаєрвола [21].

3.6 Інструкція з моніторингу працездатності мережі

Моніторинг мережі виконується з метою відстеження навантаження, аналіз трафіку та своєчасного виявлення потенційних проблем в інфраструктурі.

1. Огляд загального стану (Dashboard): Увійти у веб-інтерфейс маршрутизатора Vigor2865ax. Відразу на головній сторінці Dashboard перевірити статус фізичних портів (WAN/LAN), поточне завантаження процесора (CPU) та використання оперативної пам'яті (див. рис. 3.18). Зелені індикатори лінків свідчать про нормальну роботу підключень.

2. Аналіз поточного трафіку: Перейти до розділу Diagnostics > Data Flow Monitor та натиснути кнопку Enable. Це дозволить у реальному часі бачити, які пристрої (за IP-адресами) споживають найбільше трафіку, скільки сесій вони відкрили та через який інтернет-канал (WAN1 чи WAN2) ідуть дані.

3. Візуалізація пропускної здатності: Перейти до меню Diagnostics > Traffic Graph. Тут у вигляді графіків відображається поточна швидкість прийому (RX) та передачі (TX) даних. Це допоможе швидко виявити «вузькі місця» або моменти пікового навантаження на інтернет-канали.

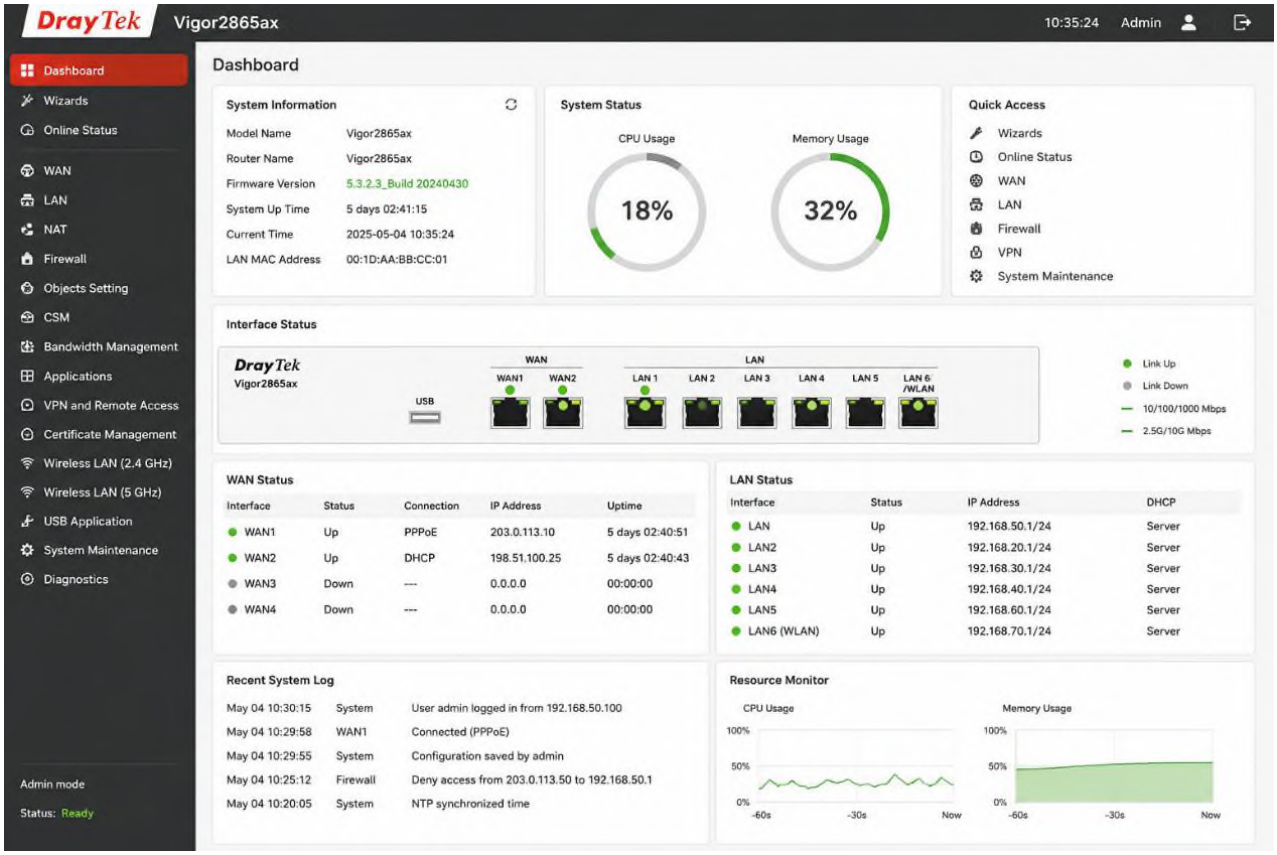

Рисунок 3.18 – Огляд загального стану КМ у веб-інтерфейс маршрутизатора Vigor2865ax

4. Централізований моніторинг обладнання: Для перевірки стану комутаторів перейти до Central Switch Management > Status, щоб побачити активність портів та загальний статус підключення комутатора VigorSwitch P2540x.

5. Для моніторингу точок доступу Wi-Fi перейти до Central AP Management > Status, де відображається статус (онлайн/офлайн) для всіх пристроїв VigorAP та кількість підключених до них бездротових клієнтів [21].

3.7 Моделювання мережі

Після розробки логічної схеми мережі було виконано її моделювання в програмному середовищі Cisco Packet Tracer (див. рис. 3.19). Для цього на робочому полі було розміщено усе мережеве обладнання відповідно до проєктної структури: маршрутизатор, керований комутатор рівня L2/L3, сервер Synology DS1825+ (S_1), сервер відеоспостереження (S_2), точки доступу бездротової мережі, робочі станції, банківські термінали, мережеві принтери та IP-камери.

На комутаторі було створено та налаштовано віртуальні локальні мережі VLAN: VLAN 10 – VLAN 90.

Для забезпечення взаємодії між мережевими сегментами було реалізовано міжмережеву маршрутизацію (Inter-VLAN Routing). Кожному VLAN призначено окрему IP-підмережу та шлюз за замовчуванням.

У процесі моделювання виконано перевірку коректності функціонування мережі за допомогою інструментів Simulation Mode та Packet Capture. Було здійснено тестування передачі пакетів між вузлами однієї VLAN, а також перевірено маршрутизацію між різними VLAN.

Для контролю доступності мережевих ресурсів використано команди Ping та Tracert. Результати тестування підтвердили коректну роботу маршрутизації, відсутність конфліктів адресації та правильність налаштування комутації.

Окремо було виконано перевірку доступності серверів S_1 та S_2, мережевих принтерів, IP-телефонів і камер відеоспостереження. Усі пристрої успішно обмінювалися пакетами в межах дозволених політик доступу.

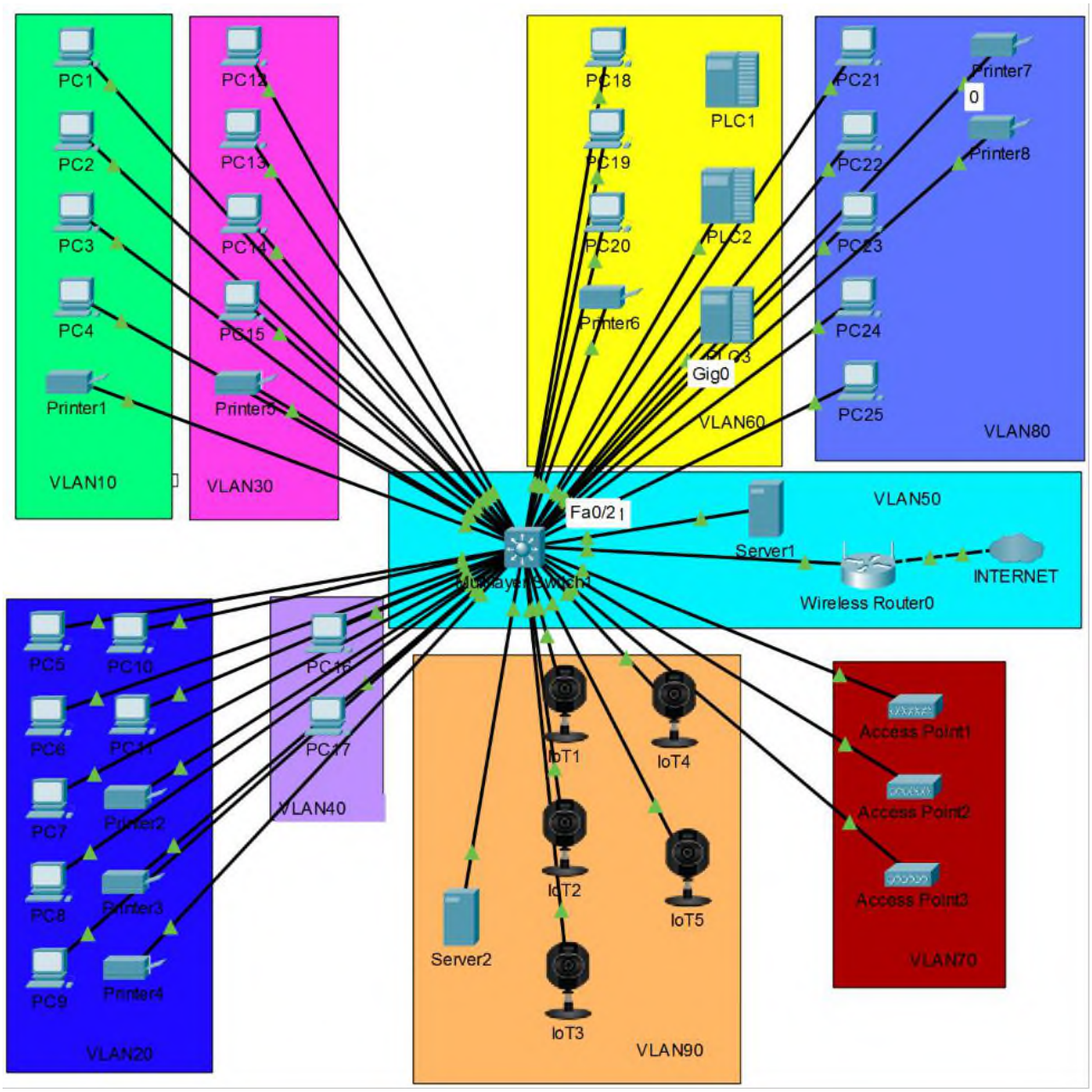

Рисунок 3.19 – Моделювання КМ в Cisco Packet Tracer

Моделювання в Cisco Packet Tracer дозволило перевірити працездатність мережевої інфраструктури ще до її фізичного впровадження, виявити можливі помилки конфігурації та підтвердити відповідність розробленої мережі технічним вимогам проєкту.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи бакалавра є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проєкту комп'ютерної мережі ПП «УК «ЖИТЛОФОНД».

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР доцільно дані витрат часу по окремих операціях технологічного процесу звести у таблицю 4.1.

Таблиця 4.1 – Середній час виконання НДР та стадії (операції) технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Передпроєктне обстеження об’єкта	керівник проєкту	2
2.	Формування технічних вимог до мережі	керівник проєкту	2
3.	Розробка фізичної структури мережі	інженер	12
4.	Проєктування кабельної інфраструктури	інженер	8
5.	Розробка логічної структури мережі	інженер	12
6.	Проєктування системи інформаційної безпеки	інженер	8

Продовження таблиці 4.1

1	2	3	4
7.	Підбір обладнання та матеріалів	керівник проєкту	8
8.	Підготовка комплекту проєктної документації	інженер	8
9.	Монтаж і налагодження мережі	технік	40
10.	Тестування та приймання мережі	інженер	4
11.	Введення в експлуатацію та супровід	керівник проєкту	2
Разом			106

Сумарний час виконання операцій технологічного процесу становить 106 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці - грошовий вираз вартості і ціни робочої сили, який виступає у формі будь-якого заробітку, виплаченого керівником підприємства найманому працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів його роботи, регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата розраховується за формулою 4.1:

$$З_{осн.}=Т_с \cdot К_г \,, \qquad (4.1)$$

де Тс – тарифна ставка, грн.; Кг – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проєкту – 320 грн./год., інженер – 220 грн./год., технік – 120 грн./год.

Основна заробітна плата становить:

1. Керівник проєкту: $З_{осн1} = 320 \cdot 14 = 4480$ грн.;

2. Інженер: $З_{осн2} = 220 \cdot 52 = 11440$ грн.;

3. Технік: $З_{осн3} = 120 \cdot 40 = 4800$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 44800 + 11440 + 4800 = 20720 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати та обчислюється за формулою 4.2:

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (4.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам: 0,1–0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проєкту: $З_{дод1} = 4480 \cdot 0,1 = 448,00$ грн.;

2. Інженер: $З_{дод2} = 11440 \cdot 0,1 = 1144,00$ грн.;

3. Технік: $З_{дод3} = 4800 \cdot 0,1 = 480,00$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод} = 448,00 + 1144,00 + 480,00 = 2072,00 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою 4.3:

$$В_{о.п.} = З_{осн.} + З_{дод.}, \quad (4.3)$$

$$В_{о.п} = 20720,00 + 2072,00 = 22792,00 \text{ грн.}$$

Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде обчислюватися за формулою 4.4:

$$B_{с.з.} = ФОП \cdot 0,22, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 22792,00 \cdot 0,22 = 5014,24 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітня плата, грн.	Нарахування на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тарифна ставка, грн.	Кількість відпрацьованих год.	Фактично нарахована заробітня плата, грн.			
1	Керівник проєкту	320	14	4480	448,00	-	-
2	Інженер	220	52	11440	1144,00	-	-
3	Технік	120	40	4800	480,00	-	-
Разом				20720	2072,00	5014,24	27806,24

Загальні витрати на оплату праці становлять 27806,24 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни (формула 4.5):

$$М_{Вi} = q_i \cdot p_i, \quad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду; p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.}=\sum M_{Bi} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Назва елемента	Одиниці виміру	Кількість	Ціна одиниці, грн.	Загальна сума витрат, грн.
1	2	3	3	4	5
1	Комутатор DrayTek VigorSwitch P2540x	шт.	1	46296	46296
2	Маршрутизатор DrayTek Vigor2865ax	шт.	1	17555	17555
3	Точка доступу DrayTek VigorAP 1060C	шт.	3	20625	61875
4	NAS Synology DS1825+	шт.	1	76757	76757
5	IP-відеореєстратор TVT TD-3316H2-B2-B	шт.	1	14940	14940
6	IP-камера TVT TD-9584SL-C(D/PE/AW2)	шт.	5	5744	28720
7	Шафа серверна підлогова 42U глибина 675 мм чорний CMS UA-MGSE4266MB	шт.	1	38528	38528

Продовження таблиці 4.3

1	2	3	5	4	6
8	Вентиляторний блок в дах для шаф MGSE CMS UA-MGSE-F3MB	шт.	1	4165	4165
9	Полиця консольна 300 мм 19" 1U черна CMS UA-SHC300B	шт.	2	477	954
10	Фільтр мережевий 19” на 8 розеток Clever AUE2250D3-08LMCPMB	шт.	1	1822	1822
11	Патч-панель екранована мережева RJ-45 19" 24 порта cat.6 1U FTP з органайзером 6PLDN-F24BK	шт.	2	3644	7288
12	Кабельний організатор 19" 1U з кришкою EPN PLMN-060Z	шт.	2	555	1110
13	ДБЖ Cover CORE 3K	шт.	1	41673	41673
14	Кабель вита пара F/UTP категорія 6 4x2x0.54 бухта 305 м OK-Net	шт.	4	11246	44984
15	Патч-корд S/FTP LSOH 0.5 м cat.6 сірий Premium Line 18642005L	шт.	44	143	6292
16	Патч-корд S/FTP LSOH 3 м cat.6 сірий Premium Line 18642030L	шт.	41	309	12669

Продовження таблиці 2.9

1	2	3	5	4	6
17	Розетка настінна на 1 порт RJ-45 FTP cat.6 EPNew 6BX-S1WHA6	шт.	41	137	5617
18	DKC лоток перфорований 100х50 гарячого цинкування	м	122	175	21350
19	Кабельний канал 15х10 мм білий серія LH Kopos LH 15X10_HD, 2м	шт.	33	37	1221
20	Серверний жорсткий диск для систем відео-спостереження Lenovo ThinkSystem 4XB7A83970 2.5" 2.5ТБ SAS	шт.	2	14587	29174
21	Серверний жорсткий диск для NAS систем Western Digital Blue SATA III 2TB	шт.	2	7799	15598
Разом					448914

Загальна сума матеріальних витрат на розробку проєкту комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» становить 448914 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію визначаються за формулою 4.7:

(4.7)

$$З_е = W \cdot T \cdot S$$

де W – необхідна потужність, кВт; Т – кількість годин роботи обладнання; S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 64 години, споживана потужність - 0,8 кВт/год., вартість 1 кВт електроенергії – 15,94 грн.

Тому витрати на електроенергію будуть становити:

$$З_е = 0,8 \cdot 64 \cdot 15,94 = 816,13 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8-10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8, де $Т_В$ – транспортні витрати.

$$Т_в = З_{м.в.} \cdot 0,08..0,1,, \quad (4.8)$$

Отже, транспортні витрати будуть становити:

$$Т_В = 448914 \cdot 0,1 = 44891,40 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп’ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань застосовуємо формулу 4.9:

$$А = \frac{Б_В \cdot Н_А}{150\%} \cdot Т_А \quad (4.9)$$

де А – амортизаційні відрахування за звітний період, грн.; $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; $Н_А$ – норма амортизації, %.

Враховуючи, що ноутбука працює над даним проектом 64 год., його балансова вартість – 26999 грн., тому:

$$А = \frac{26999 \cdot 0{,}04}{150} \cdot 64 = 460{,}78 \text{ грн.}$$

4.7 Обчислення накладних витрат

Накладні витрати - це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом певних умов роботи по організації, управлінню та обслуговуванню виробництва.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10, де $Н_В$ – накладні витрати.

$$Н_в = В_{о.п.} \cdot 0{,}2 \ldots 0{,}6, \qquad (4.10)$$

$$Н_В = 22792{,}40 \cdot 0{,}3 = 6837{,}60 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат являє собою зведений план усіх витрат підприємства на майбутній період виробничо-фінансової діяльності.

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 – Кошторис витрат НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	22792	4,32
Відрахування на соціальні заходи	5014,24	0,95
Матеріальні витрати	448914	85,09
Витрати на електроенергію	816,13	0,15
Транспортні витрати	35913,12	6,81
Амортизаційні відрахування	460,78	0,09
Накладні витрати	13675,2	2,59
Собівартість	527585,47	100

Собівартість ($С_в$) НДР розрахуємо за формулою 4.11:

$$С_В=В_{о.п.}+В_{с.з.}+З_{м.в.}+З_в+Т_в+А+Н_в \quad (4.11)$$

Отже, собівартість дорівнює $С_В$ = 527585,47 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12: де Св – собівартість виконання НДР, $Р_{рен.}$ – рівень рентабельності; ПДВ – ставка податку на додану вартість, 20%.

$$Ц = Св \cdot (1+Ррен) \cdot (1+ПДВ), \quad (4.12)$$

Ц = 527585,47·(1+0,3)·(1+0,2)=823033,33 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Прибуток розраховується за формулою 4.13:

$$П = Ц - С_в \quad (4.13)$$

П = 823033,33 - 527585,47 = 295447,86 грн.

Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14, де П – прибуток; $С_в$ – собівартість.

$$Е_р = П / С_в, \quad (4.14)$$

$$Е_р = 295447,86 / 527585,47 = 0,56$$

Поряд із економічною ефективністю розраховують (формула 4.15) термін окупності капітальних вкладень $Т_р$:

$$Т_р = 1 / Е_р \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку:

$$Т_р=1/0,56=1,8$$

Всі дані внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники проєкту комп'ютерної мережі ПП «УК «ЖИТЛОФОНД»

№п/п	Показник	Одиниця виміру	Значення
1.	Собівартість	грн.	527585,47
2.	Плановий прибуток	грн.	295447,86
3.	Ціна	грн.	823033,33
4.	Економічна ефективність	-	0,56
5.	Термін окупності	рік	1,8

Загальна вартість спроєктованої комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» становить 823033,33 грн.

Зважаючи на високі показники економічної ефективності - 0,56, кошти, вкладені в проведення проектних робіт окупляться за 1,8 року.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

5.1 Дотримання вимог пожежної безпеки в ПП «УК «ЖИТЛОФОНД»

Організація пожежної безпеки на підприємстві починається з чіткого розподілу відповідальності та належного документообігу. Керівництво має видати наказ про призначення осіб, відповідальних за пожежний стан як по підприємству загалом, так і в кожному окремому кабінеті. Усі працівники, від абонентського відділу до диспетчерського центру, зобов'язані проходити первинний та щорічний протипожежні інструктажі. Водночас персонал, залучений до робіт у приміщеннях з підвищеною небезпекою, повинен додатково проходити навчання з пожежно-технічного мінімуму. Це гарантує, що кожен співробітник знатиме порядок дій у разі задимлення чи спрацювання сигналізації.

Оскільки приміщення ПП «УК «ЖИТЛОФОНД» використовується для розміщення офісного персоналу, комп'ютерної техніки, мережевого обладнання та паперової документації, воно належить до адміністративних приміщень з помірним пожежним навантаженням. Основними джерелами потенційного займання є електрообладнання, кабельні лінії, блоки живлення комп'ютерної техніки та джерела безперебійного живлення.

З огляду на лінійне коридорне планування офісу, критично важливим є бездоганне утримання шляхів евакуації. Центральні коридори, основні та запасні двері мають бути завжди вільними від коробок, архівів чи тимчасового сміття. Категорично забороняється захаращувати меблями евакуаційні проходи; зокрема, балконні двері в кабінетах за жодних обставин не повинні перекриватися столами чи іншим інвентарем, адже це може стати фатальною перешкодою під час паніки. Крім того, евакуаційні виходи повинні забезпечувати безперешкодне відкривання дверей у напрямку евакуації відповідно до вимог чинних нормативних документів, а після закінчення робочого дня всі побутові електроприлади необхідно відключати від мережі.

Телекомунікаційна кімната є зоною найвищого пожежного ризику через високу концентрацію навантаженого обладнання. Оскільки вся мережева архітектура підприємства не має периферійних вузлів і повністю зав'язана на єдиному центральному комутаторі DrayTek VigorSwitch P2540x, куди стікається трафік з усіх дев'яти підмереж (від VLAN10 ADMIN до VLAN90 VIDEO_REC), та серверах Synology DS1825+, ця стійка виділяє багато тепла. Серверна вимагає безперебійної роботи системи кондиціонування для запобігання перегріву блоків живлення. У разі виникнення короткого замикання в цьому приміщенні дозволяється використовувати виключно вуглекислотні вогнегасники, оскільки порошкові вогнегасники небажано використовувати для гасіння електронного обладнання, оскільки порошок може спричинити пошкодження електронних компонентів та ускладнити подальшу експлуатацію обладнання.

Електроживлення серверного та мережевого обладнання повинно здійснюватися через окрему електричну групу з автоматичними вимикачами захисту від перевантаження та короткого замикання. Для захисту обладнання від аварійних режимів мережі доцільно використовувати джерела безперебійного живлення з функцією автоматичного коректного завершення роботи серверів та мережевих сховищ.

Для оперативного локального реагування на займання вся будівля має бути рівномірно забезпечена сертифікованими первинними засобами пожежогасіння. Для приміщень з великою кількістю паперової документації (архів, бухгалтерія, відділ роботи зі зверненнями громадян) доцільно використовувати порошкові вогнегасники, які ефективно справляються з горінням твердих речовин. Натомість біля кабінетів з великою кількістю комп'ютерної техніки слід розміщувати вуглекислотні вогнегасники. Усі вогнегасники повинні висіти у легкодоступних місцях, не перекривати прохід, мати цілі пломби та актуальні бирки про проходження щорічного технічного обслуговування.

Обов’язковою умовою безпечного функціонування офісу є наявність автоматичної пожежної сигналізації та системи оповіщення про пожежу. Для забезпечення оперативного виведення людей з будівлі на видних місцях у коридорах розміщуються затверджені графічні плани евакуації (див. рис. 5.1). Вони чітко вказують маршрути руху до основного та запасних виходів, а також місця розташування первинних засобів пожежогасіння, що дозволяє уникнути паніки та ефекту «пляшкового горла» під час позаштатних ситуацій. Справність пожежної сигналізації та системи оповіщення повинна періодично перевірятися відповідальними особами з фіксацією результатів у відповідній документації.

Рисунок 5.1 – План евакуації

У разі виявлення ознак пожежі працівник повинен негайно повідомити про подію за телефоном 101, активувати систему оповіщення (за наявності), повідомити керівництво підприємства та розпочати евакуацію згідно із затвердженим планом евакуації. За умови відсутності загрози життю допускається використання первинних засобів пожежогасіння для локалізації осередку займання до прибуття підрозділів ДСНС [4].

5.2 Аналіз небезпеки ураження електричним струмом та заходи електробезпеки під час обслуговування серверного обладнання та комутаційних вузлів ПП «УК «ЖИТЛОФОНД»

Відповідно до умов експлуатації серверна кімната належить до приміщень без підвищеної небезпеки ураження електричним струмом, оскільки характеризується нормальною температурою повітря, відсутністю струмопровідного пилу, агресивного середовища та підвищеної вологості.

Специфіка серверної інфраструктури підприємства полягає у високій концентрації обчислювальних та мережевих потужностей у єдиному вузлі. Апаратна архітектура базується на єдиному центральному керованому комутаторі DrayTek VigorSwitch P2540x, до якого підключається все без винятку обладнання, оскільки інші комутатори в топології відсутні. Разом із мережевими сховищами, такими як Synology DS1825+, це створює локалізоване джерело підвищеної електричної та теплової небезпеки. Основний ризик ураження струмом формується через постійне живлення великої кількості портів, наявність високоємних блоків живлення та джерел безперебійного живлення, компактно розміщених в одній телекомунікаційній шафі.

Окрім прямого дотику до струмопровідних частин, серйозну загрозу становить накопичення статичної електрики на металевих корпусах обладнання. Такий розряд може не лише пошкодити чутливі електронні компоненти комутатора чи NAS, а й спричинити неконтрольований

рефлекторний рух працівника, що в тісних умовах серверної кімнати часто призводить до механічних травм. Можливий пробій ізоляції кабелів у щільно заповненій стійці здатний викликати появу небезпечної напруги на шафі. Через відсутність периферійних комутаторів будь-які апаратні зміни вимагають безпосереднього доступу персоналу до головного магістрального вузла живлення та передачі даних, що об'єктивно збільшує частоту потенційно небезпечних контактів.

Головним принципом безпеки в умовах використання єдиного центрального комутатора є мінімізація фізичних втручань у роботу обладнання на користь віддаленого керування. Мережа підприємства чітко сегментована на логічні підмережі. Завдяки такій структурі абсолютну більшість завдань із перерозподілу доступу, ізоляції трафіку чи підключення нових вузлів інженери повинні виконувати програмно через вебінтерфейс. Це дозволяє повністю уникати ручного перемикання патч-кордів під напругою та зводить до нуля ризик випадкового дотику до струмопровідних елементів стійки.

Під час виконання ремонтних або профілактичних робіт персонал повинен використовувати індивідуальні засоби захисту: діелектричні рукавички, інструмент з ізольованими ручками, антистатичні браслети та захисне взуття. До виконання робіт допускаються лише працівники, які пройшли відповідне навчання та інструктаж з електробезпеки.

Перед початком будь-яких невідкладних фізичних робіт з апаратною частиною, як-от додавання дисків у Synology DS1825+ або профілактичне чищення системи охолодження DrayTek, обладнання необхідно повністю знеструмити. Виняток становлять лише процедури «гарячої заміни» (hot-swap), які прямо дозволені інструкцією виробника. Усі роботи мають виконуватися виключно з використанням сертифікованого діелектричного інструменту та антистатичних браслетів, надійно підключених до загального контуру заземлення серверної. Інженер зобов'язаний перед кожним сеансом обслуговування візуально перевіряти цілісність захисного заземлення

металевих корпусів комутатора, серверів та телекомунікаційної шафи. Категорично забороняється залишати відкритими клеми джерел безперебійного живлення та допускати хаотичне скупчення кабелів живлення, що підвищує ризик їх механічного пошкодження і короткого замикання.

Крім того, всі металеві дверцята та напрямні телекомунікаційної шафи повинні мати надійне електричне з'єднання (перемички) для вирівнювання потенціалів та унеможливлення ураження струмом у разі пробою ізоляції на корпус [3].

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було успішно вирішено актуальне науково-практичне завдання — спроєктовано, обґрунтовано та сконфігуровано комплексну корпоративну інформаційно-обчислювальну мережу для підприємства ПП «УК «ЖИТЛОФОНД». Запропонована архітектура базується на сучасному обладнанні екосистеми DrayTek, серверних рішеннях Synology та системах відеонагляду TVT, що в сукупності забезпечує високу продуктивність, надійність та безпеку інфраструктури.

За результатами проведеної роботи можна зробити наступні основні висновки:

1. Реалізовано апаратну L3-маршрутизацію та логічну сегментацію: Використання керованого комутатора ядра DrayTek VigorSwitch P2540x дозволило розділити загальну мережу на 9 ізольованих віртуальних сегментів (VLAN 10–90). Перенесення маршрутизації між відділами на рівень комутатора (L3) дозволило досягти маршрутизації пакетів на максимальній швидкості портів без перенавантаження центрального маршрутизатора.

2. Забезпечено високу відмовостійкість інтернет-з'єднання: Налаштування маршрутизатора DrayTek Vigor2865ax з використанням двох паралельних каналів зв'язку (Dual WAN) та протоколів балансування навантаження гарантує безперебійний доступ до глобальної мережі та захист від відключень з боку провайдерів.

3. Розгорнуто безшовну бездротову інфраструктуру: Впровадження трьох точок доступу DrayTek VigorAP 1060C із застосуванням технології Mesh та протоколів Fast Roaming (802.11r/k/v) створило єдиний Wi-Fi простір. Це забезпечило мобільність працівників та стабільне підключення при переміщенні територією підприємства.

4. Побудовано надійний центр зберігання даних: Інтеграція NAS-сервера Synology DS1825+ дозволила створити централізоване файлове сховище з розмежуванням прав доступу на базі файлової системи Btrfs.

Впровадження інструментів Active Backup for Business та Snapshot Replication гарантує захист корпоративних даних від апаратних збоїв та вірусів-шифрувальників.

5. Інтегровано ізольовану систему фізичної безпеки: Проєктування окремої віртуальної мережі (VLAN 90 VIDEO_REC) для IP-камер та відеореєстратора TVT захистило відеотрафік від несанкціонованого доступу та виключило його вплив на пропускну здатність робочих мереж підприємства. Живлення камер реалізовано централізовано через технологію PoE з комутатора ядра.

6. Впроваджено багаторівневий захист інформації: Налаштування правил доступу (ACL) та брандмауера на маршрутизаторі дозволило суворо регламентувати трафік між відділами, ізолювати гостьову мережу та захистити сервери від зовнішніх та внутрішніх загроз.

7. Економічна ефективність проєкту: Загальна вартість спроєктованої комп'ютерної мережі ПП «УК «ЖИТЛОФОНД» становить 823033,33 грн. Зважаючи на високі показники економічної ефективності - 0,56, кошти, вкладені в проведення проектних робіт, окупляться за 1,8 року.

8. Проаналізовано та враховано дотримання вимог пожежної безпеки в ПП «УК «ЖИТЛОФОНД», а також проведено аналіз небезпеки ураження електричним струмом та заходи електробезпеки під час обслуговування серверного обладнання та комутаційних вузлів ПП «УК «ЖИТЛОФОНД».

Розроблена корпоративна мережа підприємства ПП «УК «ЖИТЛОФОНД» повністю відповідає сучасним стандартам масштабованості, кібербезпеки та відмовостійкості. Усі поставлені в роботі завдання виконано в повному обсязі, а запропонована інфраструктура готова до практичної експлуатації та подальшого розширення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Журавська І. М. Проектування та монтаж локальних комп'ютерних мереж: навчальний посібник. Миколаїв: Видавництво ЧДУ ім. Петра Могили, 2016. 396 с.
2. Б. Ю. Жураковський, І.О. Зенів. Комп'ютерні мережі. Частина 1. Навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2020. 336 с.
3. В.І. Кошель, Г.П. Сав'юк, Б.С. Дзундза. Основи охорони праці. навчально-методичний посібник для студентів вищих навчальних закладів педагогічного напрямку. Івано-Франківськ: НАІР, 2020. 182 с.
4. Пожарова О.В. Охорона праці: навчальний посібник. Одеса. 2022. 86 с.
5. Ременяк Л.В Конспект лекцій з навчальної дисципліни «Проектування інформаційних систем» для студентів ІІІ курсу денної форми навчання напрямку – комп'ютерні науки спеціальності – інформаційні управляючі системи та технології. Одеса: ОДЕкУ, 2016. 152 с.
6. Шестопалов С.В. Дослідження та проектування комп'ютерних систем та мереж: конспект лекцій. Одеса: Одеська національна академія харчових технологій, 2017. 82с.
7. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 7th ed. Boston: Pearson, 2016. 864 p.
8. Lammle T. CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125. 2nd ed. Indianapolis: John Wiley & Sons, Inc., 2016. 1152 p.
9. Поради (рекомендації) щодо створення КСЗІ в ІКС, які використовуються для надання послуг доступу до мережі Інтернет. URL: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet (дата звернення: 23.05.2026).

10. Порівняння товарів. Відеореєстратори. URL: https://nadzor.ua/uk/compare/table?categoryId=65 (дата звернення: 29.05.2026).

11. Порівняння товарів. Камери відеоспостереження. URL: https://nadzor.ua/uk/compare/table?categoryId=358 (дата звернення: 29.05.2026).

12. Порівняння 3 товарів Мережеві накопичувачі (NAS). URL: https://hotline.ua/ua/computer/setevye-nakopiteli-nas/cmp/?s=26046072-26388238-17270257 (дата звернення: 29.05.2026).

13. Порівняння товарів. Комутатори. URL: https://comtrade.ua/ua/kommutatory/filter/kolichestvoPortovDostupaLan=34,36;page=3;urovenUpravlenija=3/ (дата звернення: 25.05.2026).

14. Порівняння товарів. Роутери. URL: https://comtrade.ua/ua/routery/filter/page=8;sort_price=ASC;standartii=11,19,21/ (дата звернення: 25.05.2026).

15. Порівняння товарів. Точки доступу. URL: https://comtrade.ua/ua/wi-fi-tochki-dostupa/filter/price=20000-30000;standartWiFi=11/ (дата звернення: 25.05.2026).

16. ПП «УК «ЖИТЛОФОНД». URL: https://vkursi.pro/card/pp-uk-zhytlofond-37587589 (дата звернення: 21.05.2026).

17. Система створення комп'ютерних мереж: основні етапи і рекомендації. URL: https://infopard.com/systema-stvorennya-kompyuternyh-merezh-osnovni-etapy-i-rekomendacziyi/ (дата звернення: 21.05.2026).

18. DrayTek VigorSwitch P2540X PoE L2+ Managed Switch User's Guide. URL: https://draytek.com/download_de/Firmwares-Switch/VigorSwitch%20P2540xs/DrayTek_UG_VigorSwitch%20P2540x_V1.0.pdf (дата звернення: 02.06.2026).

19. DrayTek VigorSwitch P2540xs. URL: VigorSwitch P2540xs | DrayTek (дата звернення: 25.05.2026).

20. DrayTek Vigor2865 Series. URL: https://www.draytek.com/products/vigor2865 (дата звернення: 24.05.2026).

21. DrayTek Vigor2865 Series 35b Security Firewall User's Guide. URL: https://draytek.com/download_de/Firmwares-Router/Vigor2865-Serie/DrayTek_UG_Vigor2865_V1.6.pdf (дата звернення: 05.06.2026).

22. DrayTek VigorAP 1060C. URL: https://www.draytek.com/products/vigorap-1060c/ (дата звернення: 25.05.2026).

23. Synology DiskStation DS1825+. URL: https://www.synology.com/en-us/products/DS1825%2B (дата звернення: 29.05.2026).

24. DrayTek VigorAP 1060C 11ax Ceiling AP User's Guide. URL: https://draytek.pl/wp-content/uploads/2022/05/userguide_vigorap1060c_v1.2_en.pdf (дата звернення: 04.06.2026).

25. DS1825+ Product Manual. URL: https://kb.synology.com/en-uk/HIGs/DS1825p_HIG/4 (дата звернення: 06.06.2026).

26. Synology NAS User's Guide for DSM 7.4. URL: https://kb.synology.com/en-global/UG/Syno_UsersGuide_NAServer_7_4/6 (дата звернення: 07.06.2026).

27. TVT NVMS Lite. Інструкція користувача. URL: tvtdigital.com.ua/wp-content/uploads/NVMS_2_1_4_lite_User_Manual_ua.pdf (дата звернення: 04.06.2026).