Форма № Н-9.02

Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-кваліфікаційний рівень)

на тему: Розробка проєкту комп'ютерної мережі ТОВ «Аверс НК» (м. Рівне)

Виконав: студент IV курсу, групи КІ-406

Спеціальності **123 «Комп'ютерна інженерія»**

(шифр і назва напряму підготовки, спеціальності)

Давид МАСЛОВСЬКИЙ

(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 **інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян**
Циклова комісія **комп'ютерної інженерії**
Освітньо-професійний ступінь **фаховий молодший бакалавр**
Освітньо-професійна програма: **Обслуговування комп'ютерних систем і мереж**
Спеціальність: **123 Комп'ютерна інженерія**
Галузь знань: **12 Інформаційні технології**

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"30" березня 2026 року

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

Масловському Давиду Анатолійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі ТОВ "АВЕРС НК" (м. Рівне)**

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

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 27.03.2026р № 4/9-167.

2. Строк подання студентом роботи: 15 червня 2026 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проєктування, стандарти ANSI/EIA/TIA 568 - "Commercial Building Telecommunications Wiring Standart" і ANSI/EIA/TIA 569 - "Commercial Building Standart for Telecommunications Pathwais and Spaces

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

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Богдана МАРТИНЮК викладач		
Охорона праці та безпека життєдіяльності	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	01.04	
2	Збір і узагальнення інформації	08.05	
3	Написання першого розділу	15.05	
4	Розробка технічного та робочого проекту	22.05	
5	Написання спеціального розділу	28.05	
6	Розрахунок економічної частини	1.06	
7	Написання розділу охорони праці	3.06	
8	Виконання графічної частини	8.06	
9	Оформлення проєкту	10.06	
10	Погодження нормоконтролю	11.06	
11	Попередній захист роботи	12.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 1 квітня 2026 року

Студент _____ Давид МАСЛОВСЬКИЙ
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Масловський Д.А. Розробка проєкту комп'ютерної мережі ТОВ «АВЕРС НК» (м. Рівне): кваліфікаційна робота на здобуття освітньо-професійного ступеню «фаховий молодший бакалавр», за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. 113 с.

Кваліфікаційна робота присвячена розробці проєкту високонадійної комп'ютерної мережі для логістичної компанії ТОВ «АВЕРС НК» з метою створення єдиного безпечного інформаційного середовища. Реалізація проєкту забезпечує безперебійну координацію транспортних потоків, цілодобовий контроль рейсів та оперативне опрацювання документації завдяки оптимізованій фізичній і логічній структурі мережі. Апаратну основу архітектури сформовано на базі трьох продуктивних серверів Dell PowerEdge R750xs, керованого L3-комутатора D-Link та сучасного пасивного обладнання категорії Cat.6, що гарантує високу швидкість обробки даних та ізоляцію критичних сервісів компанії.

Для підвищення відмовостійкості та безпеки інфраструктури в роботі реалізовано сегментацію мережі на шість віртуальних підмереж (VLAN), налаштовано правила Firewall Access Control для суворого розмежування доступу між підрозділами та впроваджено схему Dual-WAN з двома незалежними провайдерами через міжмережевий екран TP-Link Omada. Проєкт містить комплексні практичні рекомендації щодо централізованого захисту серверів і робочих станцій за допомогою вбудованих інструментів безпеки Windows, а також визначає чіткі алгоритми налагодження, тестування та моніторингу мережі з використанням стандартних утиліт і журналів подій.

Ключові слова: вита пара, віртуальна мережа, комутатор, комп'ютерна мережа, міжмережевий екран, операційна система, патч-корд, сервер, СКС, топологія, точка доступу, шлюз, IP-адреса, DHCP, DNS, Wi-Fi.

ANNOTATION

Davyd MASLOVSKYI. Computer Network Project Development for LLC “AVERS NK” (Rivne): Qualification thesis for the award of the educational and professional degree of «Professional Junior Bachelor» in the field of study 123 Computer Engineering. Ternopil: SSS «TPC TNTU», 2026. 113 p

This qualification thesis is devoted to the development of a highly reliable computer network project for the logistics company AVERS NK LLC with the aim of creating a unified and secure information environment. The implementation of the project ensures uninterrupted coordination of transport flows, round-the-clock monitoring of routes, and prompt processing of transport documentation through an optimized physical and logical network structure. The hardware foundation of the architecture is based on three high-performance Dell PowerEdge R750xs servers, a managed D-Link L3 switch, and modern Cat.6 passive network components, which provide high-speed data processing and isolation of the company’s critical services.

To improve the fault tolerance and security of the infrastructure, the network is segmented into six virtual local area networks (VLANs), Firewall Access Control rules are configured to strictly separate access between departments, and a Dual-WAN scheme with two independent Internet service providers is implemented through a TP-Link Omada firewall/router. The project also includes comprehensive practical recommendations for the centralized protection of servers and workstations using built-in Windows security tools, and defines clear procedures for network configuration, testing, and monitoring using standard utilities and event logs.

Keywords: Twisted pair, Virtual network (VLAN), Network switch, Computer network, Firewall, Operating system, Patch cord, Server, Structured Cabling System, Network topology, Wireless access point, Gateway, IP address, DHCP, DNS, Wi-Fi.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

ДБЖ – джерело безперебійного живлення;

КМ – комп’ютерна мережа;

ОС – операційна система;

ПЗ – програмне забезпечення;

ППЗ – прикладне програмне забезпечення;

ПК – персональний комп’ютер;

СКС – структурована кабельна система;

ТЗ – технічне завдання.

ВСТУП

Сучасний етап розвитку глобального ринку вантажоперевезень характеризується високою динамічністю, жорсткою конкуренцією та постійною мінливістю зовнішнього середовища. У таких умовах успіх логістичної компанії залежить не лише від фізичної наявності автопарку, а й від ефективності управління інформаційними потоками, які синхронно супроводжують рух товарів від відправника до одержувача. Проєктування та розгортання надійної комп'ютерної мережі є тим критично важливим технологічним фундаментом, який пов'язує постачання, внутрішній менеджмент і збут в єдину відмовостійку систему, здатну миттєво адаптуватися до ринкових викликів [12].

Використання локальних і глобальних обчислювальних мереж дозволяє автоматизувати базові бізнес-процеси завдяки впровадженню спеціалізованих систем управління ланцюгами постачання та транспортних систем управління. Інтеграція мережевої інфраструктури забезпечує швидкий обмін даними між підрозділами підприємства, клієнтами та іноземними партнерами. Це мінімізує обсяги рутинної «паперової» роботи, оптимізує калькуляцію логістичних витрат, знижує ймовірність людських помилок в обліку та дозволяє в режимі реального часу відстежувати статус, безпеку і мікрокліматичні умови транспортування вантажів.

Використання інформаційних технологій у логістиці має глибокий позитивний вплив на всі аспекти діяльності підприємства, що виражається у трьох головних чинниках:

1. Підвищення прозорості процесів. Завдяки впровадженню інноваційних рішень, кожен учасник ланцюга постачання отримує безперешкодний доступ до актуальних даних про стан вантажів, точний маршрут їхнього переміщення та відповідність умовам транспортування. Це є критично важливим, наприклад, у харчовій та медичній логістиці для дотримання стандартів безпеки та якості.

2. Зростання ефективності та швидкості операцій. Застосування алгоритмів штучного інтелекту дозволяє повністю автоматизувати процеси планування та виконання замовлень, суттєво скорочуючи витрати часу та мінімізуючи людський фактор. Яскравим прикладом є сучасні автоматизовані склади, обладнані робототехнічними системами, які здатні виконувати завантаження та відвантаження товарів у кілька разів швидше, ніж це можливо вручну.

3. Суттєве зниження витрат. Використання аналітичних платформ дозволяє підприємствам оптимізувати розміщення складських хабів, зменшувати логістичні витрати на транспортування та підвищувати ефективність використання наявних ресурсів — палива, складських площ і транспортних засобів [19].

Актуальність розробки проєкту комп'ютерної мережі для ТОВ «АВЕРС НК» базується на специфіці її діяльності як логістичного оператора, що працює у режимі 24/7. У сфері, де швидкість обробки інформації прямо пропорційна прибутку, застаріла або несистематизована IT-інфраструктура стає «вузьким місцем», яке гальмує розвиток бізнесу. Стабільне мережеве підключення є головною запорукою кібербезпеки та безперервності операцій. Захищені канали зв’язку дають змогу логістам здійснювати цілодобовий моніторинг рейсів, координувати роботу водіїв на маршрутах та оперативно взаємодіяти з митними органами, гарантуючи прозорість, швидкість і безпеку кожної доставки.

Головною метою проєкту є створення високонадійної, безпечної, масштабованої та відмовостійкої мережевої інфраструктури, яка об'єднає усі відділи компанії та забезпечить стабільний доступ до хмарних або локальних сервісів моніторингу та ERP/CRM-систем

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Враховуючи специфіку діяльності ТОВ «АВЕРС НК» як міжнародної транспортно-експедиційної компанії, її корпоративна комп'ютерна мережа є критично важливим бізнес-інструментом. Мережа повинна забезпечувати безперебійну роботу логістів у режимі 24/7, підтримувати постійний зв'язок із клієнтами та водіями на міжнародних маршрутах, гарантувати безпеку конфіденційних комерційних даних та інформації про вантажі (зокрема категорій ADR).

1.1.2 Призначення розробки

Розробка комп'ютерної мережі для ТОВ «АВЕРС НК» — це перехід на новий рівень операційної ефективності. Це капітальна інвестиція в цифрову безпеку, швидкість обробки замовлень та надійність ланцюжків постачання, що є головною конкурентною перевагою на міжнародному ринку логістики.

Проєктування професійної мережі дозволить:

- Об'єднати всі сервіси в єдину відмовостійку систему.

- Пріоритезувати критично важливий трафік (наприклад, IP-телефонію для зв'язку з клієнтами) за допомогою технології QoS.

- Усунути затримки (лаги) під час обміну важкими файлами та координації збірних вантажів.

- Розробка КМ із дублюванням інтернет-каналів та резервуванням живлення усуне ризик раптової втрати зв'язку, яка може призвести до простою транспорту, порушення термінів доставки та фінансових штрафів.

- Впровадженні багаторівневого захисту, такого як сегментація мережі (VLAN) для ізоляції фінансових та операційних даних від гостьового

корпоративного простору та встановлення міжмережевих екранів, захистить компанію від зовнішніх кібератак.

1.1.3 Технічні вимоги до мережевої інфраструктури

Зазначені в таблиці 1.1 вимоги слугують безпосереднім орієнтиром для підбору активного та пасивного мережевого обладнання, забезпечуючи створення стабільного цифрового середовища з високим потенціалом для подальшого масштабування бізнесу.

Таблиця 1.1 - Технічні вимоги до мережевої інфраструктури

№ п/п	Параметр мережі	Технічна вимога та обґрунтування
1	2	3
1.	Організація каналів зв'язку	Обов'язкове підключення двох незалежних інтернет-провайдерів (Dual-WAN) із технологією автоматичного перемикання каналів у разі аварії на лінії.
2.	Сегментація мережі (VLAN)	Розділення мережі на ізольовані підмережі: адміністрація/бухгалтерія, відділ логістики, сервери/БД та гостьова зона Wi-Fi.
3.	Кібербезпека та захист	Впровадження міжмережевого екрана із функціями виявлення вторгнень та фільтрації шкідливого трафіку.
4.	Віддалений доступ	Організація шифрованих VPN-каналів із обов'язковою двофакторною автентифікацією для мобільних пристроїв та домашніх ПК логістів.
5.	Бездротова мережа (WLAN)	Покриття офісного простору Wi-Fi (стандарту не нижче Wi-Fi 6) із підтримкою корпоративного шифрування WPA3.

Продовження таблиці 1.1

1	2	3
6.	Енергонезалежність	Забезпечення центрального комутаційного вузла джерелами безперебійного живлення (ДБЖ) з можливістю автономної роботи активного обладнання не менше 2 годин.
7.	Планова вартість мережі	До 1,25 млн. грн.

1.1.4 Вимоги до документації

По завершенню проєктування виконавець повинен надати замовнику повний пакет документації, який включає три основні блоки.

По-перше, технічну частину: структурну та логічну схеми мережі, схему розподілу IP-адрес та налаштування VLAN, а також опис політик безпеки та рівнів доступу користувачів.

По-друге, специфікацію обладнання: точний перелік необхідного активного (маршрутизатори, керовані комутатори, точки доступу) та пасивного (патч-панелі, кабелі, шафи) мережевого устаткування із зазначенням рекомендованих брендів.

По-третє, інструкції з експлуатації: регламент дій системного адміністратора у разі аварійних ситуацій (відмова провайдера, збій обладнання) та правила підключення нових робочих місць для розширення штату компанії.

1.1.5 Стадії та етапи розробки

Розробка проєкту комп’ютерної мережі доцільно виконується не лише як вибір активного обладнання та IP-адресації, а як комплексне проєктування структурованої кабельної системи (СКС), яка є фізичною основою майбутньої мережі. Саме СКС визначає місця розташування робочих точок,

телекомунікаційних розеток, кабельних трас, комутаційного обладнання, серверної кімнати, точок доступу Wi-Fi та резервів для подальшого розширення.

Початковою стадією є передпроєктне обстеження об’єкта. На цьому етапі аналізують план приміщень, кількість кабінетів, розміщення робочих місць, серверної кімнати, принтерів, точок доступу Wi-Fi, електроживлення та можливих кабельних трас. Також визначаються вимоги замовника: кількість користувачів, потреба в дротовому й бездротовому доступі, необхідність створення зони Wi-Fi, підключення серверів, мережевих принтерів, систем безпеки та можливість майбутнього розширення. Для комп’ютерних мереж важливо врахувати як фізичну модель, так і топологічну модель мережі, оскільки вони є базовими складовими системного опису мережевої архітектури.

Другою стадією є формування технічного завдання (ТЗ). У ТЗ визначають призначення мережі, перелік приміщень, кількість інформаційних розеток, вимоги до швидкості передавання даних, тип кабелю, категорію СКС, місце встановлення комутатора, серверного обладнання, маршрутизатора, міжмережевого екрана та точок доступу. Також задаються вимоги до надійності, адміністрування, безпеки, резерву портів і кабельних ліній. Такий підхід узгоджується з вимогами до проєктної документації: ДБН А.2.2-3:2014 встановлює склад і зміст проєктної документації для нового будівництва, реконструкції та капітального ремонту будівель і споруд.

Наступною є стадія ескізного або концептуального проєктування. На ній визначають загальну архітектуру КМ: вибирають топологію, місце центрального комутаційного вузла, принцип підключення робочих місць, серверів, принтерів і Wi-Fi-обладнання. Для офісних мереж найчастіше застосовують дротову топологію типу «зірка» або ієрархічна «зірка», яка добре поєднується з принципами побудови СКС. Якщо в мережі передбачено бездротовий сегмент, топологія стає гібридною: дротова частина будується на основі СКС, а мобільні пристрої підключаються через точки доступу Wi-Fi.

Після цього виконується архітектурна фаза проєктування СКС. Вона пов’язана з прив’язкою мережевої інфраструктури до конкретного плану приміщення. На цьому етапі визначають місця встановлення телекомунікаційних розеток, комутаційної шафи, кабельних каналів, лотків, проходів через стіни, вертикальних і горизонтальних ділянок кабельної системи. Також враховують розташування меблів, робочих зон, дверей, технічних приміщень, електрощитів та інших інженерних систем. У чинному ДСТУ EN 50173-1:2022 загальні кабельні системи розглядаються як стандартизована інформаційна інфраструктура, а ДСТУ EN 50173-2:2022 окремо стосується офісних приміщень.

Далі проводиться телекомунікаційна фаза проєктування. На цьому етапі уточнюють схему підключення робочих місць до комутатора, нумерацію портів, структуру патч-панелей, типи кабелів і розеток, категорію кабельної системи, довжину кабельних трас, розміщення активного обладнання, принципи маркування та комутації. Саме тут формується фізична топологія мережі: від кожного робочого місця, принтера або точки доступу прокладається окрема лінія до комутаційного вузла. У ДСТУ EN 50174-1:2022 наведено вимоги до монтажу кабелів, зокрема до специфікації монтажу та забезпечення якості; у структурі документа передбачені питання документації, планування, продуктів і процесів, обслуговування, вимог до інсталяторів, перевірок та планів якості.

Окремою стадією є розробка логічної структури мережі. Вона включає поділ мережі на підмережі, VLAN, визначення IP-адресації, правил маршрутизації, доступу до серверів, принтерів, Інтернету та гостьового Wi-Fi. Якщо фізична СКС показує, як прокладені кабелі, то логічна схема визначає, як саме взаємодіють користувачі, сервери, принтери, комутатори, маршрутизатор і міжмережевий екран. Для підприємства з кількома відділами доцільно передбачити окремі VLAN для серверної інфраструктури, адміністрації, фінансового відділу, інженерно-IT-підрозділів, операційних відділів і бездротового сегмента.

Після вибору логічної структури виконується підбір обладнання та матеріалів. До складу проєкту включають комутатори, маршрутизатор або міжмережевий екран, точки доступу, серверне обладнання, патч-панелі, телекомунікаційні шафи, кабель, розетки, конектори, кабельні канали, маркувальні елементи та джерела безперебійного живлення. Вибір обладнання має відповідати кількості користувачів, пропускній здатності, резерву портів, вимогам до VLAN, PoE, Wi-Fi, адміністрування та захисту мережі.

Наступним етапом є розробка робочої документації. Вона повинна містити план розміщення обладнання, схему кабельних трас, логічну схему мережі, таблиці підключення портів, специфікацію обладнання й матеріалів, маркування кабелів, перелік телекомунікаційних розеток, схему розміщення шафи та правила комутації. ДСТУ 9243.4:2023 визначає вимоги до проєктної документації різних стадій, зокрема ескізного проєкту, техніко-економічного обґрунтування, техніко-економічного розрахунку, проєкту та робочої документації.

Після затвердження проєкту переходять до монтажної стадії. Вона включає прокладання кабельних трас, монтаж телекомунікаційних розеток, встановлення шаф, патч-панелей, укладання кабелю, обтискання або термінування ліній, підключення активного обладнання, організацію електроживлення та заземлення. Важливо дотримуватися вимог до радіусів вигину кабелю, допустимих довжин ліній, відстаней від силових кабелів, маркування й акуратності монтажу. Для таких робіт профільним нормативним джерелом є ДСТУ EN 50174-1:2022, який стосується монтажу кабелів, специфікації монтажу та забезпечення якості.

Завершальною технічною стадією є тестування, сертифікація та введення мережі в експлуатацію. Після монтажу перевіряють цілісність кабельних ліній, правильність розшивки, відповідність категорії кабелю, якість з’єднань, роботу комутаторів, маршрутизацію, VLAN, доступ до серверів, принтерів, Інтернету та Wi-Fi. У навчальній програмі з СКС тестування та сертифікація СКС

виділені як окрема тема, що підтверджує важливість цього етапу для завершення побудови кабельної інфраструктури.

Останнім етапом є оформлення виконавчої документації та передавання мережі в обслуговування. До виконавчої документації вносять фактичні схеми прокладання кабелів, маркування ліній, таблиці підключення портів, налаштування активного обладнання, IP-план, VLAN-план, облікові дані адміністратора, результати тестування та рекомендації з експлуатації. Надалі ця документація використовується для адміністрування, ремонту, модернізації та розширення мережі [8; 9].

1.1.6 Порядок контролю та прийому

Після завершення монтажу комп'ютерної мережі обов'язково виконується контроль якості робіт і приймання мережі замовником. Приймання комп'ютерної мережі замовником має завершувати не тільки монтажні роботи, а й повний цикл перевірки її працездатності. Цей етап потрібний для підтвердження того, що змонтована кабельна система, активне мережеве обладнання, Wi-Fi-сегмент, VLAN, серверні підключення та робочі місця відповідають проєктній документації й технічному завданню.

Перед підписанням акта замовник має переконатися, що всі робочі місця підключені, мережеві розетки промарковані, принтери доступні користувачам, сервери працюють, Wi-Fi покриває заплановані зони, безпровідний доступ ізольований, а результати тестування не містять критичних помилок. Якщо виявлено недоліки, складається перелік зауважень із термінами їх усунення. Після усунення зауважень виконується повторна перевірка і лише після цього мережа приймається в експлуатацію.

Лише після підтвердження відповідності кабельної системи, активного обладнання, логічної структури, Wi-Fi-сегмента та документації вимогам проєкту мережу можна вважати готовою до експлуатації [9].

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

ТОВ «АВЕРС НК» є надійним гравцем на ринку транспортно-експедиційних послуг, який спеціалізується на автомобільних перевезеннях як у межах України, так і в міжнародному сполученні. Компанія побудувала ефективну мережу співпраці з українськими та іноземними підприємствами, успішно обслуговуючи потреби експортерів, імпортерів та суміжних перевізників. Важливим гарантом прозорості та юридичної надійності підприємства є його офіційне членство в Торгово-промисловій палаті, що робить компанію безпечним та відкритим партнером для довгострокового бізнесу.

Маючи значний практичний досвід та сучасний автопарк, компанія ефективно вирішує транспортні завдання будь-якого рівня складності. Географія перевезень охоплює всю територію України, а також країни Європейського Союзу. Спектр можливостей підприємства включає стандартні автомобільні перевезення та регулярну доставку збірних вантажів у внутрішніх і міжнародних напрямках. Окрім цього, компанія професійно працює зі специфічними категоріями, забезпечуючи безпечне транспортування небезпечних вантажів усіх класів ADR (з 1 по 9), а також логістику товарів, що потребують регульованого мікроклімату, за допомогою сучасних рефрижераторів та ізотермів.

Головна мета діяльності ТОВ «АВЕРС НК» полягає в забезпеченні стабільного розвитку бізнесу своїх клієнтів шляхом організації швидких, надійних і безпечних поставок. Бездоганна якість послуг тримається на сервісі високого рівня, професіоналізмі згуртованого колективу та підборі оптимальних рішень під конкретний маршрут і специфіку товару. Клієнти компанії отримують результативний досвід співпраці та вагому перевагу у вигляді безперервної комунікації з персональним логістом у режимі 24/7, що гарантує цілковитий контроль над вантажем на кожному етапі руху [10].

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Для приміщення ТОВ «АВЕРС НК», враховуючи необхідність організації ізольованого гостьового Wi-Fi сегмента у зоні переговорної кімнати, є впровадження гібридної топології. Вона поєднує надійність та гігабітну швидкість дротової «зірки» на базі технології Gigabit Ethernet для стаціонарних ПК та серверів із гнучкістю бездротової інфраструктури Wi-Fi для мобільних клієнтів [1].

Для провідної частини мережі найбільш обґрунтованим є вибір локальної мережі з топологією «зірка» з розміщенням центрального комутаційного обладнання в серверній кімнаті. Такий тип мережі є найбільш доцільним, оскільки кабінети працівників розміщені по периметру та в окремих функціональних зонах [4]. Така структура приміщень передбачає розміщення робочих місць у різних частинах будівлі, тому найзручніше підводити до кожного кабінету окрему кабельну лінію від центральної точки. Саме це відповідає топології «зірка», де всі робочі місця підключаються до одного центрального вузла. Це спрощує монтаж, маркування кабелів, пошук несправностей і подальше розширення мережі [2].

Використання керованого комутатора SW_1 у повнодуплексному режимі (Full-Duplex) повністю ізолює трафік кожного порту. Це ліквідує колізії (зіткнення пакетів даних), забезпечуючи кожному працівнику гарантовану пропускну здатність (1 Гбіт/с) під час взаємодії із серверами S_1–S_3.

У разі випадкового пошкодження кабелю або роз'єму на будь-якому робочому місці (наприклад, у відділі маркетингу та аналітики або кабінеті диспетчерів), з ладу виходить лише одна конкретна лінія зв'язку. Вся інша мережа підприємства, включно з критично важливими серверами баз даних та бухгалтерією, продовжує функціонувати в штатному режимі.

Інші топології для проєктування кабельного сегменту менш доцільні.

Наприклад, шинна топологія погано підходить для великої кількості кабінетів, оскільки спільна магістраль ускладнює пошук несправностей і розширення мережі. Кільцева топологія також незручна, бо вимагає послідовного з'єднання приміщень, що не відповідає реальному плануванню офісу з багатьма відокремленими кабінетами. Натомість «зірка» дозволяє підключати кожне приміщення незалежно від інших.

Ще однією перевагою обраної топології є масштабованість. Якщо в майбутньому з'являться нові робочі місця, додаткові принтери, IP-телефонія, точки доступу Wi-Fi або мережеві камери, їх можна буде підключити до вільних портів комутатора або додати ще один комутатор доступу. У зірковій топології додавання нового пристрою зазвичай не потребує перебудови всієї мережі й не порушує роботу вже підключених користувачів. Це особливо важливо для офісної будівлі, де кількість працівників і обладнання може змінюватися. Наприклад, якщо у відділі управління персоналом або кабінеті менеджера з постачання виникне потреба розширити штат, підключення нових робочих станцій (наприклад, WS_29, WS_30) зведеться до прокладання додаткового кабелю до комутатора в серверну, без необхідності зупиняти чи переналаштовувати існуючий сегмент мережі.

Водночас потрібно враховувати основний недолік топології «зірка»: центральний комутатор є критично важливим вузлом. Якщо SW_1 вийде з ладу, зв'язок між більшістю пристроїв буде порушено. Тому для підвищення надійності доцільно використовувати якісний керований комутатор, джерело безперебійного живлення, резервування конфігурації, належне охолодження в серверній кімнаті та, за потреби, резервний комутатор або ієрархічну схему з окремими комутаторами доступу для різних зон будівлі [32; 27].

На поданій на рисунку 2.1 логічній схемі мережі всі робочі станції WS_1–WS_28, принтери PR_1–PR_7, сервери S_1–S_3 та міжмережевий екран FW_1 з виходом до мережі Інтернет зведені до центрального комутатора SW_1.

З урахуванням плану приміщень, фізичної топології та наявності дротової й бездротової мережі доцільно виконати логічний поділ мережі на

VLAN. Фізично всі кабельні лінії з робочих місць, принтерів і серверів сходяться до центрального комутаційного вузла SW_1 в серверній кімнаті, однак логічно не варто залишати всі пристрої в одній широкомовній мережі. Для підприємства з кількома відділами це створює зайвий широкомовний трафік, ускладнює адміністрування, знижує рівень безпеки та не дає можливості гнучко обмежувати доступ між групами користувачів.

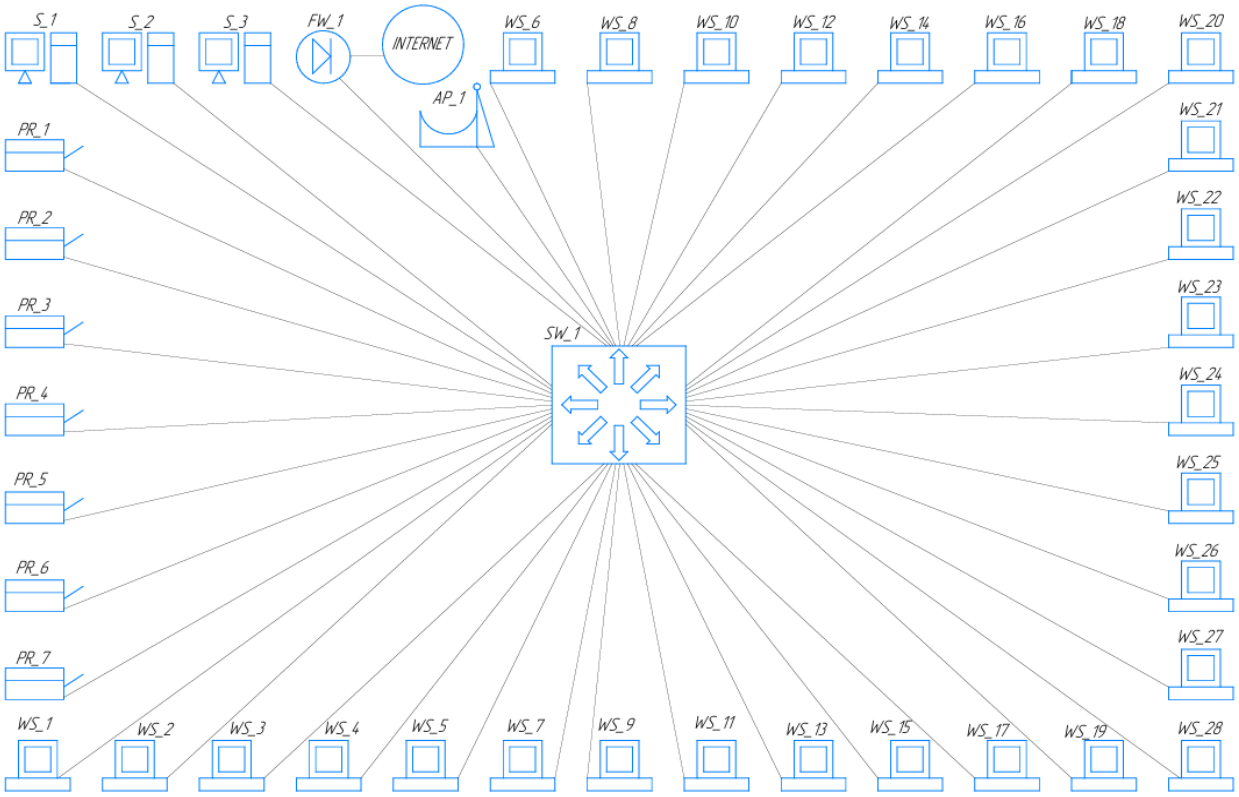

Рисунок 2.1 – Логічна топологія КМ

Впровадження технології VLAN (Virtual Local Area Network) є обов'язковим кроком. Централізована структура «Зірки» ідеально підходить для логічного сегментування мережі на рівні ядра.

Розподіл КМ на VLAN надасть такі переваги:

1. Безпека та розмежування прав доступу: Без сегментації будь-який співробітник або гість компанії (наприклад, через Wi-Fi в Переговорній кімнаті) матиме прямий мережевий доступ до серверів (S_1–S_3), фінансових баз даних у бухгалтерії або комп'ютера директора. VLAN ізолює трафік різних

відділів на 2-му рівні (L2) моделі OSI.

2. Оптимізація мережевої продуктивності: мережа налічує 28 ПК, 7 принтерів, сервери та мобільні пристрої. У єдиному просторі широкомовні пакети (Broadcast: ARP-запити, DHCP, службовий трафік ОС) надсилаються на всі пристрої одночасно. Це перевантажує мережу, особливо бездротовий сегмент (через точку AP_1). Розподіл на VLAN зменшує розмір широкомовних доменів.

3. Контроль та фільтрація трафіку: маршрутизація між VLAN здійснюватиметься через міжмережевий екран FW_1. Це дозволить налаштувати гнучкі правила безпеки (наприклад: дозволити логістам доступ лише до сервера баз даних, але повністю заборонити їм доступ до підмережі бухгалтерії та директора) [30].

4. Захист бездротового інфраструктурного периметра: гість, який підключився до Wi-Fi, має потрапляти в ізольований гостьовий VLAN, який має вихід виключно в INTERNET і заблокований до локальних ресурсів офісу [21].

Для даного ТОВ доцільно передбачити логічне розділення мережі за функціональними групами. Таке рішення підвищує керованість і безпеку мережі, зменшує зайвий широкомовний трафік і дозволяє обмежувати доступ між підрозділами відповідно до службових потреб.

Оптимальним рішенням буде використання 6 VLAN. Така кількість не є надмірною для офісної мережі, але дозволяє відокремити критичні ресурси, адміністративні робочі місця, бухгалтерію, загальні робочі станції та гостьовий доступ через Wi-Fi.

Серверну кімнату доцільно винести в окрему VLAN 10 (INFRASTRUCTURE), оскільки саме там розміщується ключове обладнання: сервери, комутатор, міжмережевий екран, система резервного копіювання. Доступ до цієї підмережі має бути обмежений лише для адміністраторів та потрібних службових сервісів за чітко визначеними IP-адресами.. Це зменшує ризик несанкціонованого доступу до критичних ресурсів підприємства.

Адміністративні кабінети варто об’єднати в окрему VLAN 20 (MANAGEMENT), оскільки ці робочі місця зазвичай працюють з управлінською, договірною та організаційною інформацією. До цього сегмента можна віднести кабінет директора, заступника директора, відділ управління персоналом та юридичний відділ. Їхній трафік бажано відокремити від загальної мережі користувачів.

Фінансово-економічний відділ і бухгалтерію доцільно винести в окрему VLAN 30 (FINANCE) через підвищені вимоги до конфіденційності. У цій підмережі можуть працювати програми бухгалтерського обліку, фінансові документи, банківські сервіси, зарплатні дані та звітність. Обмеження доступу до цієї VLAN дозволить зменшити ризик випадкового або несанкціонованого доступу з інших відділів.

Інженерно-технічні та IT-підрозділи також доцільно виділити в окрему VLAN 40 (ENGINEERING&IT), куди увійдуть IT-служба, кабінет інженера з охорони праці, інженерно-технічний відділ, кабінет охорони. Для таких робочих місць можуть бути потрібні окремі права доступу до обладнання, серверів, мережевих налаштувань або технічної документації.

Основним генератором внутрішнього трафіку будуть кабінет диспетчерів, відділ логістики, кабінет менеджера з постачання, адміністративно-господарський відділ та відділ маркетингу та аналітики, співробітники яких інтенсивно працюють з базами даних постачання, CRM та логістичними програмами. Потрібна висока пропускна здатність. Тому доцільно їх виокремити в в окрему VLAN 50 (OPERATIONS).

Оскільки в мережі передбачена бездротова мережа, її також потрібно логічно розділити в окрему VLAN 60 (WIRELESS). Корпоративний Wi-Fi доцільно використовувати для службових ноутбуків і мобільних пристроїв працівників, залишивши лише доступ до Інтернету.

Для проєктованої мережі доцільно використати приватний адресний простір класу 10.10.0.0/16, а кожній VLAN виділити окрему підмережу формату 10.10.X.0/24, де X відповідає номеру VLAN. Такий підхід зручний для

адміністрування, бо за IP-адресою одразу видно, до якого логічного сегмента належить пристрій.

Схема адресації мережі:

10.10.10.0/24 — INFRASTRUCTURE;

10.10.20.0/24 — MANAGEMENT;

10.10.30.0/24 — FINANCE;

10.10.40.0/24 — ENGINEERING-IT;

10.10.50.0/24 — OPERATIONS;

10.10.60.0/24 — WIRELESS.

Рекомендована схема розподілу на групи VLAN наведена в таблиці 2.1, а виділені для підключення кожного мережевого пристрою порти на керованому комутаторі SW_1 - в таблиці 2.2.

Таблиця 2.1 – Рекомендована схема розподілу на групи VLAN

Вузли КМ	Кількість вузлів	Приміщення	Група VLAN	Адреса підмережі/ маска	Шлюз
1	2	3	4	5	6
WS_1	1	Адмінстративно-господарський відділ	50	10.10.50.0 /24	10.10.50.1
WS_2-WS_4, PR_1	4	Кабінет диспетчерів	50	10.10.50.0 /24	10.10.50.1
WS_5-WS_8, PR_2	5	Відділ логістики	50	10.10.50.0 /24	10.10.50.1

Продовження таблиці 2.1

1	2	3	4	5	6
WS_9-WS_10	2	Служба IT-підтримки та системного адмінстрування	40	10.10.40.0/24	10.10.40.1
WS_11	1	Кімната охорони	40	10.10.40.0/24	10.10.40.1
SW_1, FW_1, S_1-S_3	5	Серверна кімната	10	10.10.10.0/24	10.10.10.1
WS_12-WS_15, PR_3	5	Фінансово-економічний відділ	30	10.10.30.0/24	10.10.30.1
WS_16	1	Кабінет інженера з охорони праці	40	10.10.40.0/24	10.10.40.1
WS_17-WS_18, PR_4	3	Кабінет інженерно-технічного відділу	40	10.10.40.0/24	10.10.40.1
WS_19-WS_20, PR_5	3	Відділ маркетингу та аналітики	50	10.10.50.0/24	10.10.50.1
WS_21	1	Кабінет головного бухгалтера	30	10.10.30.0/24	10.10.30.1

Продовження таблиці 2.1

1	2	3	4	5	6
WS_22	1	Кабінет директора	20	10.10.20.0 /24	10.10.20.1
WS_23	1	Кабінет заступника директора	20	10.10.20.0 /24	10.10.20.1
WS_24-WS_25, PR_6	3	Відділ управління персоналом	20	10.10.20.0 /24	10.10.20.1
WS_26-WS_27, PR_7	3	Юридичний відділ	20	10.10.20.0 /24	10.10.20.1
WS_28	1	Кабінет менеджера з постачання	50	10.10.50.0 /24	10.10.50.1
AP_1	1	Переговорна кімната	60	10.10.60.0 /24	10.10.60.1

Таблиця 2.2 – Призначення портів комутатора SW_1

Вузли КМ	Задіяні порти	Тип порту	Група VLAN
1	2	3	4
WS_1-WS_8, PR_1-PR_2	1-10	Access	50
WS_9-WS_11	11-13	Access	40
WS_12-WS_15, PR_3	14-18	Access	30
WS_16-WS_18, PR_4	19-22	Access	40
WS_19-WS_20, PR_5	23-25	Access	50
WS_21	26	Access	30

Продовження таблиці 2.2

1	2	3	4
WS_22-WS_27, PR_6- PR_7	27-34	Access	20
WS_28	35	Access	50
AP_1	41	Access	60
FW_1	47	Trunk	10
S_1- S_3	48-50	Access	10

2.2 Вибір середовища передачі даних у проєктованій мережі

Середовище передачі даних є фізичною основою комп'ютерної мережі, через яку здійснюється обмін інформацією між робочими станціями, серверами, мережевими принтерами, комутаторами, міжмережевим екраном та точками доступу Wi-Fi [4].

Для проєктованої мережі ТОВ «АВЕРС НК» доцільно застосувати комбіноване середовище передачі даних: основою має бути дротова кабельна інфраструктура на базі мідної витої пари, а для мобільних пристроїв — бездротове середовище Wi-Fi. Такий вибір відповідає гібридній топології мережі: стаціонарні робочі місця, сервери, принтери, комутатор і міжмережевий екран підключаються кабелем, а ноутбуки, смартфони та гостьові пристрої можуть працювати через бездротовий сегмент.

Для підключення робочих станцій WS_1–WS_28, мережевих принтерів PR_1–PR_7, точок доступу Wi-Fi та іншого офісного обладнання доцільно використовувати кабель типу «вита пара» категорії Cat 6. Це найбільш практичний варіант для офісної локальної мережі, оскільки він забезпечує достатню пропускну здатність, порівняно невисоку вартість, простий монтаж, сумісність із типовими мережевими розетками RJ-45, патч-панелями та комутаторами Gigabit Ethernet.

Використання кабелю Cat 6 є доцільним з огляду на потребу забезпечити швидкість передавання даних 1 Гбіт/с для робочих місць і мережевих пристроїв. Стандарт 1000BASE-T працює по чотирьох парах мідного кабелю категорії 5 або вище; для сучасної офісної мережі доцільно закладати саме Cat 6 як більш перспективне середовище з кращим запасом за характеристиками.

Окрім дротової частини, у проєктованій мережі доцільно передбачити бездротове середовище передачі даних Wi-Fi. Воно потрібне для підключення ноутбуків, смартфонів, планшетів, службових мобільних пристроїв, а також для організації гостьового доступу в переговорній кімнаті. Wi-Fi є сімейством бездротових мережевих протоколів на основі стандартів IEEE 802.11 і використовується для локальних мереж та доступу до Інтернету через радіохвилі [1].

2.3 Обґрунтування вибору обладнання для мережі (активного та пасивного)

Обґрунтування вибору активного та пасивного обладнання є одним із найважливіших етапів проєктування та розгортання комп'ютерної мережі. Від правильного підбору компонентів залежить продуктивність, надійність, масштабованість, безпека та економічна ефективність усієї телекомунікаційної інфраструктури підприємства.

Процес вибору мережевого обладнання базується на аналізі ТЗ, архітектури будівлі, кількості користувачів та вимог до трафіку. Головне правило проєктування — забезпечення балансу між технічними характеристиками та вартістю рішень, а також закладання резерву модернізації (зазвичай до 20–30%) для майбутнього розширення компанії.

Активне обладнання відповідає за обробку, маршрутизацію, комутацію та керування потоками даних у мережі.

Пасивне обладнання створює фізичний тракт для передачі сигналів. Воно не потребує живлення від електромережі, але визначає довговічність і стабільність фізичного рівня (Layer 1 OSI).

Головною вимогою під час обґрунтування є повна сумісність активних та пасивних компонентів. Якщо активний комутатор підтримує швидкість 1Гбіт/с, а пасивна інфраструктура (кабель і патч-панелі) розрахована лише на категорію 5 (до 100 Мбіт/с), мережа працюватиме на найнижчій швидкості. Тому всі елементи тракту мають відповідати єдиному технічному стандарту.

2.3.1 Вибір керованого комутатора рівня L3

Обґрунтування вибору комутатора рівня L3 для проєктуваної комп'ютерної мережі базується на аналізі техніко-економічних характеристик трьох комутаторів рівня L3 [17], наведених у таблиці 2.3.

Таблиця 2.3 - Техніко-економічні характеристики комутаторів рівня L3

Характеристика	Модель 1	Модель 2	Модель 3
1	2	3	4
Модель комутатора	Ubiquiti UniFi Switch Pro 48 PoE USW-PRO-48-POE	Ruijie Networks RG-NBS5100-48GT4SFP	D-Link DGS-1520-52
Орієнтовна ціна, грн.	54107	34949	49999
Клас / рівень	Керований L3, PoE-комутатор	Керований L3, без PoE	Керований L3, без PoE
Загальна кількість портів	52	52	52
Порти доступу RJ-45	48 x 1 GbE RJ-45, з них 40 PoE+ і 8 PoE++	48 x 10/100/1000 BASE-T RJ-45	48 x 10/100/1000 BASE-T RJ-45
Uplink / високошвидкісні порти	4 x 10G SFP+	4 x 1G SFP	2 x 10GBASE-T + 2 x 10G SFP+

Продовження таблиці 2.3

1	2	3	4
Підтримка PoE	Так	Ні	Ні
Комутаційна здатність, Гбіт/с	176	104	176
Продуктивність пересилання пакетів, Mpps	131	77,38	130,95
Підтримка VLAN	Так	Так	Так
MAC-таблиця	16 000 адрес	16 000 адрес	16 000 адрес
Буфер пакетів / Jumbo Frame	Буфер 4 МБ; Jumbo Frames 9216 байт	Буфер 4 МБ; Jumbo frame 9216 байт	Буфер 4 МБ; Jumbo frame 12288 байт
L3-функції	DHCP Server, DHCP Relay, Inter-VLAN Routing, Static Routing	Static routing, DHCP Server, DHCP Relay; RIP, OSPF	OSPF, RIP/RIPng, IGMP, MLD, PIM
Функції безпеки	802.1X, ACL, DHCP Snooping/Guarding, storm control, port isolation, rate limiting	Port isolation, broadcast storm control, захист від перенапруги 6 кВ, security policies	ACL, Web GUI, Zero Touch Provisioning; розширені функції керування і стекування
Керування	UniFi Network Controller, Web/SSH/SNMP	Ruijie Cloud, Web/Cloud, віддалене керування	Web GUI, D-View 8, Zero Touch Provisioning, CLI/console
Живлення	100–240 В AC; внутрішній БЖ 660 Вт	100–240 В AC	100–240 В AC
Робоча температура	-5…+40 °C	0…+50 °C	-5…+50 °C
Монтаж	Стійковий 1U	Стійковий 1U	Стійковий 1U
Розміри	442 x 400 x 44 мм	440 x 267,5 x 43,6 мм	441 x 207,4 x 44 мм
Маса, кг	6,2	3,6	2,78

Ubiquiti UniFi Switch Pro 48 PoE (USW-PRO-48-POE) є найфункціональнішим варіантом для мережі з великою кількістю PoE-пристроїв: точок доступу, IP-камер, IP-телефонів або іншого обладнання, яке живиться через Ethernet. Він має 48 PoE-портів, зокрема 8 PoE++, сумарний PoE-бюджет 600 Вт, 4 порти 10G SFP+ та зручне централізоване керування через UniFi Network. Однак для проєктованої мережі, де основними пристроями є ПК, сервери, принтери та обмежена кількість точок доступу, такий PoE-бюджет може бути надлишковим. Вартість пристрою також найвища серед трьох варіантів.Оскільки функція PoE для архітектури мережі не є ключовою, адже під'єднання єдиної точки доступу здійснюватиметься через PoE-інжектор ключовими критеріями оцінки стають чиста продуктивність пристрою, швидкість магістральних інтерфейсів, можливості масштабування та загальна вартість рішення.

Ruijie Networks RG-NBS5100-48GT4SFP є найбільш економним рішенням. Він має 48 гігабітних портів, 4 SFP-uplink, підтримку L3, хмарне керування Ruijie Cloud. Це добрий вибір для офісної мережі з обмеженим бюджетом, коли не потрібні 10G uplink-порти та PoE. Його слабка сторона — нижча офіційна комутаційна здатність 104 Гбіт/с та відсутність 10G uplink, що може обмежувати перспективу розвитку серверного сегмента.

D-Link DGS-1520-52 є найбільш збалансованим варіантом за співвідношенням ціна–якість–потужність. За ціною він дешевший за Ubiquiti, але має таку ж комутаційну здатність 176 Гбіт/с і практично таку саму продуктивність пересилання пакетів — 130,95 Mpps. На відміну від Ruijie, D-Link має не лише гігабітні порти доступу, а й 2 порти 10GBase-T та 2 порти 10G SFP+, що важливо для підключення серверів, міжмережевого екрана, майбутнього комутатора агрегації або високошвидкісного uplink. Також він підтримує стекування до 8 комутаторів і має розширені L3-функції, зокрема OSPF та RIP/RIPng.

Порівняльний аналіз показує, що найменш ефективним є використання моделі Ruijie Networks RG-NBS5100-48GT4SFP, яка попри найнижчу ціну

суттєво обмежує пропускну здатність мережі через відсутність 10-гігабітних портів. Модель Ubiquiti UniFi Switch Pro 48 PoE, хоч і має високі технічні показники, є економічно недоцільною через значну переплату за невикористовувану технологію PoE та її потужну систему живлення. Відтак, для проєктованої мережі ТОВ «АВЕРС НК» найбільш оптимальним і технічно виправданим рішенням для розгортання мережі є вибір комутатора D-Link DGS-1520-52 (див. рис. 2.2), як основного комутатора ядра/агрегації.

Рисунок 2.2 – Комутатор D-Link DGS-1520-52

Комутатор D-Link DGS-1520-52 забезпечує максимальну продуктивність на рівні ядра та агрегації завдяки наявності чотирьох високошвидкісних магістральних портів із підтримкою швидкості 10 Гбіт/с як через оптичні інтерфейси SFP+, так і через мідні Base-T. Це дозволяє уникнути утворення «вузьких місць» при підключенні серверної інфраструктури чи центрального маршрутизатора та гарантує стабільну роботу 48 клієнтських портів під час пікових навантажень. Важливою перевагою цієї моделі є повноцінне розширене керування на третьому рівні (L3) із підтримкою протоколів динамічної маршрутизації OSPF, що забезпечує автоматичне перенаправлення трафіку та високу гнучкість при сегментації мережі. Крім того, наявність 52 портів у сумі дає додатковий технологічний резерв для підключення критично важливих вузлів без необхідності придбання допоміжних комутаційних пристроїв.

Перспективи розвитку інфраструктури підприємства надійно захищені завдяки підтримці в комутаторі D-Link технології фізичного стекування, яка дозволяє об'єднувати до восьми пристроїв у єдиний логічний стек із

пропускною здатністю до 80 Гбіт/с. Це гарантує легке масштабування мережі в майбутньому та спрощує адміністрування системи за рахунок керування через одну IP-адресу. З економічного погляду вибір D-Link DGS-1520-52 дозволяє заощадити понад чотири тисячі гривень порівняно з моделлю від Ubiquiti, повністю виключаючи неефективні витрати на непотрібний функціонал живлення по крученій парі. У підсумку, цей комутатор демонструє найкраще співвідношення вартості та функціональних можливостей, забезпечуючи високу відмовостійкість, швидкість і готовність корпоративної мережі до подальшої модернізації [23].

2.3.2 Вибір міжмережевого екрану (Dual-WAN)

Обґрунтування вибору міжмережевого екрану з підтримкою кількох WAN-інтерфейсів для проєктованої комп'ютерної мережі базується на аналізі технічних характеристик, рівня безпеки, можливостей масштабування та інтеграції пристрою в корпоративну інфраструктуру підприємства. Оскільки логістична чи офісна мережа потребує високої відмовостійкості, надійного захисту каналів зв'язку та стабільної обробки трафіку від багатьох користувачів, пристрій має забезпечувати балансування навантаження та мати достатній запас продуктивності.

У таблиці 2.4 порівняно три міжмережеві екрани [16] з підтримкою багатоканального WAN-підключення, резервування або балансування навантаження між каналами Інтернету.

Таблиця 2.4 - Техніко-економічні характеристики міжмережевих екранів

Характеристика	Модель 1	Модель 2	Модель 3
1	2	3	4
Модель	Ruijie Reyee RG-EG209GS	TP-LINK Omada ER7406	Hikvision DS-3WG507G-SI
Орієнтовна ціна, грн.	6 879	6 804	8 793

Продовження таблиці 2.4

1	2	3	4
Призначення	Офісний / серверний маршрутизатор для SMB, офісу, готелю, школи, роздрібної торгівлі, CCTV.	Офісний / серверний VPN-шлюз Omada для малого та середнього бізнесу.	Серверний маршрутизатор для SMB, офісу, готелю та сценаріїв високошвидкісного доступу до Інтернету.
Підтримка двох і більше каналів Інтернету	Є Multi-WAN, балансування навантаження та резервування каналів; до 4 WAN за рахунок перемикання портів LAN/WAN та SFP.	До 5 WAN-портів і додатковий USB WAN через LTE-модем; підтримка балансування навантаження.	До 6 WAN із балансуванням; 3 WAN-порти з 2 перемикними WAN/LAN.
Порти Ethernet / SFP	8 × 10/100/1000BASE-T, з них 5 фіксованих LAN і 1 фіксований WAN; 1 × SFP LAN/WAN.	5 × Gigabit RJ45: 1 × WAN і 4 × WAN/LAN; 1 × Gigabit SFP WAN/LAN; 1 × USB 3.0.	3 × Gigabit WAN з 2 WAN/LAN switchable; 4 × Gigabit LAN з 3 LAN/WAN switchable
Швидкість LAN-портів, Гбіт/с	1	1	1
Продуктивність / пропускна здатність	600 Мбіт/с у звичайному режимі; до 1000 Мбіт/с у Turbo Mode.	NAT близько 945 Мбіт/с; DPI TCP/UDP близько 933/927 Мбіт/с.	Throughput 1000 Мбіт/с; forwarding capacity 14 Гбіт/с.
VPN	Підтримка IPSec, OpenVPN, PPTP, L2TP.	SSL/IPSec/GRE/WireGuard/PPTP/L2TP VPN та OpenVPN.	IPSec VPN, L2TP VPN; до 100 IPSec-з'єднань.
VLAN / мережеві функції	Підтримка політик трафіку, multi-WAN, bandwidth management.	IEEE 802.1Q, multi-net DHCP, NAT, PPPoE, SNMP, ACL, VPN, DPI.	ARP, VLAN, DHCP Server, DDNS, UPnP, IGMP/MLD Snooping, multicast, NAT.

Продовження таблиці 2.4

1	2	3	4
Функції безпеки	Firewall, контроль доступу, керування смугою пропускання, політики трафіку, хмарне адміністрування.	DoS/DDoS protection, IP/MAC/URL filtering, DPI, IPS/IDS, ACL, ARP inspection, web filtering.	Firewall policies, DDoS defending, IP/MAC/URL filtering, ARP defending, захист від Ping of Death, SYN Flood, UDP Flood, IP spoofing тощо.
Керування	Ruijie Cloud / Reyee App, віддалене керування та моніторинг.	Omada SDN: централізоване хмарне керування через web або Omada app.	Web management, Hik-Partner Pro, віддалене керування, перегляд топології, перезапуск портів, віддалене оновлення.
Пам’ять	Flash 32 МБ; RAM 256 МБ.	Flash 128 МБ NAND; DRAM 512 МБ DDR4.	Flash 32 МБ; RAM 512 МБ.
Живлення	12 В.	100–240 В AC, 50/60 Гц.	100–240 В AC, 50/60 Гц, 1 А.
Монтаж	Настільний.	Настільний або монтаж у стійку.	Настільний або монтаж у стійку.
Габарити	202 × 108 × 28 мм.	294 × 140 × 44 мм.	440 × 227,4 × 44 мм.

Аналіз наданих варіантів показує, що пристрій Ruijie Reyee RG-EG209GS хоч і є привабливим за ціною, має обмежений об'єм оперативної пам'яті та настільне виконання, що ускладнює його монтаж у серверну стійку. Модель Hikvision DS-3WG507G-SI пропонує високу щільність портів та стоєчне виконання, проте є найдорожчою серед представлених та має дещо вужчий

набір підтримуваних VPN-протоколів. У результаті комплексного оцінювання найбільш збалансованим та технічно виправданим рішенням є вибір маршрутизатора TP-LINK Omada ER7406 (див. рис. 2.3) для офісної мережі ТОВ «АВЕРС НК.

Рисунок 2.3 - Маршрутизатор TP-LINK Omada ER707-M2

Маршрутизатор TP-LINK Omada ER7406 забезпечує безпрецедентний рівень відмовостійкості завдяки можливості організації до п'яти WAN-портів одночасно з підтримкою інтелектуального балансування навантаження. Це дозволяє підключати лінії від кількох незалежних інтернет-провайдерів та додатковий мобільний брекаут через USB LTE-модем, що гарантує безперебійну роботу інформаційних систем компанії навіть у разі аварії на магістральному кабелі. Продуктивність пристрою на рівні 945 Мбіт/с для трансляції мережевих адрес (NAT) у поєднанні з великим об'ємом сучасної оперативної пам'яті DRAM 512 МБ DDR4 дозволяє стабільно обробляти до 150 тисяч одночасних сесій без затримок у передачі даних. Пристрій також має суттєву перевагу у сфері безпеки, пропонуючи вбудовані інструменти захисту від DoS/DDoS-атак, інспекцію пакетів DPI, системи IPS/IDS та фільтрацію за IP, MAC та URL-адресами, що мінімізує ризики зовнішнього втручання в корпоративну мережу.

Ще одним вагомим інженерним аргументом на користь TP-LINK Omada ER7406 буде його повна готовність до побудови безпечних розподілених мереж, тобто підтримка широкого спектру VPN-технологій та сучасного високошвидкісного протоколу WireGuard, а також SSL, IPsec, GRE та OpenVPN, що дуже важливо для безпечного підключення віддалених філій або

складських терміналів. Інтеграція в екосистему Omada SDN забезпечує можливість зручного централізованого хмарного керування всією мережевою інфраструктурою через єдиний веб-інтерфейс. Конструктивне виконання пристрою передбачає як настільне розміщення, так і повноцінний монтаж у телекомунікаційну стійку, а офіційна п'ятирічна гарантія підтверджує високу надійність компонентної бази. З урахуванням оптимальної вартості, яка є нижчою за рішення від Hikvision, цей маршрутизатор гарантує найкраще співвідношення функціональності, безпеки та економічної доцільності для створення ядра сучасної комп'ютерної мережі [35].

2.3.3 Вибір єдиної апаратної платформи для розгортання трьох серверів

Для мережі логістичної компанії ТОВ «АВЕРС НК» з трьома серверами доцільно розподілити їхні функції так, щоб забезпечити стабільну роботу користувачів, збереження даних, безпеку, централізоване адміністрування та підтримку логістичних бізнес-процесів. Оптимально виділити окремий сервер для інфраструктурних служб, окремий — для бізнес-систем, і окремий — для файлів, резервного копіювання та допоміжних сервісів.

S_1 — інфраструктурний сервер має бути основою адміністрування мережі. На ньому доцільно розмістити Active Directory, DNS і DHCP. Це дозволить централізовано створювати облікові записи працівників, об’єднувати їх у групи за відділами, налаштовувати права доступу та автоматично видавати IP-адреси пристроям у відповідних VLAN. Для логістичної компанії це важливо, оскільки різні підрозділи мають мати різні права доступу: бухгалтерія — до фінансових ресурсів, логістика — до логістичних систем, адміністрація — до управлінських документів. Наприклад, користувачі з VLAN FINANCE можуть отримувати доступ лише до бухгалтерських ресурсів, а користувачі з VLAN OPERATIONS — до логістичних баз і CRM.

S_2 — сервер прикладних систем логістики та баз даних CRM, ERP або WMS/TMS-система, база даних перевезень, облік заявок, маршрути, клієнтська база, складські операції, взаємодія з диспетчерами та відділом логістики Це основний робочий сервер для бізнес-процесів компанії. Саме цей сервер буде найбільш критичним для щоденної роботи диспетчерів, логістів, менеджерів із постачання, адміністративно-господарського відділу та відділу маркетингу й аналітики. Він обслуговує диспетчерів, логістів, відділ постачання, маркетинг, адміністрацію та інші підрозділи, які працюють із замовленнями, маршрутами, залишками, клієнтами й перевезеннями. Його варто виділити окремо, щоб бізнес-додатки не залежали від файлового сервера чи служб домену.

S_3 — файловий і резервний сервер потрібен для централізованого зберігання документів та резервного копіювання. У логістичній компанії накопичується багато робочих файлів: договори, рахунки, акти, накладні, маршрути, скановані документи, звіти, таблиці, службова переписка. Якщо зберігати все лише на окремих ПК, зростає ризик втрати даних. Тому файловий сервер дає змогу створити окремі папки для бухгалтерії, логістики, адміністрації, юридичного відділу, постачання та інших підрозділів із різними правами доступу. Окрема роль резервного копіювання важлива для захисту даних у разі збою, помилки користувача, вірусної атаки або пошкодження основного сервера.

Такий поділ функцій зменшує навантаження на кожен сервер і підвищує надійність мережі. Якщо файловий сервер тимчасово недоступний, доменна авторизація та логістична система можуть продовжувати працювати. Якщо потрібно обслуговувати або оновлювати бізнес-додатки на S_2, це не вплине безпосередньо на роботу DNS, DHCP чи облікових записів користувачів на S_1.

Крім того, такий розподіл полегшує налаштування правил доступу між VLAN. Наприклад, до S_1 мають звертатися всі корпоративні сегменти для автентифікації та DNS, до S_2 — лише підрозділи, що працюють із логістичними й управлінськими системами, а до S_3 — користувачі відповідно

до своїх прав на файлові ресурси. Гостьовий Wi-Fi при цьому не повинен мати доступу до жодного з цих серверів.

Для мережі логістичної компанії планується використання єдиної апаратної платформи для розгортання трьох серверів. Тому важливим є підібрати максимально універсальне, продуктивне та економічно вигідне рішення, здатне ефективно виконувати ролі бази даних, інфраструктурного вузла та сховища резервних копій. На основі наданих техніко-економічних характеристик у таблиці 2.5 [18] беззаперечним лідером є сервер Dell PowerEdge R750xs (див. рис. 2.4). Ця модель пропонує обчислювальні потужності корпоративного класу, високу відмовостійкість та найкращі можливості масштабування дискової підсистеми за найнижчою ціною серед усіх представлених конкурентів.

Таблиця 2.5 - Техніко-економічні характеристики апаратних платформ серверів

Характеристика	Модель 1	Модель 2	Модель 3
1	2	3	4
Модель	HP ProLiant DL380 Gen10 (P0571-B21)	Lenovo ThinkSystem SR630 V2 (7Z73A06FEA)	Dell PowerEdge R750xs (210-R750XS-16SFF)
Орієнтовна вартість, грн.	115722	137034	109505
Висота	2U	1U	2U
Тип сервера	Стійковий (Rack)	Стійковий (Rack)	Стійковий (Rack)
Тип пам’яті	DDR4	DDR4	DDR4
Обсяг оперативної пам’яті, ГБ	32	32	32
Кількість слотів пам’яті	24	32–64	Не зазначено в наданій таблиці
Процесор	Intel Xeon Silver 4210R	Intel Xeon	Intel Xeon Gold 6248R
Кількість процесорів	1	1	1

Продовження таблиці 2.5

1	2	3	4
Форм-фактор дисків	3,5"	2,5"	2,5"
Блоки живлення	2	1	2
RAID-контролер	HPE Smart Array P408i-a/2GB, RAID 0/1/5/6/10/50/60	Intel C621A controller SATA 6 Gb/s; RAID 0/1/5/10, M.2	PERC/H755; підтримка RAID
Мережева підсистема	1 × 1GbE; можливість встановлення додаткових мережевих адаптерів	1 × LAN, 2 × USB 2.0; модуль OCP NIC 3.0	1 × iDRAC, 1 × 1GbE; окреме керування
Накопичувачі / дискова підсистема	8SFF, підтримка до 16 дисків, гаряча заміна	8 × 2,5" hot-swap; можливість встановлення NVMe/SAS/SATA	16 × 2,5" hot-swap; 1 × 480 ГБ SSD

Рисунок 2.4 - Сервер Dell PowerEdge R750xs

Головною технічною перевагою моделі від Dell є використання високопродуктивного процесора Intel Xeon Gold 6326 із базовою тактовою частотою 2,9 ГГц та 16 обчислювальними ядрами. Для порівняння, дорожчі варіанти від HP та Lenovo оснащені значно слабшими процесорами лінійки Intel Xeon Silver на 10 та 12 ядер відповідно. Наявність процесора рівня Gold є критично важливою для першого сервера (операційного ядра), оскільки гарантує миттєву обробку тисяч транзакцій у системі управління складом (WMS) та базах даних без затримок. Крім того, Dell PowerEdge R750xs оснащено двома дубльованими блоками живлення потужністю 800 Вт, що

забезпечує безперебійну роботу інфраструктури в разі проблем з електромережею, тоді як модель від Lenovo має лише один блок живлення. Не менш важливим є дисковий потенціал: Dell підтримує встановлення до 16 накопичувачів та має апаратний RAID-контролер H755. Це ідеально задовольняє потреби третього сервера (безпеки та резервного копіювання), дозволяючи створити величезний масив для зберігання відеоархівів та бекапів, з чим базові 8 слотів у конкурентів впоралися б значно гірше.

З економічної точки зору вибір Dell PowerEdge R750xs є максимально раціональним рішенням для бюджету логістичної компанії. Вартість одного такого сервера становить 109 505 гривень, що робить його найдешевшим з трьох варіантів. Оскільки для побудови повноцінної архітектури необхідно придбати відразу три однакові машини, загальна економія порівняно з рішенням від HP (115 722 грн) складе понад 18 тисяч гривень, а порівняно з невиправдано дорогим Lenovo (137 034 грн) бюджет компанії збереже понад 82 тисячі гривень. Таким чином, обираючи Dell, підприємство отримує найпотужнішу апаратну базу з найкращим процесором, відмінним потенціалом для зберігання даних та повним резервуванням живлення за найнижчою ринковою вартістю.

2.3.4 Вибір безпровідної точки доступу

Обґрунтування вибору бездротових точок доступу для проєктованої комп'ютерної мережі логістичної компанії базується на зіставленні технічних параметрів, ємності клієнтської бази, можливостей централізованого керування та цінового фактора. Порівняльний аналіз трьох моделей стандарту Wi-Fi 6 у таблиці 2.6 [14] дозволяє одразу відхилити точку доступу Huawei eKit AP361, оскільки за ціни 4044 гривні вона суттєво поступається конкурентам за швидкісними характеристиками, маючи обмеження максимальної швидкості на рівні 1775 Мбіт/с та ширину каналу лише 80 MHz. Модель Cudy AP3000 хоч і має перевагу у вигляді швидкісного мережевого порту на 2.5 Gigabit Ethernet

та ширшого температурного діапазону, є найдорожчою серед представлених варіантів (4253 грн.) і має меншу рекомендовану кількість одночасних клієнтів. З огляду на це, найбільш технічно доцільним та економічно вигідним рішенням є вибір точки доступу TP-Link EAP653.

Таблиця 2.6 - Техніко-економічні характеристики точок доступу

Характеристика	Модель 1	Модель 2	Модель 3
1	2	3	4
Модель	TP-Link EAP653 WiFi 6	Cudy AP3000 White	Huawei eKit AP361 Wi-Fi 6
Орієнтовна вартість, грн.	3959	4253	4044
Клас / стандарт Wi-Fi	Wi-Fi 6 (IEEE 802.11ax/ac/n/g/b/a)	Wi-Fi 6	Wi-Fi 6 (IEEE 802.11ax, сумісність із 802.11a/b/g/n/ac)
Частотні діапазони	2.4 ГГц і 5 ГГц	2.4 ГГц і 5 ГГц	2.4 ГГц і 5 ГГц
Максимальна сумарна швидкість Wi-Fi	2976 Мбіт/с: 574 Мбіт/с (2.4 ГГц) + 2402 Мбіт/с (5 ГГц)	2976 Мбіт/с: 574 Мбіт/с (2.4 ГГц) + 2402 Мбіт/с (5 ГГц)	1775 Мбіт/с: 575 Мбіт/с (2.4 ГГц) + 1200 Мбіт/с (5 ГГц)
Просторові потоки / MIMO	2x2 на 2.4 ГГц + 2x2 на 5 ГГц; MU-MIMO, OFDMA	2 потоки на 2.4 ГГц + 3 потоки на 5 ГГц; MU-MIMO, OFDMA	2x2 на 2.4 ГГц + 2x2 на 5 ГГц; MU-MIMO, OFDMA
Максимальна ширина каналу	До 160 МГц	До 160 МГц	До 80 МГц
Мережевий порт	1 x Gigabit Ethernet RJ-45	1 x 2.5 Gigabit Ethernet RJ-45	1 x Gigabit Ethernet RJ-45
Живлення	802.3at PoE, 48V Passive PoE або 12 В DC; адаптер живлення не входить у комплект	802.3at/af PoE, 48–57 В Passive PoE або 12 В DC; адаптер залежить від версії	PoE за стандартом IEEE 802.3af
Максимальне споживання	14.7 Вт	12 Вт	9.4 Вт
Кількість одночасних клієнтів	250+	Рекомендовано до 150; максимальна місткість 256	До 128 клієнтів

Продовження таблиці 2.6

1	2	3	4
Орієнтовна площа покриття	До 140 м²	До 130 м²	До 130 м²
Антени	Вбудовані: 2x4 dBi (2.4 ГГц), 2x5 dBi (5 ГГц)	5 вбудованих антен	Вбудовані smart-антени: 4 dBi (2.4 ГГц), 5 dBi (5 ГГц)
Кількість SSID / VLAN	До 16 SSID, SSID-to-VLAN Mapping, Management VLAN	До 8 SSID, VLAN Support	До 12 SSID, SSID-based VLAN assignment, VLAN trunk
Безпека	WPA/WPA2/WPA3 Personal/Enterprise, captive portal, ACL, ізоляція клієнтів, rogue AP detection	WPA/WPA2/ WPA3, captive portal, MAC-фільтр, SPI Firewall, DoS Protection	WPA/WPA2/WPA3, 802.1X, ACL, STA isolation, CAPWAP/DTLS у Fit AP
Роумінг / Mesh	Omada Mesh, Seamless Roaming, Band Steering, Load Balancing	Cudy Mesh, wired/wireless backhaul, 802.11k/v, band steering	802.11k/v smart roaming, 802.11r fast roaming, Fat/Fit/cloud mode
Централізоване керування	Omada Cloud-Based / Hardware / Software Controller, Omada App, Cloud Access	Cudy AP Controller C200P, централізоване керування до 200 AP	Cloud management, Fit/Fat AP, HUAWEI eKit app
Робоча температура	0 °C ... +40 °C	-10 °C ... +60 °C	-10 °C ... +50 °C
Розміри	160 x 160 x 33.6 мм	Ø231.9 x 57.1 мм	Ø180 x 35 мм

Точка доступу TP-Link EAP653 (див. рис. 2.5) пропонує найнижчу ціну на ринку, яка становить 3959 гривень, забезпечуючи при цьому максимальну сумарну швидкість бездротового зв'язку до 2976 Мбіт/с та підтримку повноцінної ширини каналу до 160 MHz у діапазоні 5 ГГц. Це гарантує швидкий та стабільний обмін даними для більш ніж 250 одночасних пристроїв, що повністю закриває потреба складських приміщень з великою кількістю

терміналів збору даних та офісної частини компанії. Вирішальним архітектурним аргументом на користь цієї моделі є її повна інтеграція в єдину централізовану екосистему Omada SDN, що забезпечує безшовну синергію з раніше обраним головним маршрутизатором TP-LINK Omada ER7406. Таке рішення дозволяє адміністратору здійснювати керування, моніторинг та налаштування всієї мережевої інфраструктури, включаючи безпеку, гостьові портали та мапування віртуальних мереж на 16 різних бездротових мереж (SSID), через один зручний інтерфейс управління без додаткових витрат на стороннє програмне забезпечення.

Рисунок 2.5 - Точка доступу TP-Link EAP653

Окрім значних переваг в адмініструванні, модель від TP-Link підтримує передові стандарти безшовного роумінгу (802.11k/v), що критично важливо для логістичного комплексу, де персонал із мобільними терміналами постійно переміщується між зонами покриття без ризику розриву сесії чи втрати пакетів даних. Пристрій гнучко підтримує живлення за стандартом Power over Ethernet (802.3at PoE) або пасивне 48 В, що полегшує його монтаж на стелях та високих конструкціях без підведення окремих силових розеток. У підсумку, вибір TP-Link EAP653 забезпечує підприємству не лише пряму фінансову економію під час закупівлі обладнання, а й створює масштабовану, безпечну та надзвичайно просту в обслуговуванні бездротову інфраструктуру з найвищими експлуатаційними показниками [33].

2.3.5 Вибір мережевого принтера з двостороннім друком

Обґрунтування вибору мережевого принтера для проєктування інфраструктури логістичної компанії базується на оцінці сукупної вартості володіння, типу друку, мережевої інтеграції та кросплатформеної сумісності обладнання. Аналіз наданих у таблиці 2.7 [15] рішень дозволяє обрати найкращим варіантом для комп'ютерної мережі принтер HP Color LaserJet Pro 3202dn.

Таблиця 2.7 - Техніко-економічні характеристики мережевих принтерів

Характеристика	Модель 1	Модель 2	Модель 3
Модель	Brother HL-L6250DN	Kyocera ECOSYS PA2100CX	HP Color LaserJet Pro 3202dn
Тип пристрою	Принтер	Принтер	Принтер
Тип друку	Лазерний, ч/б	Лазерний, кольоровий	Лазерний, кольоровий
Формат друку	A4	A4	A4
Максимальна роздільна здатність	1200×1200 dpi	1200×1200 dpi	600×600 dpi
Автоматичний дуплекс	Так	Так	Так
Мережевий інтерфейс	Ethernet 10/100/1000	Ethernet 10/100/1000	Ethernet 10/100/1000
Підтримка ОС	Linux, Windows	Linux, MacOS, Windows	Android, Linux, MacOS, Windows, iOS
Орієнтовна ціна, грн.	17541	18156	13632

Принтер HP Color LaserJet Pro 3202dn (див. рис. 2.6) забезпечує повноцінний лазерний кольоровий друк, що дозволяє логістичній компанії якісно виготовляти не лише стандартні товарно-транспортні накладні, а й кольорові маркування для вантажів, брендовані бланки чи аналітичні звіти. Максимальна роздільна здатність у 600x600 dpi у поєднанні з функцією автоматичного дуплексу є повністю достатньою для чіткого відображення штрих-кодів і дрібних шрифтів, а режим двостороннього друку допомагає підприємству суттєво оптимізувати витрати на папір.

Рисунок 2.6 - Принтер HP Color LaserJet Pro 3202dn

Вирішальною інфраструктурною перевагою рішення від HP є його безпрецедентна сумісність із широким спектром операційних систем. З економічного погляду вибір HP Color LaserJet Pro 3202dn є найбільш виправданим, оскільки його ціна становить 13632 гривні, що дозволяє заощадити близько чотирьох тисяч гривень на кожному пристрої порівняно з конкурентами. Така значна фінансова економія у поєднанні з передовим мережевим потенціалом робить цей принтер найкращим вибором для успішної реалізації проєкту [25].

2.3.6 Вибір пасивного мережевого обладнання

Для побудови сучасної та надійної локальної мережі необхідне використання якісного пасивного мережевого обладнання, яке забезпечить

стабільну передачу даних, зручність адміністрування та можливість подальшого розширення інфраструктури. Кабелі категорії Cat.6, патч-корди, мережеві розетки та патч-панелі дозволяють організувати структуровану кабельну систему з підтримкою високошвидкісного Gigabit Ethernet. Використання екранованого мідного кабелю забезпечує мінімальні втрати сигналу та захист від електромагнітних завад, що особливо важливо для стабільної роботи офісної мережі та серверного обладнання.

Монтажна серверна шафа, кабельні організатори, сітчасті лотки та пластикові короби необхідні для правильного розміщення й захисту кабельної інфраструктури. Вони забезпечують впорядкованість мережі, покращують вентиляцію обладнання та спрощують технічне обслуговування. Додатково використання PoE-інжектора дозволить передавати живлення до точки доступу, що зменшує витрати на електропроводку та спрощує монтаж.

Для забезпечення безперервної роботи мережі та захисту обладнання від перепадів напруги необхідно використовувати джерело безперебійного живлення Smart-UPS. Воно дозволяє уникнути втрати даних і пошкодження техніки під час аварійного вимкнення електроенергії.

SSD-накопичувачі великого обсягу забезпечують швидке зберігання та обробку інформації для серверів.

Придбання вказаного в таблиці 2.8 обладнання є необхідним для створення продуктивної, надійної та безпечної мережевої інфраструктури. В таблицю також буде занесено необхідне активне обладнання.

Таблиця 2.8 - Перелік мережевого обладнання

Обладнання	Позначення	Модель	Ціна, грн.	К-ть	Од. виміру
1	2	3	4	5	6
Комутатор	SW-1	D-Link DGS-1520-52	49999	1	шт.

Продовження таблиці 2.8

1	2	3	4	5	6
Міжмережевий екран	FW_1	TP-LINK Omada ER7406	6804	1	шт.
Сервер	S_1- S_3	Dell PowerEdge R750xs	109505	3	шт.
SSD диск	-	CUSU C300 2TB 2.5" SATAIII	8499	6	шт.
Точка доступу	AP_1	TP-Link EAP653	3959	1	шт.
PoE-інжектор	-	2E PowerLink PSE801G (1xGE, 1xGE PoE, 802.3af/at	629	1	шт.
Мережевий принтер	PR_1- PR_7	HP Color LaserJet Pro 3202dn	13632	7	шт.
ДБЖ	-	Smart-UPS LogicPower 6000 PRO RM	73000	1	шт.
LAN кабель , 305м	-	Cablexpert CAT6 одножильна мідь гелеєве наповнення	9999	5	шт.
Шафа монтажна настінна	-	CMS MGSWA 21U	15040	1	шт.
Патч-панель 19" 24xRJ-45 UTP 1U cat.6	-	Pipo	1434	2	шт.

Продовження таблиці 2.8

1	2	3	4	5	6
Кабельний організатор 19' 1U, перфорований	-	Digitus	579	2	шт.
Подовжувач до серверної шафи RACK 1.8м 4 розетки	-	Qoltec	859	1	шт.
Розетка однопортова RJ-45, 6 cat, зовнішня	-	Cablexpert	94	36	шт.
Патч-корд CAT6 UTP 3 м	-	Cablexpert	99	36	шт.
Патч-корд литий UTP RJ45 Cat.6 0.5м	-	RITAR	73	40	шт.
Короб пластиковий 25x16x2000мм	-	АСКО STEP	63,89	35	шт.
Сітчастий лоток 100x50 мм, оцинкований,	-	Ardic	213,97	110	м

2.4 Особливості монтажу мережі

Проєктована комп'ютерна мережа будується за централізованим принципом: усі кабельні лінії від робочих станцій, принтерів, серверів та точки доступу Wi-Fi сходяться до центрального комутаційного вузла SW_1,

розміщеного в серверній кімнаті. Така схема є зручною для монтажу, оскільки всі підключення зводяться в одне технічне приміщення – серверну кімнату, де можна встановити телекомунікаційну шафу, патч-панелі, комутатор, міжмережевий екран, джерело безперебійного живлення та організувати централізоване обслуговування мережі.

Оскільки в приміщенні передбачено підвісну стелю, основні кабельні траси доцільно прокладати саме в застельовому просторі. Це дозволяє приховати кабелі, не порушувати зовнішній вигляд кабінетів і коридорів, а також спростити прокладання магістральних ділянок до віддалених робочих місць. Кабелі від серверної кімнати прокладаються над підвісною стелею вздовж коридорів, після чого виконуються відгалуження до окремих кабінетів і робочих місць.

Для монтажу використовуватиметься кабель вита пара категорії Cat 6, оскільки він забезпечує роботу мережі на швидкості до 1 Гбіт/с і має достатній запас для офісної локальної мережі. Кожне робоче місце, мережевий принтер або точка доступу повинні підключатися окремою кабельною лінією до патч-панелі в серверній. Це відповідає фізичній топології «зірка», де пошкодження однієї лінії не впливає на працездатність інших підключень.

У серверній кімнаті необхідно встановити телекомунікаційну шафу 24”, у якій розміщуються патч-панелі, комутатор SW_1, міжмережевий екран, ДБЖ та інше мережеве обладнання. Усі кабельні лінії з кабінетів мають заводитися в цю шафу, термінуватися на патч-панелі тієї ж категорії та з’єднуватися з комутатором короткими патч-кордами (0,5м). Такий підхід спрощує адміністрування, дозволяє швидко змінювати підключення портів і полегшує пошук несправностей.

Прокладання кабельних трас над підвісною стелею потрібно виконувати впорядковано. Кабелі не слід просто укладати на плити підвісної стелі або залишати вільно звисати. Їх доцільно прокладати в кабельних лотках. Це захищає кабелі від механічних пошкоджень, спрощує подальше

обслуговування і дозволяє акуратно організувати велику кількість ліній, що сходяться до серверної.

Основні кабельні траси доцільно прокласти вздовж центральних коридорів, а від них виконати відгалуження до приміщень з мережевими пристроями та ПК. Така організація зменшує довжину окремих ліній, робить трасування більш логічним і полегшує маркування.

У кожному кабінеті кабель із застельового простору потрібно опускати до робочого місця у вертикальному кабельному каналі. На кінці лінії встановлюється інформаційна розетка RJ-45 категорії 6.

Для бездротової мережі на схемі передбачена точка доступу AP_1 в переговорній кімнаті. Кабель до точки доступу також прокладається над підвісною стелею. Оскільки точка доступу підтримує PoE, її живлення буде організоване без окремої електричної розетки — через мережевий кабель від PoE-інжектора.

Під час прокладання кабелів важливо дотримуватися відстані від силових електричних ліній, світильників, кабелів живлення кондиціонерів та іншого обладнання, яке може створювати електромагнітні завади. Якщо перетин із силовим кабелем неминучий, його бажано виконувати під прямим кутом. Також потрібно уникати різких перегинів кабелю, надмірного натягу, стискання стяжками та прокладання поруч із джерелами нагрівання.

Усі кабельні лінії потрібно промаркувати з обох боків: біля інформаційної розетки в кабінеті та на патч-панелі в серверній кімнаті. Маркування має відповідати таблиці підключень, наприклад: номер кабінету, номер робочого місця, номер розетки, номер порту патч-панелі та номер порту комутатора. Це значно спростить експлуатацію мережі, пошук несправностей і подальше розширення.

Після завершення монтажу необхідно виконати тестування кожної кабельної лінії. Перевіряють правильність обтискання, цілісність пар, відсутність коротких замикань, переплутаних жил, обривів і відповідність лінії обраній категорії. За результатами перевірки формується кабельний журнал або

таблиця підключень. Лише після цього можна виконувати підключення активного обладнання, налаштування VLAN, IP-адресації та перевірку доступу до серверів, принтерів, Wi-Fi і мережі Інтернет.

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій

Для логістичної компанії ТОВ «АВЕРС НК» вибір операційних систем та програмного забезпечення базується на створенні надійної, безпечної та високоефективної екосистеми. Розподіл завдань між трьома окремими серверами дозволяє уникнути взаємного впливу сервісів, підвищує загальну відмовостійкість і допомагає оптимізувати ліцензійні витрати. Клієнтська частина мережі при цьому будується так, щоб забезпечити безперешкодний, але контрольований доступ до корпоративних ресурсів із дотриманням суворих інструментів безпеки.

Для проектованої мережі логістичної компанії ТОВ «АВЕРС НК» доцільно використовувати серверні ОС сімейства Windows Server 2022, оскільки вони забезпечують централізоване адміністрування, підтримку доменної структури Active Directory, інтеграцію мережевих служб та високий рівень безпеки. Для робочих ПК оптимальним вибором є Windows 11 Pro, яка підтримує роботу в домені, групові політики, віддалене адміністрування та сучасні механізми захисту корпоративної мережі. Таке поєднання забезпечує сумісність усіх служб мережі, зручність централізованого управління користувачами та стабільну роботу ППЗ.

Перший сервер S_1, який виконує роль інфраструктурного ядра мережі, доцільно розгорнути на базі операційної системи Windows Server 2022 Standard із ролями Active Directory Domain Services, DNS та DHCP. Active Directory дозволяє централізовано створювати облікові записи працівників, об’єднувати їх у групи за підрозділами та призначати права доступу відповідно до структури підприємства. DNS забезпечує коректне функціонування доменної мережі та

швидкий доступ до ресурсів, а DHCP автоматизує видачу IP-адрес у різних VLAN. Таке інженерне рішення дозволяє централізовано керувати обліковими записами всіх працівників компанії, об’єднуючи їх у логічні групи за специфікою діяльності, наприклад, бухгалтерію, логістику чи адміністрацію. Завдяки тісній інтеграції цих служб стає можливим автоматичний розподіл пристроїв за відповідними віртуальними мережами. Додатково на сервері можуть використовуватись Group Policy, Windows Defender та служби журналювання подій для централізованого контролю безпеки мережі, що мінімізує ризики внутрішніх витоків інформації.

Другий сервер S_2, призначений для бізнес-систем і баз даних, доцільно побудувати на базі Windows Server 2022 у поєднанні з Microsoft SQL Server або PostgreSQL залежно від використовуваного ПЗ. На ньому можуть працювати CRM, ERP, WMS або TMS-системи, які забезпечують управління перевезеннями, маршрутами, замовленнями, складськими операціями та клієнтською базою. Винесення бізнес-додатків на окремий сервер підвищує продуктивність і надійність роботи всієї мережі, оскільки навантаження від логістичних систем не впливає на доменні служби чи файловий сервер. Для доступу користувачів до бізнес-додатків можуть використовуватись веб-інтерфейси, віддалені служби Remote Desktop Services або спеціалізовані клієнтські програми. Окремий сервер також спрощує резервування даних, оновлення програмного забезпечення та масштабування системи у майбутньому.

Третій сервер, S_3, який виконує функції файлового та резервного сервера, доцільно використовувати Windows Server 2022 із ролями File Server та Backup Server. Файловий сервер дозволяє централізовано зберігати документи компанії: договори, накладні, маршрути, звіти, бухгалтерські документи та службову документацію. За допомогою NTFS-дозволів і груп Active Directory можна організувати різні рівні доступу до папок для бухгалтерії, юридичного відділу, логістики, маркетингу та адміністрації. Для резервного копіювання доцільно використовувати Veeam Backup & Replication

або вбудовані засоби Windows Server Backup. Це дозволить автоматично створювати резервні копії критично важливих даних, захищати інформацію від вірусних атак, помилок користувачів чи відмов обладнання. Наявність окремого файлового та резервного сервера суттєво підвищує надійність і відмовостійкість усієї інформаційної системи підприємства.

Для робочих станцій, єдиним технічно виправданим вибором є операційна система Windows 11 Professional. Вибір саме професійної редакції обумовлений її здатністю підключатися до створеного домену Active Directory, що закриває питання централізованого оновлення безпеки, віддаленого встановлення клієнтських частин логістичних програм та контролю за використанням периферійних пристроїв. На кожній робочій станції розгортається пакет офісних програм, антивірус із хмарним керуванням. Наявність вбудованої технології шифрування BitLocker у версії Pro гарантує повний захист комерційної таємниці та клієнтської бази компанії у випадку фізичної втрати або викрадення мобільних пристроїв менеджерів поза межами офісу.

Така конфігурація забезпечить сумісність із серверною інфраструктурою, підтримку доменної авторизації та ефективну взаємодію між усіма підрозділами логістичної компанії [20; 22].

2.6 Тестування та налагодження мережі

Після завершення монтажу локальної мережі ТОВ «АВЕРС НК» необхідно провести комплексне тестування та налагодження всієї мережевої інфраструктури. Основною метою цього етапу є перевірка правильності побудови структурованої кабельної системи, коректності роботи серверних служб, доступності мережевих ресурсів та забезпечення стабільної взаємодії між усіма VLAN і мережевими пристроями. Особливу увагу необхідно приділити працездатності інфраструктурного сервера S_1, на якому функціонують Active Directory, DNS та DHCP, оскільки саме ці служби

забезпечують централізовану авторизацію користувачів, автоматичну видачу IP-адрес і коректне функціонування доменної мережі.

Першим етапом тестування є перевірка фізичної кабельної системи. Для цього використовуються кабельні тестери типу Fluke Networks або аналогічні LAN-тестери, які дозволяють визначити правильність обтиску витої пари, наявність обривів, коротких замикань, переплутаних пар та відповідність кабельної системи стандарту Cat.6. Додатково перевіряється цілісність патч-панелей, мережевих розеток та правильність маркування кабельних трас. Після цього виконується тестування комутаторів та VLAN: перевіряється доступність міжмережевої маршрутизації, коректність налаштування trunk-портів і ізоляція трафіку між логічними сегментами мережі. Для контролю з'єднання використовуються стандартні утиліти ping, tracert та ipconfig, які дозволяють перевірити маршрутизацію, отримання IP-адрес через DHCP та доступність серверів.

Окремим етапом виконується тестування серверних служб Active Directory, DNS та DHCP. Перевіряється коректність авторизації користувачів у домені, застосування Group Policy, автоматичне оновлення DNS-записів і правильність видачі IP-адрес для різних VLAN. Для цього використовуються оснастки Windows Server Manager, DHCP Manager, DNS Manager та Active Directory Users and Computers. Також проводиться перевірка резервного копіювання на сервері S_3, тестове відновлення даних і контроль працездатності системи Windows Server Backup. Після завершення всіх перевірок здійснюється моніторинг навантаження мережі та серверів за допомогою журналів подій Windows Event Viewer і системних засобів Performance Monitor. Такий комплекс заходів дозволяє забезпечити стабільну, безпечну та безперебійну роботу мережевої інфраструктури логістичної компанії [13].

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Конфігурування активного комутаційного обладнання

3.1.1 Налаштування міжмережевого екрану TP-LINK Omada ER7406

FW_1 (10.10.10.254) виконує роль міжмережевого екрана та шлюзу виходу до Інтернету для локальної мережі. Маршрутизація між VLAN виконуватиметься на L3-комутаторі SW_1, де для кожного сегмента створено шлюзи 10.10.X.1. На FW_1 покладаються функції підключення до двох незалежних інтернет-каналів, NAT для виходу користувачів в Інтернет, резервування каналу зв'язку, балансування навантаження, контроль доступу між підрозділами та захист критичних серверів S_1, S_2 і S_3.

1. Підключитись до пристрою та здійснити вхід у веб-інтерфейс:

1) Підключити комп'ютер адміністратора до LAN-порту ER7406 патчкордом.

2) На ПК тимчасово встановити автоматичне отримання IP-адреси або адресу з підмережі пристрою за замовчуванням.

3) У браузері відкрити адресу http://192.168.0.1. Під час першого входу створити обліковий запис адміністратора та складний пароль.

4) Після входу змінити стандартні параметри керування: увімкнути HTTPS, обмежити віддалений доступ до веб-інтерфейсу лише з VLAN 40 ENGINEERING-IT або з конкретної IP-адреси адміністратора.

5) Виконати початкові системні налаштування: часовий пояс, дату й час або NTP-синхронізацію; перевірити актуальність прошивки. За потреби оновити прошивку відповідно до інструкції TP-Link.

2. Встановити зрозумілу назву пристрою, наприклад FW_1.

3. Налаштувати два WAN-канали:

1) Перейти до Network → WAN → WAN Mode (див. рис. 3.1).

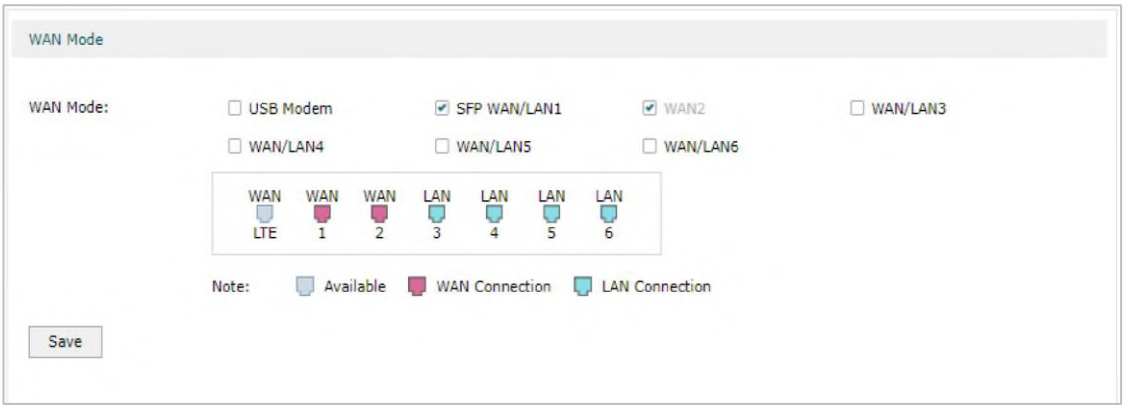

Рисунок 3.1 – Конфігурування WAN

2) Активувати два WAN-порти: WAN1 для основного провайдера та WAN2 / WAN-LAN / SFP WAN для резервного або другого провайдера.

3) Для WAN1 перейти до Network → WAN → WAN1 та вибрати тип підключення згідно з договором провайдера: Dynamic IP (див. рис. 3.2).

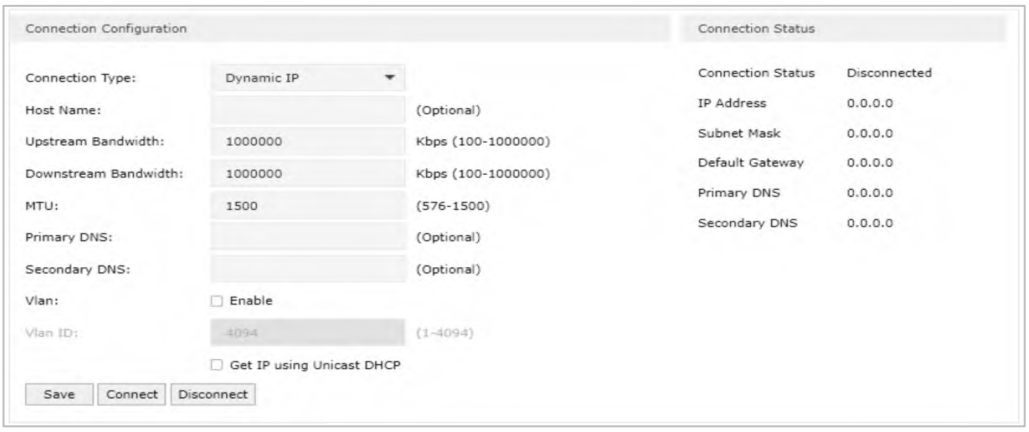

Рисунок 3.2 – Налаштування динамічної IP-адреси

4) Для WAN2 повторити аналогічне налаштування: Static IP (див. рис. 3.3).

5) Для кожного WAN-каналу вказати фактичні значення Upstream Bandwidth і Downstream Bandwidth, оскільки вони використовуються для коректного балансування навантаження.

6) Перевірити, що обидва WAN-інтерфейси мають статус Connected і окремо забезпечують доступ до Інтернету.

Рисунок 3.3 – Налаштування статичної IP-адреси

4. Створити LAN/VLAN-інтерфейси:

1) Перейти до Network → LAN → LAN.

2) У Network List додати шість VLAN відповідно до таблиці адресації 2.2.

3) Для кожної VLAN задати IP-адресу шлюзу 10.10.X.1 та маску 255.255.255.0.

4) У полі DHCP Mode вибрати DHCP Relay, оскільки DHCP-сервером у мережі є S_1.

5) У полі Server Address вказати IP-адресу S_1: 10.10.10.10.

6) Зберегти зміни та перевірити, що кожна VLAN відображається у списку локальних мереж (див. рис. 3.4).

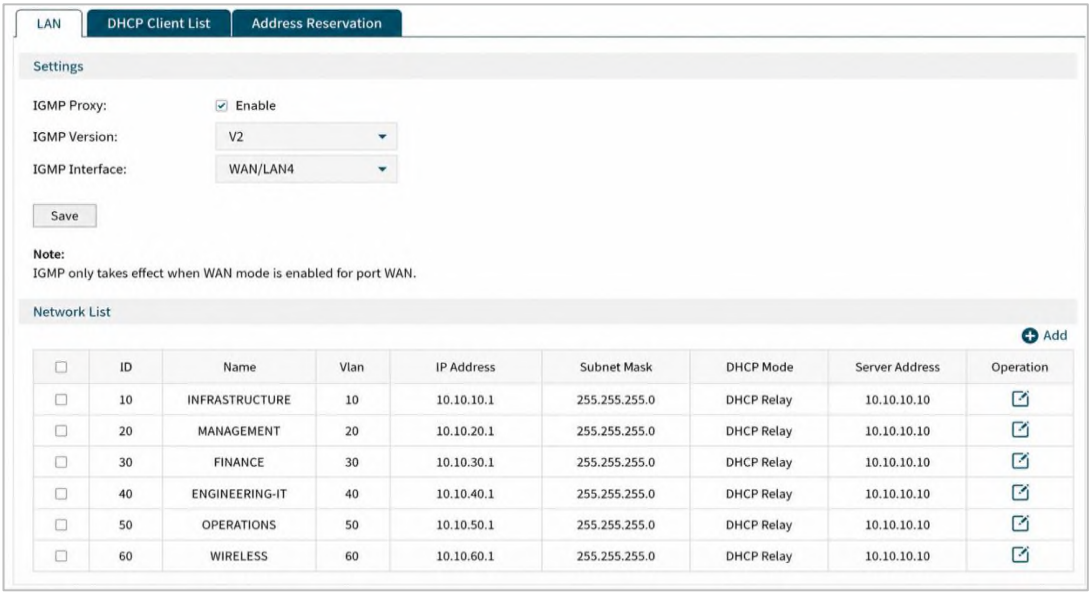

Рисунок 3.4 – Налаштування LAN/VLAN-інтерфейсів

5. Налаштувати trunk-порт до керованого комутатора:

1) Перейти до Network → VLAN → VLAN.

2) Для uplink-порту, який підключений до основного комутатора, дозволити проходження VLAN 10, 20, 30, 40, 50 і 60 у режимі TAG.

3) Для портів, які підключають окремі пристрої безпосередньо до ER7406, встановити відповідну VLAN у режимі UNTAG (див. рис. 3.5).

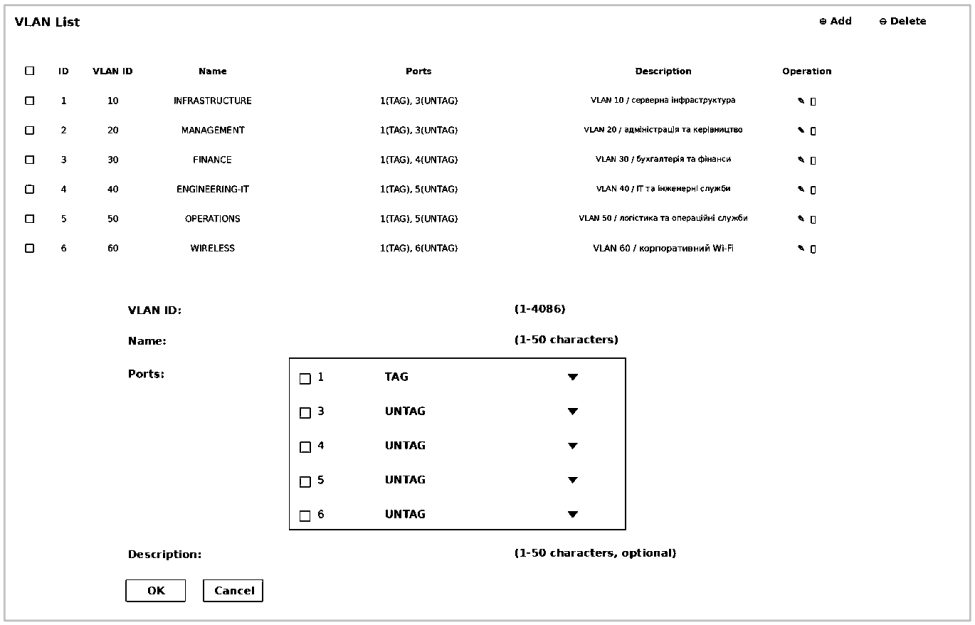

Рисунок 3.5 – Налаштування trunk-порта підключення до комутатора

4) Перейти до Network → VLAN → Port або PVID та призначити PVID для access-портів відповідно до VLAN підключеного обладнання.

5) На комутаторі з іншого боку лінії налаштувати відповідний 48 trunk-порт з такими самими VLAN.

6. Налаштування NAT для доступу до Інтернету:

1) Перейти до Transmission → NAT.

2) Перевірити, що локальні мережі мають трансляцію адрес у напрямку WAN1 і WAN2 (див. рис. 3.6).

3) Не відкривати доступ із Інтернету до внутрішніх серверів без службової потреби. Для віддаленого доступу рекомендовано використовувати VPN, а не пряме відкриття портів.

4) Якщо потрібен публічний доступ до сервісу, створити Virtual Server / Port Forwarding лише для конкретного порту і конкретного внутрішнього сервера з додатковими обмеженнями за IP.

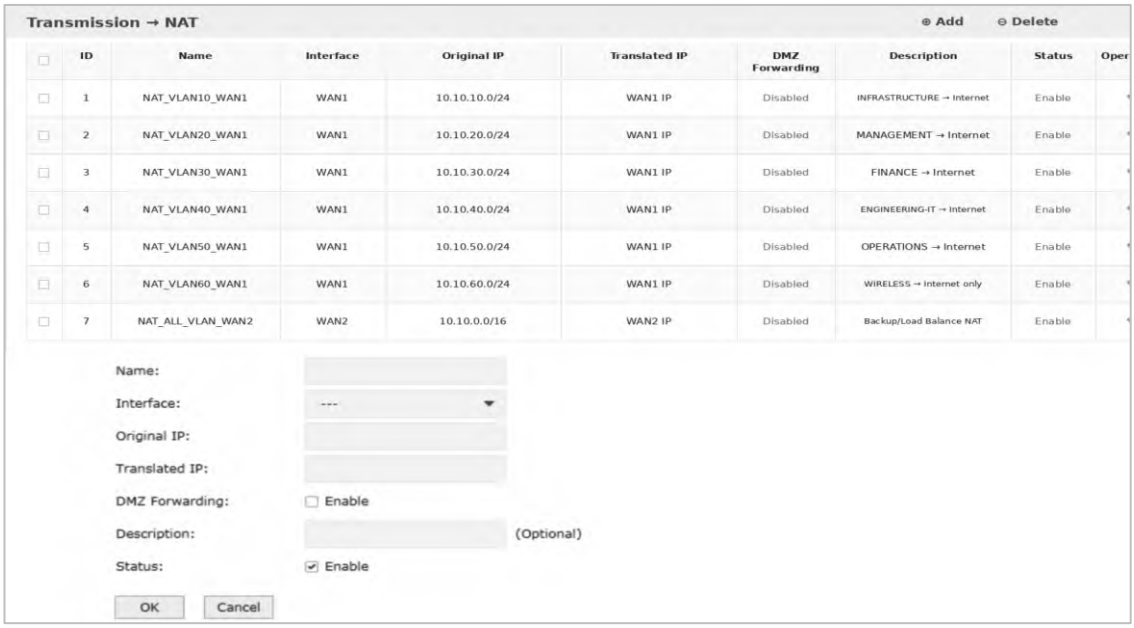

Рисунок 3.6 – Налаштування NAT для доступу до Інтернету

7. Налаштувати Load Balancing:

1) Перейти до Transmission → Load Balancing → Basic Settings.

2) Увімкнути Load Balancing globally.

3) Увімкнути Application Optimized Routing, щоб сесії одного застосунку не розривалися через хаотичне перемикання каналів.

4) Увімкнути Bandwidth Based Balancing Routing для WAN1 і WAN2.

5) Перевірити, що швидкості Upstream/Downstream для WAN1 і WAN2 внесені коректно.

6) Встановити WAN1 як Primary WAN, WAN2 як Backup WAN, якщо пріоритетом є резервування. Зберегти налаштування та виконати тест: тимчасово відключити WAN1 і перевірити, що вихід в Інтернет працює через WAN2.

8. Створити IP-групи для сегментів мережі:

1) Перейти до Preferences → IP Group → IP Address.

2) Створити записи для кожної підмережі: 10.10.10.0/24, 10.10.20.0/24, 10.10.30.0/24, 10.10.40.0/24, 10.10.50.0/24, 10.10.60.0/24.

3) Перейти до Preferences → IP Group → IP Group і створити групи NET_INFRASTRUCTURE, NET_MANAGEMENT, NET_FINANCE, NET_ENGINEERING_IT, NET_OPERATIONS, NET_WIRELESS.

4) Окремо створити записи для серверів S_1, S_2, S_3, щоб правила доступу були точними.

9. Налаштувати правила Firewall Access Control.

10. Налаштувати захист від атак.

11. Виконати резервне копіювання конфігурації:

1) Після успішного тестування перейти до System Tools → Management → Backup & Restore.

2) Натиснути Backup і зберегти файл конфігурації.

3) Розмістити копію конфігурації на сервері S_3 у захищеній папці, доступній лише адміністраторам [28].

3.1.2 Налаштування керованого комутатора D-Link DGS-1520-52

На рисунку 3.7 наведено схему підключення усіх пристроїв до керованого комутатора D-Link DGS-1520-52 рівня L3, який використовується як центральний комутаційний вузол проєктованої мережі. На рисунку показано розподіл портів між робочими станціями, мережевими принтерами, точкою доступу Wi-Fi, uplink-з’єднанням, а також серверами S_1, S_2 і S_3. Окремо виділено підключення серверів S_2 та S_3 до високошвидкісних 10G-портів, оскільки вони обслуговують бізнес-системи, бази даних, файлові ресурси та резервне копіювання.

Налаштування комутатора виконуватиметься через вебінтерфейс, що дозволяє зручно створювати VLAN, призначати порти в режимах Access або Trunk, налаштувати IP-інтерфейси VLAN, пересилання DHCP-запитів до сервера S_1 та зберегти конфігурацію в пам’яті пристрою.

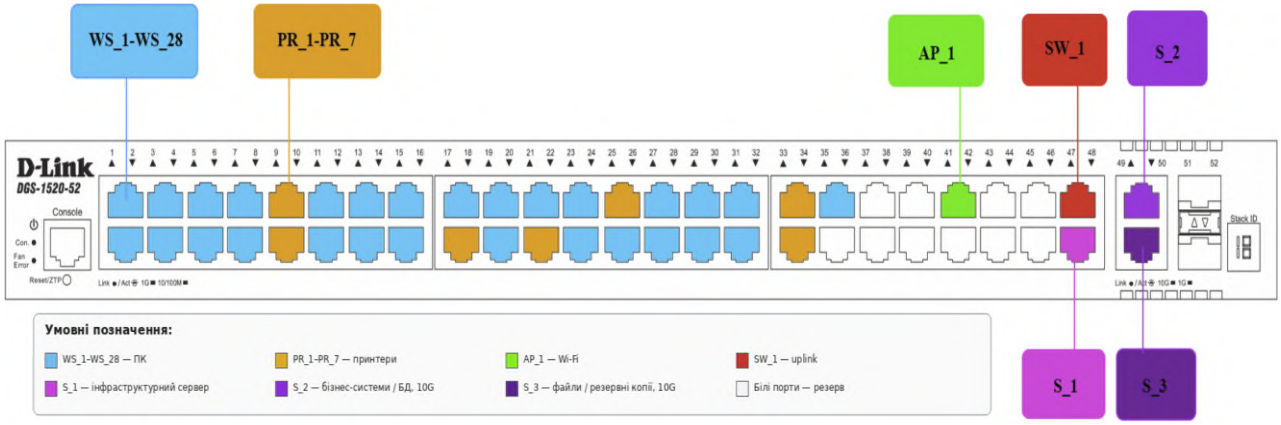

Рисунок 3.7 – Схема підключення пристроїв до комутатора

1. Підключити ПК адміністратора до LAN-порту комутатора. У браузері відкрити IP-адресу комутатора. За замовчуванням для DGS-1520 використовується адреса 10.90.90.90, логін і пароль — admin (див. рис. 3.8). Після входу потрібно змінити пароль адміністратора та виконати базове налаштування через Smart Wizard або вручну.

Рисунок 3.8 – Вікно авторизації на комутаторі

2. Налаштувати ім’я та інтерфейс керування комутатором:

Перейти до System > System Information Settings. Задати System Name, наприклад SW_1. Для інтерфейсу керування бажано вказати адресу з VLAN 10, наприклад 10.10.10.100/24, шлюз 10.10.10.1. Доступ до конфігурування SW_1 дозволити лише з VLAN 40 або VLAN 10 (див. рис. 3.9).

3. Перейти до System > Port Configuration > Port Settings. Для портів 1–48 залишити Auto Negotiation, для портів 49–50 перевірити роботу в режимі 10G.

4. Створити VLAN 802.1Q:

Перейти до L2 Features > VLAN > 802.1Q VLAN. Створити VLAN ID 10, 20, 30, 40, 50 і 60 та задати назву.

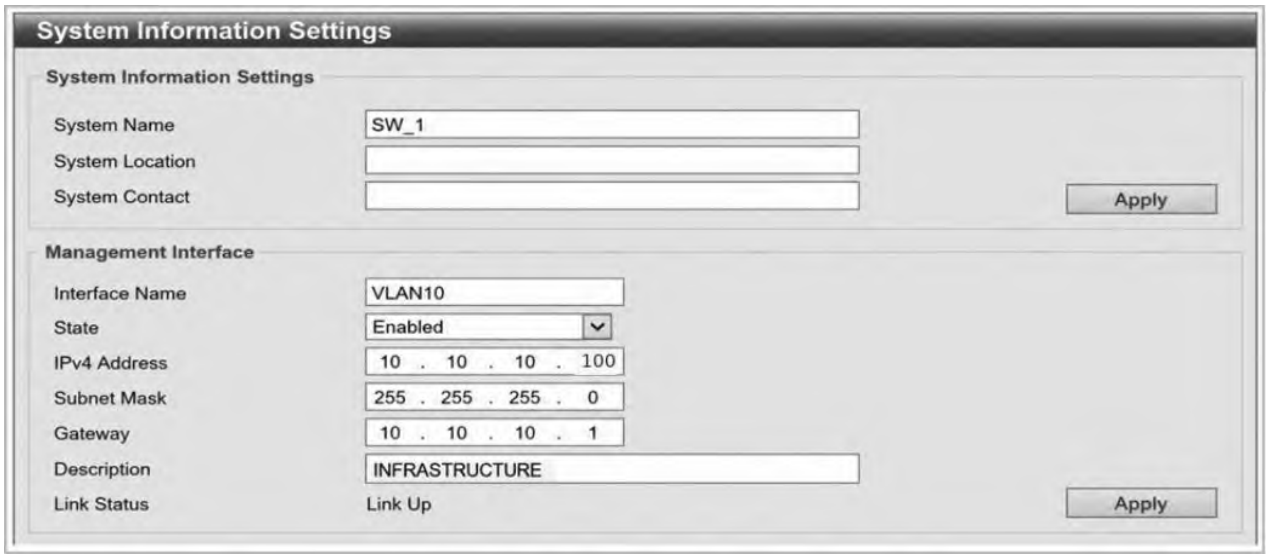

Рисунок 3.9 – Налаштування інтерфейсу керування SW_1

5. У розділі налаштування VLAN призначити порти. Порти робочих станцій і принтерів налаштовуються як access-порти в режимі UNTAG у VLAN відповідного підрозділу. Порт 47, який використовується як uplink/trunk, має пропускати VLAN 10, 20, 30, 40, 50 і 60 у режимі TAG. Порти 48, 49 і 50 для серверів S_1, S_2 і S_3 налаштувати як UNTAG VLAN 10 (див. рис. 3.10).

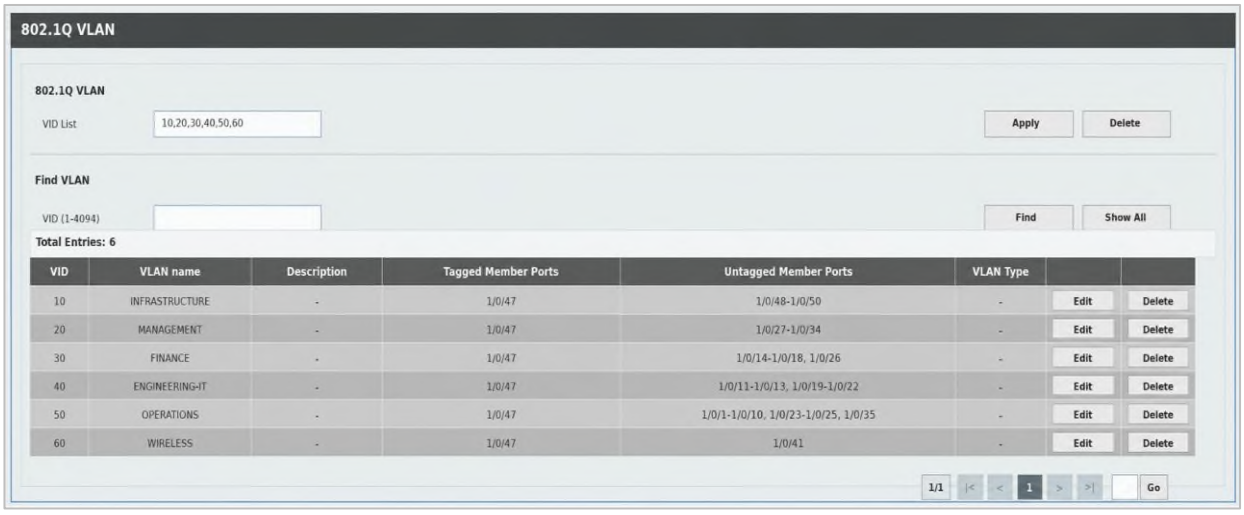

Рисунок 3.10 – Налаштування груп VLAN

6. Для кожного access-порту встановити PVID відповідно до його VLAN. Наприклад, для порту S_1 встановити PVID 10, для порту AP_1 при одному Wi-Fi сегменті — PVID 60, для портів бухгалтерії — PVID 30. Для trunk-порту 47 PVID обрати INFRASTRUCTURE VLAN.

7. Перейти до L3 Features > Interface > IPv4 Interface. Для кожної VLAN створити IPv4 interface: VLAN 10 — 10.10.10.1/24, VLAN 20 — 10.10.20.1/24, VLAN 30 — 10.10.30.1/24, VLAN 40 — 10.10.40.1/24, VLAN 50 — 10.10.50.1/24, VLAN 60 — 10.10.60.1/24. Ці адреси будуть шлюзами за замовчуванням для клієнтів відповідних сегментів (див. рис. 3.11).

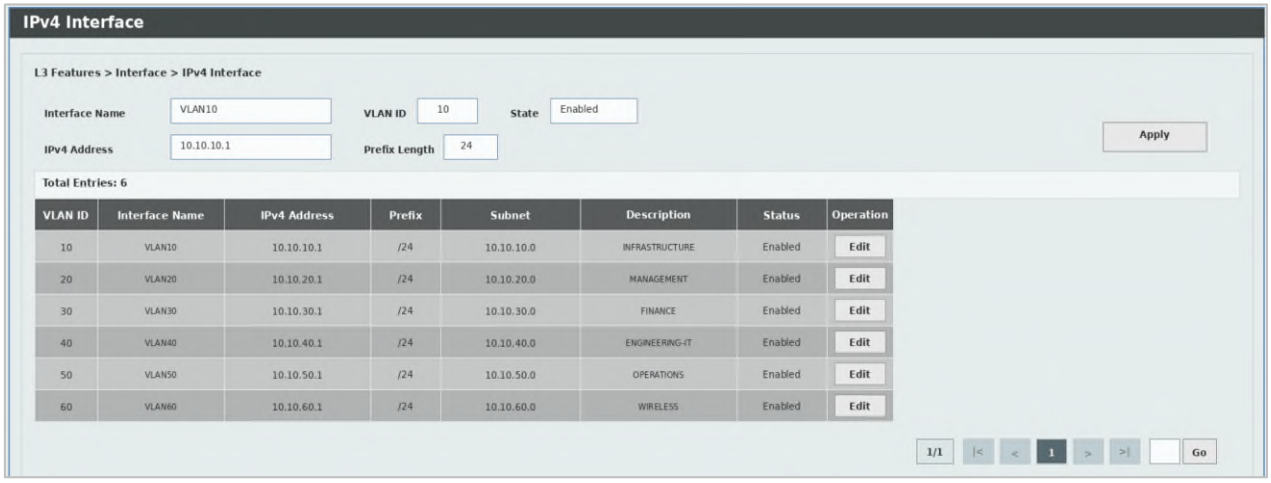

Рисунок 3.11 – Налаштування L3-інтерфейсів VLAN

8. Налаштувати IP Helper Address для DHCP:

Оскільки DHCP-сервером є S_1 з адресою 10.10.10.10, перейти до L3 Features > UDP Helper > IP Helper Address. Для VLAN 20, 30, 40, 50 і 60 додати Helper Address 10.10.10.10 (див. рис. 3.12).

9. Оскільки вихід до Інтернету виконується через FW_1, то для того щоб налаштуванти маршрут за замовчуванням необхідно перейти до L3 Features > IPv4 Static/Default Route. Створити default route 0.0.0.0/0 через фактичну адресу інтерфейсу FW_1 10.10.10.254 у VLAN 10. На FW_1 потрібно також налаштувати маршрути назад до підмереж 10.10.20.0/24–10.10.60.0/24 через L3-комутатор (див. рис. 3.13).

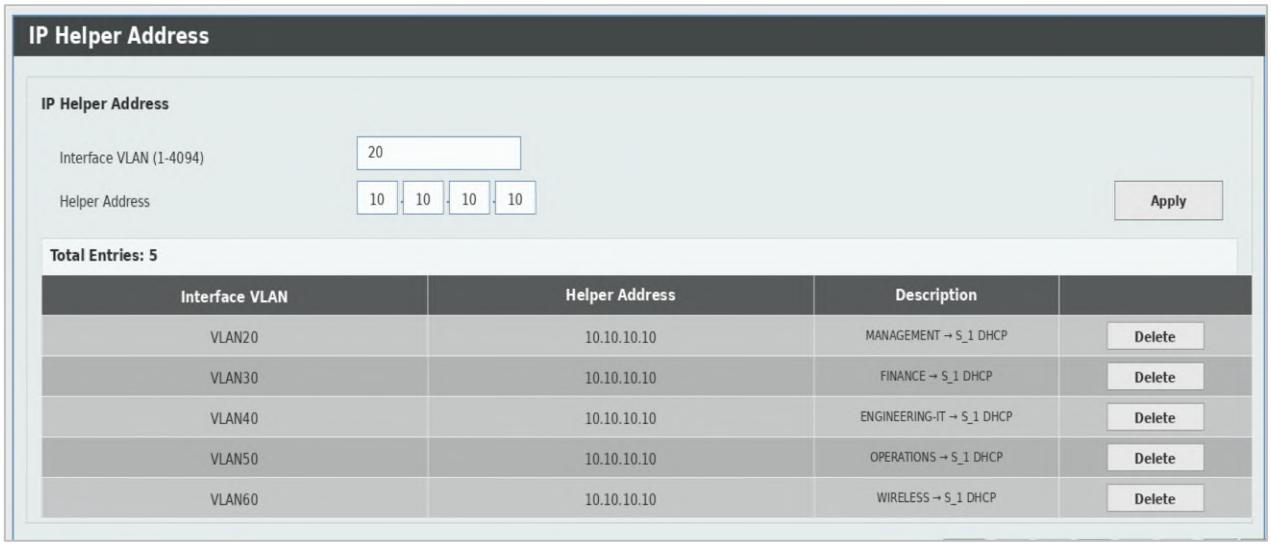

Рисунок 3.12 – Налаштування IP Helper Address для DHCP

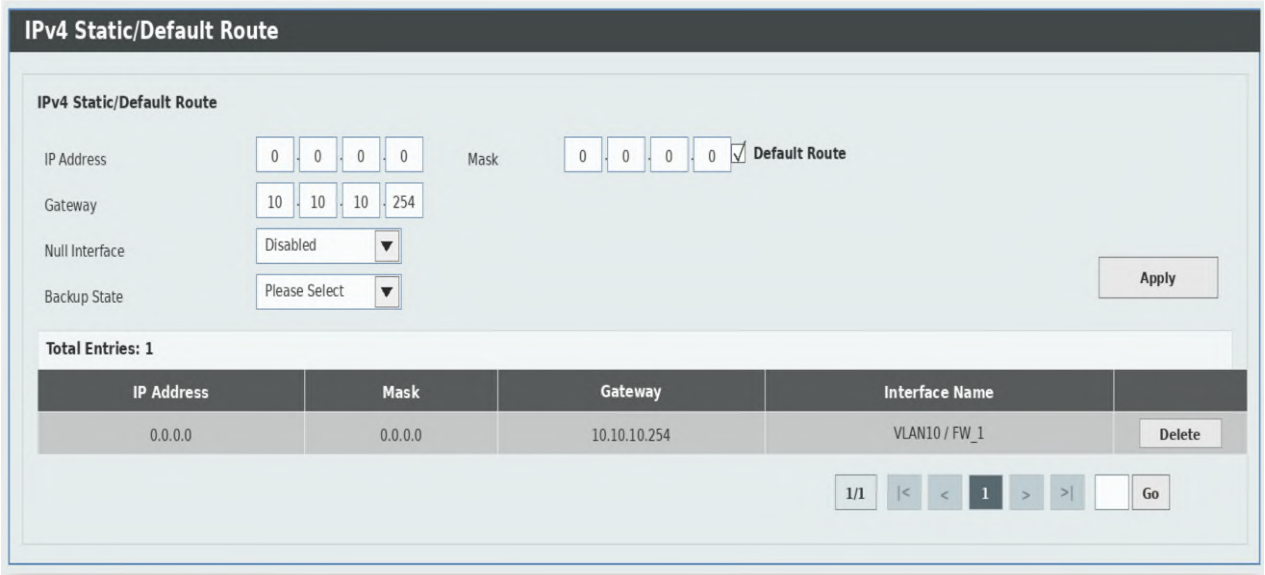

Рисунок 3.13 – Налаштування маршруту за замовчуванням

10. Для невикористаних портів 36–40, 42–46, 51–52 обрати стан Disabled або залишити їх без підключення. Для access-портів бажано ввімкнути базовий Port Security, Storm Control і BPDU Protection, щоб зменшити ризик петель, несанкціонованих підключень і широкомовних штормів.

11. Після успішної перевірки роботи комутатора натиснути Save у верхній панелі Web UI або перейти до Toolbar > Save > Save Configuration. Це потрібно для запису налаштувань у постійну пам’ять, інакше після перезавантаження комутатора зміни можуть бути втрачені [24].

3.1.3 Налаштування точки доступу TP-Link EAP653

На рисунку 3.14 наведено схему підключення точки доступу TP-Link EAP653 у проєктованій мережі. Точка доступу AP_1 під'єднується до комутатора SW_1 не напряму, а через PoE-інжектор, який одночасно передає мережевий трафік і забезпечує живлення пристрою. Такий варіант підключення обрано тому, що при проєктуванні КМ обирався комутатор без PoE, у зв'язку із підключенням лише одної точки доступу.

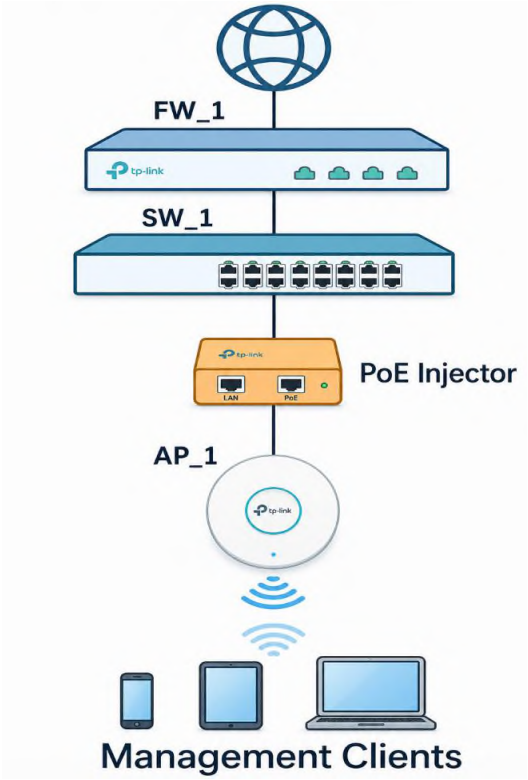

Рисунок 3.14 – Схема підключення точки доступу TP-Link EAP653

Налаштування TP-Link EAP653 виконуватиметься через вебінтерфейс. Через нього буде задано IP-адресу пристрою, параметри бездротової мережі, SSID, режим безпеки, VLAN для Wi-Fi-сегмента та параметри доступу для клієнтів. Це дозволить централізовано підготувати точку доступу до роботи в мережі та забезпечити підключення бездротових клієнтів відповідно до запроєктованої структури VLAN. Основним завданням налаштування є підготовка бездротового сегмента VLAN 60 WIRELESS, призначення

параметрів IP-адресації, створення захищеного SSID та обмеження адміністративного доступу до пристрою.

1. Підключити порт комутатора SW_1, призначений для AP_1, до LAN-входу PoE-інжектора. Вихід PoE інжектора підключити до Ethernet-порту точки доступу TP-Link EAP653. Перевірити індикацію живлення та наявність лінку.

2. Після підключення точка доступу може отримати динамічну IP-адресу від DHCP-сервера.

3. На комп'ютері адміністратора відкрити браузер і перейти за IP-адресою точки доступу або за адресою http://tplinkeap.net, якщо вона доступна в поточній мережі. Для першого входу використати стандартні облікові дані, після чого обов'язково створити новий обліковий запис адміністратора зі складним паролем (див. рис. 3.15). Стандартні логін і пароль залишати заборонено, оскільки це створює ризик несанкціонованого доступу до бездротової інфраструктури.

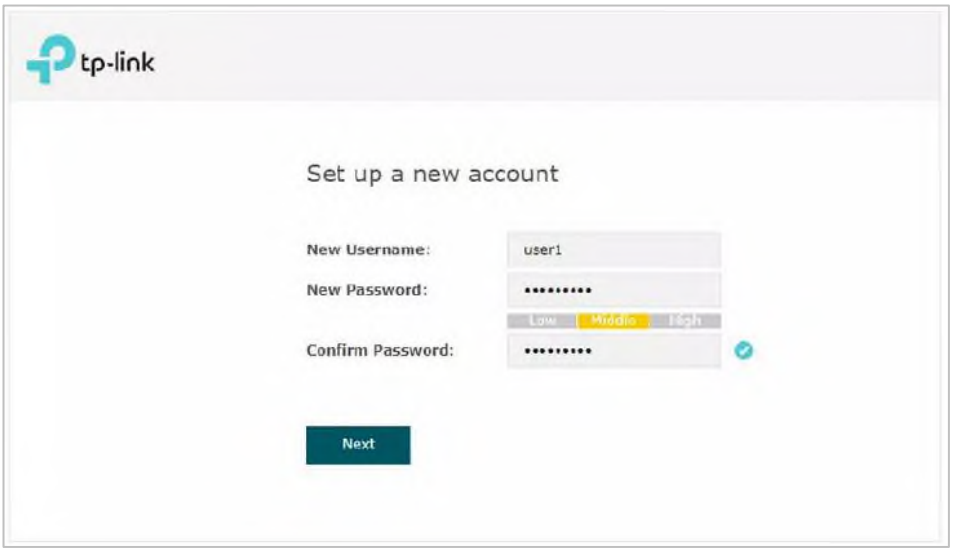

Рисунок 3.15 – Зміна паролю доступу

4. Налаштування IP-адреси точки доступу:

Перейти до Management > Network. Для стабільного адміністрування задати статичну адресу або створити DHCP-резервування. Для AP_1 доцільно використати адресу 10.10.60.2/24, шлюз 10.10.60.1 і DNS 10.10.10.10 (див. рис.

3.16). Якщо управління точкою планується з окремої адміністративної VLAN, потрібно забезпечити коректну маршрутизацію та правила доступу між VLAN.

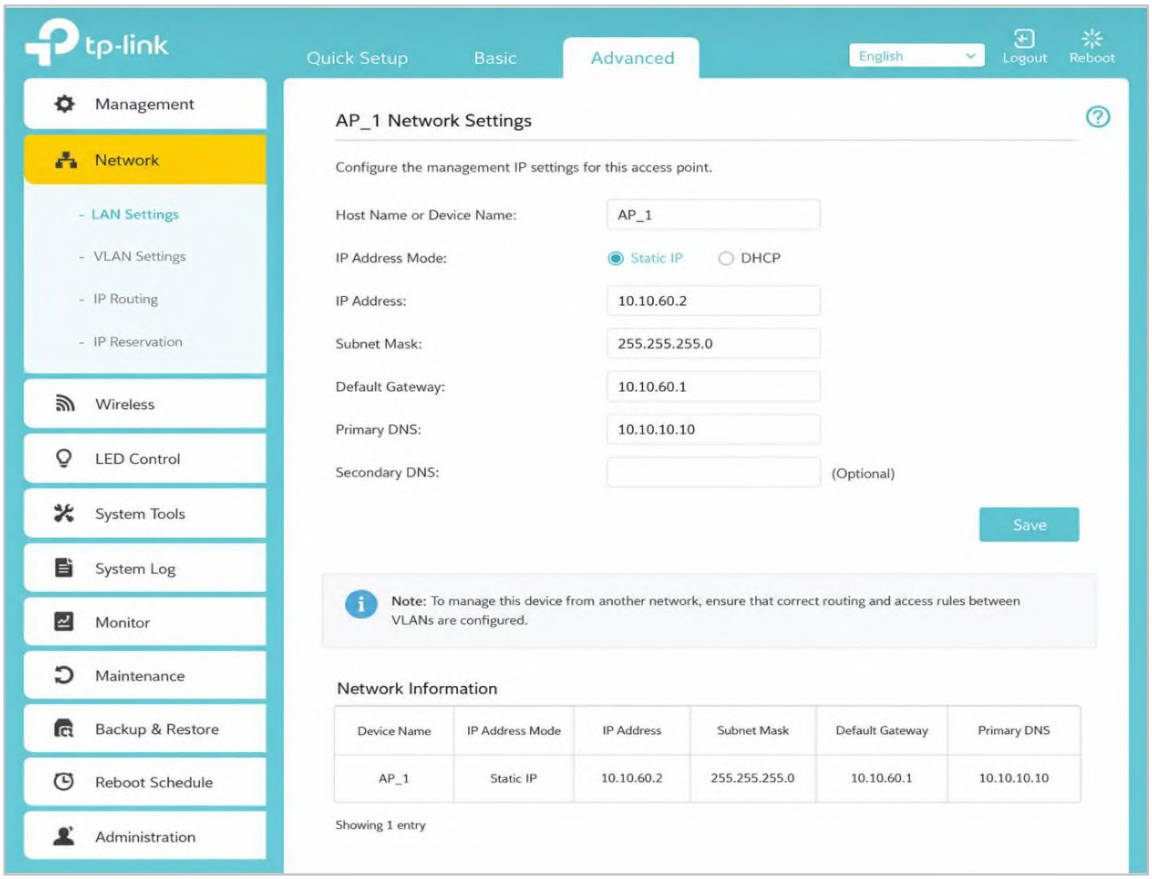

Рисунок 3.16 – Налаштування IP-адреси для AP_1

5. Перейти до Wireless > Wireless Settings. Для діапазонів 2.4 GHz і 5 GHz увімкнути Wireless Radio та створити корпоративний SSID, наприклад AVERS-WiFi (див. рис. 3.17). У параметрах безпеки вибрати WPA2/WPA3-Personal або WPA-Personal, задати складний пароль і зберегти налаштування. Для кращої сумісності можна налаштувати однаковий SSID для 2.4 GHz і 5 GHz. Перейти до Wireless > VLAN. Для створеного SSID увімкнути VLAN і вказати VLAN ID 60. Це забезпечить потрапляння трафіку бездротових клієнтів у сегмент 10.10.60.0/24 WIRELESS.

На комутаторі порт 1/0/41 має бути налаштований відповідно до обраної схеми: UNTAG VLAN 60 для одного SSID. Канал можна залишити Auto або задати вручну після аналізу завантаженості ефіру.

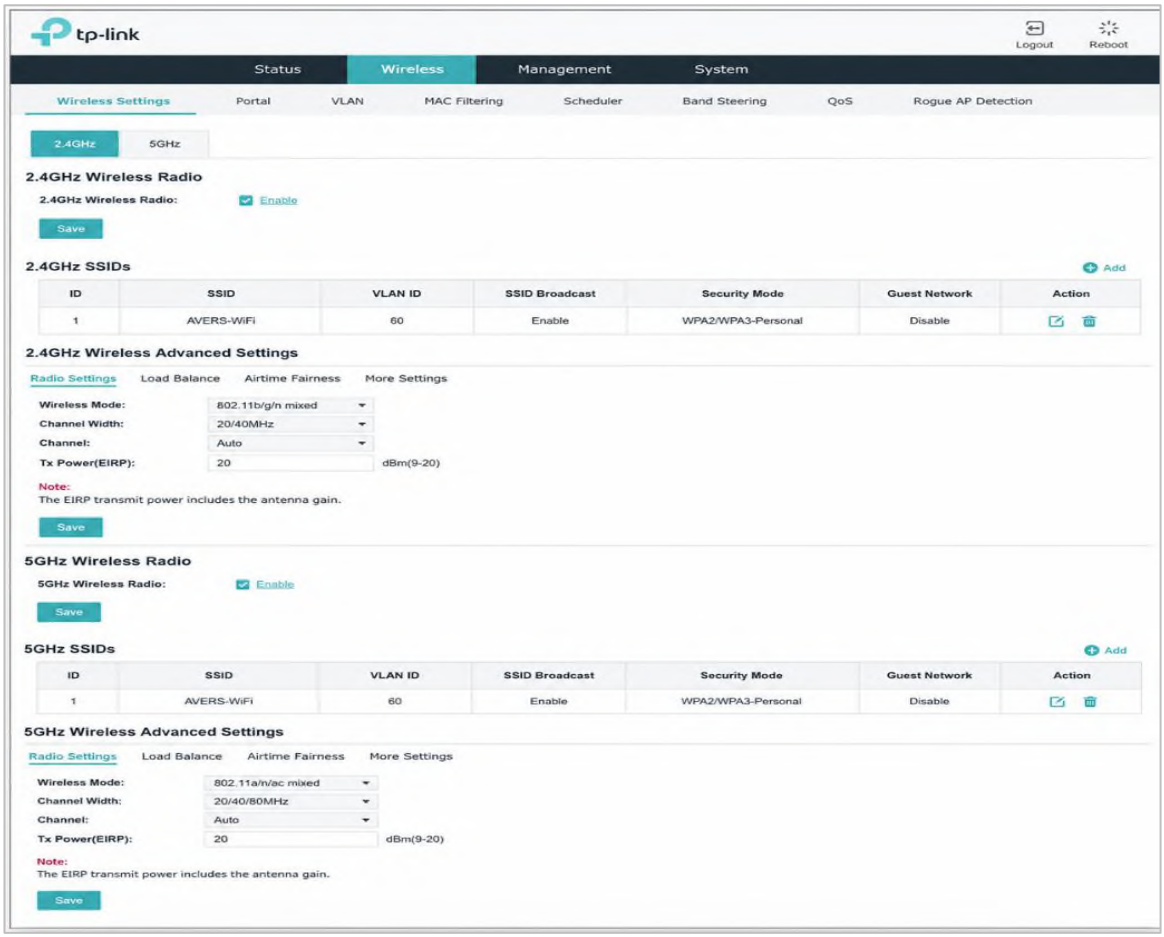

Рисунок 3.17 – Налаштування корпоративного SSID

6. Для безпечного адміністрування бажано дозволити доступ до вебінтерфейсу лише адміністраторам з VLAN 10 INFRASTRUCTURE або VLAN 40 ENGINEERING-IT.

7. Після успішної перевірки перейти до System > Backup and Restore та зберегти резервну копію конфігурації точки доступу. Файл конфігурації бажано зберігати на сервері S_3 у захищеній папці, доступній лише IT-адміністраторам [34].

3.1.4 Налаштування мережевих принтерів HP LaserJet Pro 3202dn

Для підключення мережевих принтерів HP Color LaserJet Pro 3202dn до проєктованої мережі необхідно використовувати дротове Ethernet-з’єднання через порт LAN.

1. Кожен принтер під’єднати патч-кордом Cat.6 до відповідного access-порту комутатора SW_1, який попередньо налаштований у потрібній VLAN згідно з розміщенням принтера у відділі.

Після фізичного підключення потрібно перевірити індикацію мережевого порту на принтері та комутаторі. На комутаторі для портів принтерів слід залишити режим Auto Negotiation, а сам порт має працювати як Access / UNTAG у VLAN відповідного підрозділу. Наприклад, принтери бухгалтерії підключаються до VLAN 30, адміністративні принтери — до VLAN 20, а принтери операційних підрозділів — до VLAN 50. Це дозволяє обмежити доступ до друку відповідно до логічної структури мережі підприємства.

2. IP-адресу принтера доцільно задавати не вручну на самому пристрої, а через DHCP-резервування на сервері S_1, який виконує роль DHCP-сервера. Для цього потрібно визначити MAC-адресу мережевого інтерфейсу принтера, створити для неї резервування у відповідній підмережі VLAN та призначити зрозумілу адресу, наприклад 10.10.50.21 для принтера операційного відділу або 10.10.30.21 для принтера бухгалтерії. Як шлюз використовується адреса відповідної VLAN, наприклад 10.10.50.1, а DNS-сервером — 10.10.10.10.

3. Після отримання IP-адреси потрібно відкрити веб-інтерфейс принтера через браузер, ввівши його IP-адресу, і перевірити основні параметри: назву пристрою, мережеву адресу, маску, шлюз, DNS та стан підключення. Вимкнути непотрібні служби, якщо вони не використовуються, та встановити пароль адміністратора для доступу до веб-інтерфейсу принтера.

4. На робочих ПК потрібно додати принтер за його IP-адресою. У Windows це виконується через Параметри → Bluetooth і пристрої → Принтери та сканери → Додати пристрій → Додати вручну → Додати принтер за TCP/IP-адресою. У полі адреси ввести IP-адресу принтера, після чого встановлюється драйвер HP Color LaserJet Pro 3202dn.

5. Після завершення налаштування необхідно надрукувати тестову сторінку з робочої станції користувача, перевірити доступність принтера командою ping, а також переконатися, що друк недоступний із тих VLAN, яким

доступ до відповідного принтера не передбачений політикою безпеки. Це забезпечить контрольований доступ до друку, зручне адміністрування та відповідність підключення принтерів загальній структурі мережі ТОВ «АВЕРС НК» [26].

3.2 Інструкція з інсталяції та налаштування серверів

3.2.1 Налаштування інфраструктурного сервера S_1

З урахуванням VLAN, сервер S_1 виконує центральну роль у мережі ТОВ «АВЕРС НК». Він забезпечує доменну авторизацію, роботу DNS, централізовану видачу IP-адрес у шести логічних сегментах, застосування групових політик і аудит безпеки. Використання підмереж 10.10.X.0/24 робить структуру адресації зрозумілою, а розділення на VLAN 10, 20, 30, 40, 50 і 60 дозволяє ізолювати критичні ресурси, захистити фінансові дані, впорядкувати доступ операційних підрозділів і обмежити бездротовий сегмент.

1. Виконати базову підготовку ОС Windows Server 2022:

1) Встановити Windows Server 2022 Standard.

2) Встановити для сервера ім’я S_1.

3) Встановити рекомендовані параметри мережевого адаптера сервера S_1 в інфраструктурній VLAN 10: IP-адреса 10.10.10.10, маска 255.255.255.0, шлюз 10.10.10.1, DNS-сервер 10.10.10.10. Використання статичної адреси є обов’язковим, оскільки сервер S_1 буде контролером домену, DNS і DHCP-сервером.

2. Обрати ролі для служб домену:

1) Відкрити Server Manager.

2) Перейти до Manage -> Add Roles and Features.

3) Натиснути Role-based or feature-based installation.

4) У правій панелі вибрати сервер S_1 і натиснути Next (Далі).

5) У розділі Roles - Active Directory Domain - Performance this server to Domain Controller натиснути Install a new forest, вказавши aversnk.local та встановивши пароль DSRM. Після перезавантаження S_1 стане основним контролером домену мережі підприємства.

3. Створити структуру Active Directory:

У консолі Active Directory Users and Computers необхідно створити організаційні одиниці, які відповідають логічній структурі підприємства та VLAN: OU_INFRASTRUCTURE; OU_MANAGEMENT; OU_FINANCE; OU_ENGINEERING_IT; OU_OPERATIONS та OU_WIRELESS. Це дозволить зручно застосовувати групові політики й права доступу до користувачів різних підрозділів. У кожній OU створюються користувачі та групи безпеки, наприклад GRP_FINANCE, GRP_OPERATIONS, GRP_MANAGEMENT, GRP_ENGINEERING_IT та GRP_IT_ADMINS. Права доступу до файлових ресурсів і бізнес-систем доцільно призначати саме групам, а не окремим користувачам. Це спрощує адміністрування при прийнятті, переведенні або звільненні працівників.

4. Сконфігурувати служби DNS:

В DNS Manager необхідно переконатися в коректній роботі прямої зони перегляду aversnk.local, після чого сформувати відповідні зони зворотного перегляду (Reverse Lookup Zones) для полегшення процесів моніторингу та адміністрування мережі. Зворотні зони розподіляються за такими підмережами та призначеннями: 10.10.10.0/24 — для сегмента INFRASTRUCTURE; 10.10.20.0/24 — для сегмента MANAGEMENT; 10.10.30.0/24 — для сегмента FINANCE; 10.10.40.0/24 — для сегмента ENGINEERING-IT; 10.10.50.0/24 — для сегмента OPERATIONS; 10.10.60.0/24 — для сегмента WIRELESS.

Паралельно з цим потрібно задати перенаправлювачі запитів (DNS Forwarders), вказавши IP-адреси DNS-серверів інтернет-провайдерів або стабільних публічних служб глобальної мережі, що дозволить комп'ютерам у домені безперешкодно відкривати зовнішні інтернет-ресурси.

5. Провести інсталяцію та авторизацію сервера DHCP:

1) У Server Manager відкрити Add Roles and Features.

2) Вибрати роль DHCP Server.

3) Завершити інсталяцію ролі.

4) Виконати налаштування Complete DHCP configuration.

5) Авторизувати DHCP-сервер у Active Directory.

6) Відкрити DHCP Manager і переконатися, що сервер має активний стан.

Авторизація DHCP-сервера в домені потрібна для запобігання роботі несанкціонованих DHCP-серверів. Після авторизації створюються окремі DHCP-діапазони, як показано у таблиці 3.1 для кожної VLAN.

Для кожної VLAN створюється окремий IPv4 Scope. У кожному діапазоні задаються параметри маршрутизатора, DNS-сервера та доменного імені. Для відповідних Scope встановити DHCP Option 003 Router зі відповідним шлюзом, Option 006 DNS Servers із адресою 10.10.10.10 та Option 015 DNS Domain Name зі значенням aversnk.local.

Для VLAN 10 рекомендовано для пристроїв призначати адреси статично: S_1 — 10.10.10.10, S_2 — 10.10.10.20, S_3 — 10.10.10.30, комутатор — 10.10.10.2, міжмережевий екран — 10.10.10.1.

Таблиця 3.1 - DHCP-діапазони для VLAN

Vlan	Назва Scope	Підмережа	Діапазон видачі	Шлюз	DNS / Домен
10	INFRA-STRUCTURE	10.10.10.0 /24	10.10.10.50-10.10.10.200	10.10.10.1	10.10.10.10 /aversnk.local
20	MANAGEMENT	10.10.20.0 /24	10.10.20.50-10.10.20.60	10.10.20.1	10.10.10.10 /aversnk.local
30	FINANCE	10.10.30.0 /24	10.10.30.50-10.10.30.60	10.10.30.1	10.10.10.10 /aversnk.local
40	ENGINEERING-IT	10.10.40.0 /24	10.10.40.50-10.10.40.60	10.10.40.1	10.10.10.10 /aversnk.local
50	OPERATIONS	10.10.50.0 /24	10.10.50.50-10.10.50.70	10.10.50.1	10.10.10.10 /aversnk.local
60	WIRELESS	10.10.60.0 /24	10.10.60.50-10.10.60.100	10.10.60.1	10.10.10.10 /aversnk.local

6. DHCP Relay на маршрутизаторі або L3-комутаторі:

Оскільки DHCP-сервер S_1 розміщений у VLAN 10, а клієнти знаходяться в інших VLAN, на маршрутизаторі або L3-комутаторі потрібно налаштувати DHCP Relay / IP Helper Address. Для кожного VLAN-інтерфейсу вказується адреса DHCP-сервера 10.10.10.10. Без цього клієнти з VLAN 20-60 не зможуть отримувати IP-адреси автоматично.

7. Налаштувати групові політики:

У Group Policy Management створюються політики, які відповідають підрозділам і рівням доступу. Політики прив’язуються до відповідних OU, що дозволяє централізовано керувати параметрами безпеки, доступом до ресурсів, оновленнями та обмеженнями робочих станцій.

8. Встановити правила доступу між VLAN:

На S_1 створюються облікові записи та групи доступу, однак обмеження між групами VLAN реалізуються на міжмережевому екрані або L3-комутаторі. Рекомендована політика: за замовчуванням заборонити прямий доступ між користувацькими VLAN і дозволити лише потрібні сервіси до конкретних серверів. Наприклад, користувачі VLAN FINANCE повинні мати доступ до фінансових папок і бухгалтерських систем, але не повинні мати прямого доступу до логістичних баз без службової потреби. Користувачі VLAN OPERATIONS повинні мати доступ до CRM, ERP, WMS/TMS і баз перевезень, але не до банківських або зарплатних даних бухгалтерії.

9. Налаштувати Windows Defender Firewall, Defender Antivirus і журналювання:

У Event Viewer потрібно контролювати журнали Security, Directory Service, DNS Server, DHCP Server, System та Group Policy. Для мережі ТОВ «АВЕРС НК» доцільно ввімкнути аудит успішних і невдалих входів, змін груп безпеки, змін облікових записів, помилок DNS/DHCP та проблем застосування групових політик.

10. Підключити робочі станції до домену:

1) Підключити кожну робочу станцію та мережевий принтер до відповідного VLAN-порту згідно таблиці 2.2.

2) Перевірити, що клієнт отримав IP-адресу з правильної підмережі 10.10.X.0/24.

3) Переконатися, що DNS-сервером указано 10.10.10.10.

4) Підключити ПК Windows 11 Pro до домену aversnk.local.

5) Перезавантажити ПК і увійти під доменним користувачем.

6) Виконати gpupdate /force та gpresult /r для перевірки застосування політик.

11. Виконати резервне копіювання конфігурації S_1. Резервні копії доцільно зберігати на сервері S_3, який виконує роль файлового й резервного сервера [29; 31].

3.2.2 Налаштування сервера прикладних систем логістики та баз даних S_2

Сервер S_2 призначений для розміщення прикладних бізнес-систем і баз даних підприємства: CRM, ERP, WMS/TMS, систем обліку заявок, маршрутів, клієнтської бази, складських операцій та взаємодії диспетчерів із відділом логістики. Винесення цих сервісів на окремий сервер підвищує продуктивність мережі, оскільки навантаження від бізнес-додатків не впливає на інфраструктурні служби S_1 та файлово-резервний сервер S_3.

1. Встановити Windows Server 2022 Standard:

Встановити Windows Server 2022 Standard на фізичний або віртуальний сервер. Під час встановлення обрати редакцію з Desktop Experience, якщо адміністрування планується через графічний інтерфейс. Після першого входу встановити оновлення безпеки через Windows Update, задати часовий пояс, перевірити коректність дати й часу, оскільки помилки часу можуть призводити до проблем автентифікації в домені.

2. Налаштувати імені сервера та статичну IP-адресу:

У Server Manager змінити ім’я сервера на S_2. У властивостях мережевого адаптера встановити статичну IP-адресу 10.10.10.20/24, шлюз 10.10.10.1 і DNS 10.10.10.10. DNS має вказувати на S_1, оскільки саме він виконує роль контролера домену та DNS-сервера.

3. Приєднати сервер до домену:

Приєднати S_2 до домену aversnk.local. Після перезавантаження перевірити, що сервер з’явився в Active Directory у відповідній OU, наприклад OU_INFRASTRUCTURE. Для адміністрування використовувати доменні облікові записи IT-групи, а не локальні облікові записи.

4. Підготувати дискову структуру:

Для стабільності й зручності обслуговування розділити дані за призначенням: диск C: для ОС, D: для бізнес-додатків, E: для баз даних, F: для журналів баз даних і тимчасових файлів. Такий поділ спрощує резервне копіювання, контроль продуктивності та відновлення після збоїв.

5. Створити службові облікові записи у домені:

На сервері S_1 в Active Directory створити службові облікові записи, наприклад svc_sql_s2, svc_pgsql_s2, svc_crm_app, svc_erp_app. Для них задати складні паролі, заборонити інтерактивний вхід і надати лише мінімально необхідні права. Це відповідає принципу найменших привілеїв.

6. Вибрати СКБД Microsoft SQL Server або PostgreSQL:

Якщо обрана CRM/ERP/WMS/TMS-система потребує Microsoft SQL Server, встановити SQL Server Database Engine та SQL Server Management Studio. Якщо прикладне ПЗ використовує відкриту СКБД, встановити PostgreSQL і pgAdmin.

7. Встановити бізнес-додатки CRM/ERP/WMS/TMS:

Встановити серверну частину бізнес-системи на диск D:. Під час інсталяції вказати адресу бази даних localhost або 10.10.10.20, створену базу даних і службовий обліковий запис. Для логістичної компанії основними

модулями є заявки, маршрути, клієнти, складські операції, диспетчеризація, постачання, звітність і аналітика.

8. Налаштувати веб-доступ через IIS:

Якщо бізнес-система має веб-інтерфейс, встановити роль Web Server (IIS), необхідні ASP.NET-компоненти та створити сайт або веб-додаток. Для внутрішнього доступу бажано використовувати DNS-ім’я, наприклад crm.aversnk.local або erp.aversnk.local, і сертифікат для HTTPS.

9. Налаштувати доступ користувачів через AD-групи:

Створити групи GRP_APP_CRM_USERS, GRP_APP_ERP_USERS, GRP_APP_WMS_USERS, GRP_APP_TMS_USERS, GRP_DB_ADMINS. Доступ до додатків і баз даних призначати не окремим користувачам, а групам. Для VLAN 50 OPERATIONS надати основний доступ до логістичних систем, для VLAN 30 FINANCE - тільки до фінансових модулів, для VLAN 60 WIRELESS доступ до бізнес-систем не надавати.

10. Налаштувати параметри захисту.

11. Налаштувати резервне копіювання баз даних і конфігурації додатків на сервер S_3. Для SQL Server використовувати план обслуговування або засоби резервування, для PostgreSQL - pg_dump/pg_basebackup або інструменти резервного копіювання. Обов’язково виконати тестове відновлення бази даних.

12. Увімкнути журналювання подій Windows Event Viewer, SQL Server Logs або PostgreSQL Logs, а також журнали бізнес-додатків. Контролювати помилки автентифікації, нестачу дискового простору, повільні запити, збої служб і невдалі спроби підключення.

13. Перевірити працездатність S_2 [29; 31].

3.2.3 Налаштування файлового та резервного сервера S_3

Сервер S_3 призначений для централізованого зберігання службових документів, організації розмежованого доступу до папок підрозділів та виконання резервного копіювання критично важливих даних.

1. Після встановлення Windows Server 2022 потрібно змінити ім’я сервера на S_3, встановити статичну IP-адресу з підмережі VLAN 10 INFRASTRUCTURE 10.10.10.30/24 та вказати DNS-сервером адресу інфраструктурного сервера S_1: 10.10.10.10. Далі необхідно встановити всі актуальні оновлення Windows Update, перевірити доступність шлюзу командою ping 10.10.10.1 і перевірити коректність DNS командою nslookup aversnk.local.

2. Приєднати S_3 до домену aversnk.local

Сервер S_3 необхідно приєднати до домену aversnk.local. Для цього у властивостях системи обирають зміну домену, вводять ім’я домену aversnk.local і облікові дані адміністратора домену. Після перезавантаження сервер має відображатися в Active Directory у відповідній організаційній одиниці, наприклад OU_ INFRASTRUCTURE. Це дає змогу застосовувати до нього групові політики, централізовано керувати правами доступу та використовувати доменні групи для NTFS-дозволів.

3. Підготувати дискову підсистему:

Перед створенням файлових ресурсів необхідно розділити дисковий простір на логічні томи. Рекомендовано використовувати окремий системний диск C: для операційної системи, окремий том D: для файлових ресурсів і окремий том E: або зовнішнє/мережеве сховище для резервних копій. Для файлового тому варто використовувати NTFS, оскільки він підтримує списки контролю доступу, шифрування, квоти, розширені атрибути та інші механізми керування даними. Для підвищення надійності бажано застосувати RAID-масив або Storage Spaces, щоб відмова одного диска не призводила до втрати документів.

4. Через Server Manager відкрити Manage → Add Roles and Features, вибрати Role-based or feature-based installation, обрати сервер S_3 і встановити роль File and Storage Services → File and iSCSI Services → File Server. Після встановлення роль дозволить створювати спільні папки, керувати сховищем, правами доступу та файловими ресурсами підприємства. Цей сервер буде

основним місцем зберігання договорів, актів, накладних, маршрутів, звітів, бухгалтерських документів і службової документації.

5. На файловому томі D: потрібно створити базову структуру папок відповідно до організаційної структури ТОВ «АВЕРС НК». Наприклад: D:\Shares\Finance, D:\Shares\Management, D:\Shares\Operations, D:\Shares\Engineering_IT, D:\Shares\Marketing, D:\Shares\Legal, D:\Shares\Common, D:\Shares\Archive. Така структура забезпечить логічне розділення документів за підрозділами та спростить адміністрування доступу.

6. Створити доменні групи доступу:

На сервері S_1 створити доменні групи доступу, які будуть використовуватись для керування дозволами на S_3. Рекомендовано створювати окремі групи для читання та зміни: GRP_FINANCE_RW, GRP_FINANCE_RO, GRP_OPERATIONS_RW, GRP_MANAGEMENT_RW, GRP_LEGAL_RW, GRP_MARKETING_RW, GRP_ENGINEERING_IT_RW, GRP_COMMON_RW. Працівників додають до відповідних груп залежно від їхнього підрозділу та посадових обов’язків. Така модель є зручнішою, ніж призначення дозволів кожному користувачу окремо.

7. Для кожної папки потрібно налаштувати NTFS-дозволи через вкладку Security. Адміністратори домену отримують Full Control, відповідна група підрозділу отримує Modify або Read, а доступ для зайвих груп видаляється. Наприклад, до папки Finance повний доступ мають Domain Admins і GRP_FINANCE_RW, право читання може мати керівництво через GRP_MANAGEMENT_RO, а користувачі з Operations або Marketing доступу не отримують. Для службової папки Common можна надати ширший доступ, але без права видалення критичних документів. Такий підхід реалізує принцип найменших привілеїв. Після налаштування NTFS-дозволів папки публікуються як спільні ресурси. У клієнтських ПК ресурси можна підключати як мережеві диски за допомогою Group Policy Preferences відповідно до OU або груп Active Directory.

8. Для запобігання неконтрольованому заповненню дисків бажано встановити роль File Server Resource Manager. За її допомогою можна задати квоти для папок підрозділів, наприклад 200 ГБ для Finance, 300 ГБ для Operations, 100 ГБ для Legal, а також налаштувати повідомлення адміністратора при досягненні 85–90% використання. Додатково можна обмежити зберігання небажаних типів файлів, наприклад відео, музики або інсталяційних архівів у службових папках.

9. Для файлового тому D: варто увімкнути Shadow Copies. Це дозволить швидко відновлювати попередні версії документів у разі випадкового видалення або неправильного редагування. Рекомендовано налаштувати створення копій кілька разів на день, наприклад о 08:00, 12:00 і 17:00, та виділити окремий обсяг дискового простору для зберігання попередніх версій. Shadow Copies не замінюють повноцінне резервне копіювання, але значно спрощують відновлення окремих файлів.

10. Встановити Windows Server Backup:

Для базового резервного копіювання потрібно встановити компонент Windows Server Backup через Add Roles and Features → Features → Windows Server Backup. Після встановлення в Server Manager з’явиться відповідна консоль. Windows Server Backup дозволяє виконувати резервне копіювання томів, окремих папок, файлів і системного стану, а також відновлювати дані після збою.

11. Налаштувати розклад резервного копіювання:

У Windows Server Backup потрібно створити Backup Schedule. Для S_3 рекомендовано щоденне резервне копіювання службових папок і системного стану, а також щотижневе повне резервне копіювання файлового тому. Місцем зберігання копій може бути окремий диск, NAS або резервний репозиторій, бажано ізольований від звичайних користувачів.

12. Налаштувати параметри захисту.

13. Налаштувати журналювання та аудит.

14. На робочих станціях Windows 11 Pro мережеві диски бажано підключати централізовано через Group Policy Preferences. Наприклад, користувачам з GRP_FINANCE_RW автоматично підключається диск F: до \S_3\Finance, працівникам логістики — диск O: до \S_3\Operations, керівництву — диск M: до \S_3\Management, а всім працівникам — диск P: до \S_3\Common. Це зменшує кількість ручних налаштувань і забезпечує однакову структуру доступу для всіх користувачів.

15. Перевірити працездатність S_3 [29; 31].

3.3 Інструкції з використання тестових наборів та тестових програм

Після завершення налаштування основних компонентів мережі ТОВ «АВЕРС НК» необхідно виконати перевірку правильності роботи впроваджених засобів захисту, міжмережевої взаємодії та доступу користувачів до корпоративних ресурсів. Оскільки мережа поділена на окремі VLAN, особливу увагу потрібно приділити тестуванню правил доступу між цими сегментами.

Використання тестових наборів і програм дозволяє виявити помилки конфігурації, перевірити доступність критичних сервісів, підтвердити ефективність правил безпеки та переконатися, що мережа працює відповідно до спроєктованої логічної структури. Результати такого тестування є підставою для подальшого введення мережі в експлуатацію та підтверджують її готовність до безпечної роботи в умовах логістичної компанії.

Тестування має підтвердити, що міжмережевий екран TP-Link Omada ER7406 коректно фільтрує трафік між VLAN, дозволяє лише необхідні службові з’єднання та блокує небажаний міжсегментний доступ. Окремо перевіряється робота захисту від атак, коректність DNS- і DHCP-запитів до сервера S_1, доступ користувачів до бізнес-систем на S_2, файлових ресурсів на S_3, а також ізоляція бездротової мережі VLAN 60 від внутрішніх корпоративних сегментів.

1. Підключити до порту кожної VLAN на комутаторі тестовий ПК. Перевірити отримання IP-адреси від S_1, шлюз 10.10.X.1, доступ до DNS, доступ до потрібних серверів і заборону доступу до ізольованих сегментів [24].

2. З робочої станції VLAN 50 перевірити отримання IP-адреси з діапазону 10.10.50.0/24, доступ до шлюзу 10.10.50.1, доступ до S_2 та вихід в Інтернет.

3. З робочої станції VLAN 30 перевірити доступ до фінансових ресурсів, S_3 та відсутність доступу до логістичних сегментів, якщо це заборонено політикою.

4. З Wi Fi-клієнта VLAN 60 перевірити доступ до Інтернету та відсутність доступу до S_1, S_2, S_3 і внутрішніх VLAN.

5. Вимкнути WAN1 і перевірити, що Інтернет працює через WAN2. Потім відновити WAN1 і перевірити повернення трафіку.

6. Виконати діагностику ping, nslookup, tracert і переглянути журнали FW_1.

На клієнтських ПК Windows після підключення до відповідної VLAN виконати такі команди:

```
ipconfig /all
nslookup aversnk.local
ping 10.10.10.10
ping 10.10.50.1
tracert 8.8.8.8
```

Очікуваний результат: клієнт отримує адресу зі своєї VLAN, бачить власний шлюз, отримує DNS-відповідь від S_1, має доступ лише до дозволених серверів та виходить в Інтернет через один із WAN-каналів [28].

Крім мережевого рівня, необхідно протестувати захист серверів і точки доступу. Для серверів S_1, S_2 і S_3 перевіряється робота Windows Defender Firewall, Microsoft Defender Antivirus, дозволених портів, правил віддаленого адміністрування та журналювання подій.

1. Перевірити працездатність S_1:

Після завершення налаштування потрібно перевірити всі основні служби. На клієнтах і сервері виконуються команди ipconfig /all, nslookup aversnk.local, ping S_1, gpupdate /force, gpresult /r та dcdiag. Очікуваний результат: клієнти отримують IP-адреси зі своїх VLAN, DNS коректно розпізнає доменні імена, користувачі входять у домен, групові політики застосовуються до потрібних OU, а доступ між VLAN відповідає політиці безпеки.

2. Перевірити працездатність S_2:

Перевірити доступ до бізнес-систем із VLAN 50 OPERATIONS, обмежений доступ із VLAN 30 FINANCE та відсутність доступу з VLAN 60 WIRELESS. Перевірити вхід користувача через доменний обліковий запис, відкриття CRM/ERP/WMS/TMS, створення тестової заявки, запис у базу даних, резервне копіювання та тестове відновлення/

3. Перевірити працездатність S_3:

Після налаштування потрібно перевірити доступність сервера командою ping 10.10.10.30, коректність імені nslookup S_3.aversnk.local, доступ до ресурсів \S_3\Common, \S_3\Finance та інших папок. Окремо перевіряється, що користувачі бухгалтерії мають доступ до фінансових документів, але не мають доступу до папок інших підрозділів, а працівники Operations мають доступ лише до ресурсів логістики та загальних папок. Також потрібно виконати тестове резервне копіювання і тестове відновлення одного документа [29; 31].

Для точки доступу TP-Link EAP653 перевіряється коректність роботи SSID AVERS-WiFi, застосування режиму захисту WPA-Personal або WPA2/WPA3-Personal, використання складного пароля та прив’язка бездротових клієнтів до відповідного VLAN.

1. Підключити тестовий ноутбук або смартфон до SSID AVERS-WiFi. Перевірити отримання IP-адреси з підмережі 10.10.60.0/24, доступ до шлюзу 10.10.60.1, DNS-розв’язання і вихід в Інтернет. Також потрібно переконатися, що клієнти Wi-Fi не мають доступу до внутрішніх серверних ресурсів, якщо це заборонено політикою міжмережевого екрана [34].

3.4 Інструкція по налаштуванню засобів захисту мережі

Після налаштування основних мережевих служб, VLAN-сегментації, серверної інфраструктури, комутатора та точки доступу необхідно перейти до впровадження засобів захисту мережі. Для мережі ТОВ «АВЕРС НК» це особливо важливо, оскільки різні підрозділи підприємства працюють з інформацією різного рівня критичності: бухгалтерія — з фінансовими документами, логістичний відділ — з базами перевезень і замовленнями, адміністрація — з управлінською документацією, а IT-підрозділ — з обладнанням та серверними ресурсами.

Основою захисту мережі є правильне налаштування міжмережевого екрана TP-Link Omada ER7406, який контролює обмін трафіком між VLAN, обмежує небажаний міжсегментний доступ і дозволяє лише ті з'єднання, які необхідні для роботи корпоративних служб.

1. Налаштувати правила Firewall Access Control:

1) Перейти до Firewall → Access Control → Access Control.

2) Створювати правила зверху вниз: спочатку дозволити необхідний трафік, потім заборонити зайвий міжсегментний доступ.

3) Дозволити VLAN 40 ENGINEERING-IT адмініструвати FW_1 та сервери S_1, S_2, S_3 за HTTPS/RDP/ICMP.

4) Дозволити всім службовим VLAN звернення до S_1 за DNS і DHCP Relay.

5) Дозволити VLAN 50 OPERATIONS доступ до S_2 за портами бізнес-додатків і баз даних.

6) Дозволити VLAN 30 FINANCE доступ лише до фінансових ресурсів на S_2 і файлових папок на S_3.

7) Дозволити VLAN 20 MANAGEMENT доступ до управлінських ресурсів і необхідних сервісів.

8) Заборонити VLAN 60 WIRELESS доступ до всіх внутрішніх VLAN, залишивши тільки DNS, HTTP та HTTPS у напрямку Інтернету.

9) Наприкінці створити завершальне правило Deny для небажаного LAN-to-LAN трафіку.

2. Налаштувати захист від атак:

1) Перейти до Firewall → Attack Defense.

2) Увімкнути базові механізми захисту від DoS-атак, сканування портів і підозрілих пакетів.

3) Перейти до Firewall → Anti ARP Spoofing та за потреби створити IP-MAC Binding для критичних пристроїв: серверів, шлюзу, керованих комутаторів і точок доступу.

4) Не вмикати надмірно агресивні обмеження без тестування, щоб не заблокувати роботу бізнес-систем [28].

Додатково важливо налаштувати захист бездротової мережі на точці доступу TP-Link EAP653, використовуючи надійний режим шифрування та складний пароль для корпоративного SSID AVERS-WiFi.

1. У розділі Wireless > Wireless Settings, відкривши редагування створеного SSID AVERS-WiFi, у полі Security Mode потрібно вибрати WPA-Personal, оскільки цей режим використовує попередньо заданий спільний ключ доступу та є зручним для невеликої офісної мережі. Для підвищення рівня безпеки у полі Version варто встановити WPA/WPA2-PSK (див. рис. 3.18).

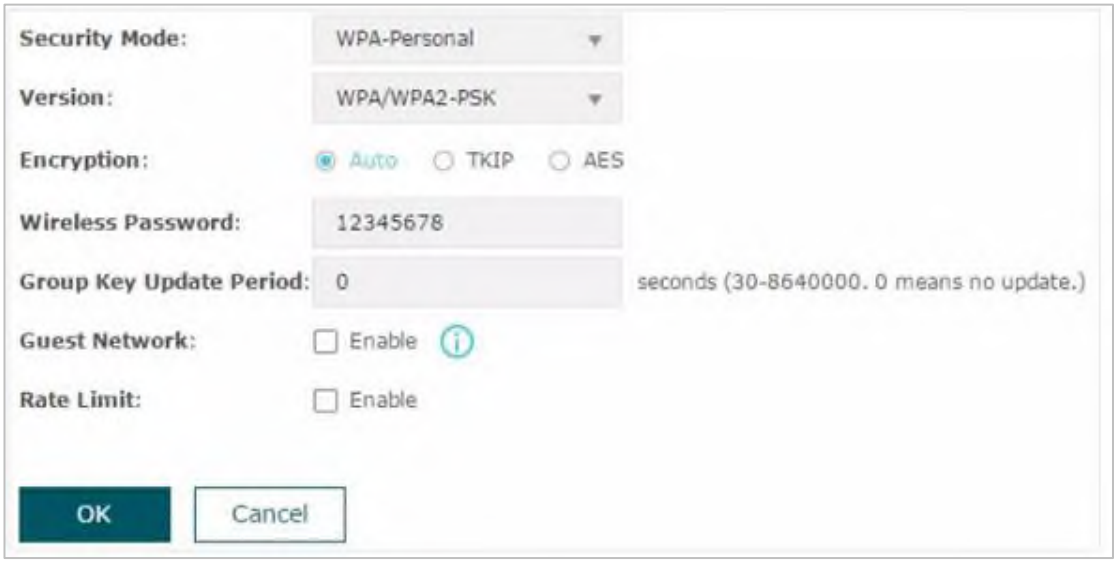

Рисунок 3.18 – Налаштування параметрів захисту

У полі Encryption рекомендується залишити значення Auto або вибрати AES, оскільки AES забезпечує кращий рівень захисту порівняно з TKIP. У полі Wireless Password необхідно задати складний пароль довжиною не менше 8 символів, який має містити великі й малі літери, цифри та спеціальні символи, наприклад AversWiFi@2026!.

Параметр Group Key Update Period можна залишити зі значенням 0, якщо немає окремих вимог до періодичного оновлення групового ключа. Параметри Guest Network і Rate Limit для корпоративної мережі можна залишити вимкненими, якщо точка доступу використовується лише для працівників компанії. Після внесення змін потрібно натиснути OK, а потім Save, щоб застосувати налаштування безпеки для SSID [34].

Окрему увагу потрібно приділити захисту серверів S_1, S_2 і S_3, оскільки вони забезпечують роботу домену, DNS, DHCP, бізнес-систем, баз даних, файлового сховища та резервного копіювання. Для цього на кожному сервері необхідно увімкнути Windows Defender Firewall, Microsoft Defender Antivirus, налаштувати дозволені порти, обмежити віддалене адміністрування лише для IT-підрозділу та забезпечити журналювання подій безпеки.

1. На сервері S_1 увімкнути Windows Defender Firewall і дозволити служби, потрібні для контролера домену, DNS і DHCP. Також слід контролювати стан Microsoft Defender Antivirus, перевірити автоматичні виключення для серверних ролей і не вимикати захист без обґрунтованої потреби.

2. На S_2 Увімкнути Windows Defender Firewall і створити правила доступу лише для необхідних портів: HTTPS 443 або HTTP 80 для веб-додатків, 1433 для SQL Server, 5432 для PostgreSQL, RDP 3389 тільки для IT-адміністраторів. Правила бажано обмежувати не лише портом, а й IP-підмережами VLAN.

3. На S_3 потрібно залишити увімкненим Windows Defender Firewall і дозволити лише необхідні служби: SMB для файлового доступу, служби домену, віддалене адміністрування тільки з VLAN 40 ENGINEERING-IT або з

робочих станцій адміністраторів. Доступ до адміністративних ресурсів має бути заборонений звичайним користувачам. Також потрібно перевірити роботу Microsoft Defender Antivirus, увімкнути регулярне сканування та контролювати спрацювання захисту [29; 31].

Таким чином, налаштування засобів захисту мережі має забезпечити контрольований доступ користувачів до ресурсів, ізоляцію критичних сегментів, захист від зовнішніх і внутрішніх загроз, а також стабільну та безпечну роботу інформаційної системи логістичної компанії.

3.5 Інструкція з експлуатації та моніторингу в мережі

Після введення мережі ТОВ «АВЕРС НК» в експлуатацію необхідно забезпечити постійний контроль її працездатності, безпеки та доступності основних сервісів. Адміністратор мережі повинен регулярно перевіряти стан серверів S_1, S_2, S_3, міжмережевого екрана FW_1, комутатора SW_1, точки доступу AP_1, мережевих принтерів і робочих станцій користувачів.

У разі втрати доступності одного із серверів потрібно перевірити живлення, мережеве підключення, стан служб Windows, завантаження процесора, оперативної пам’яті та дискової підсистеми.

На міжмережевому екрані TP-Link Omada ER7406 необхідно контролювати стан WAN-з’єднань, таблицю NAT, правила Firewall Access Control, VPN-доступ, журнали безпеки та спрацювання Attack Defense.

На комутаторі D-Link DGS-1520-52 потрібно регулярно перевіряти стан портів, швидкість з’єднання, помилки на інтерфейсах.. Якщо користувач не має доступу до мережі, спочатку слід перевірити фізичне підключення порту, стан лінку, VLAN, отриману IP-адресу та доступність шлюзу відповідної підмережі.

Для точки доступу TP-Link EAP653 потрібно контролювати доступність веб-інтерфейсу, стан SSID AVERS-WiFi, кількість підключених клієнтів, рівень сигналу, навантаження на радіомодулі 2.4 GHz і 5 GHz, а також правильність роботи VLAN 60. У разі скарг на якість Wi-Fi потрібно перевірити рівень

сигналу, кількість клієнтів, наявність перешкод, правильність вибору каналів і роботу PoE-інжектора. Також необхідно періодично оновлювати пароль Wi-Fi та стежити, щоб він не використовувався сторонніми особами.

На серверах S_1, S_2 і S_3 слід регулярно переглядати Event Viewer, журнали безпеки, стан Windows Defender Firewall, Microsoft Defender Antivirus, служб Active Directory, DNS, DHCP, баз даних, файлових служб і резервного копіювання. Для S_3 особливо важливо щоденно перевіряти успішність резервних копій, наявність вільного місця на дисках і можливість відновлення тестового файлу з backup.

Робочі станції користувачів повинні отримувати IP-адреси автоматично від DHCP-сервера відповідно до своєї VLAN. У разі проблем із доступом користувача до ресурсів потрібно перевірити IP-адресу, шлюз, DNS-сервер, членство комп'ютера в домені, права користувача в Active Directory та доступність потрібного сервера..

Періодично, не рідше одного разу на місяць, необхідно виконувати профілактичні роботи: перевіряти оновлення Windows Server і робочих станцій, оновлення прошивок мережевого обладнання, актуальність антивірусних баз, коректність резервного копіювання, вільне місце на серверах, стан UPS і журналів помилок. Перед оновленням критичних пристроїв слід створити резервну копію конфігурації та виконувати зміни у неробочий час, щоб не вплинути на бізнес-процеси компанії.

Усі зміни в мережі потрібно документувати: дату зміни, пристрій, суть налаштування, відповідального адміністратора та результат перевірки. Це дозволить швидко відновити працездатність мережі у разі помилки, полегшить подальше адміністрування та забезпечить контроль за розвитком інфраструктури. Постійний моніторинг і планове обслуговування є обов'язковими умовами стабільної, безпечної та ефективної роботи спроєктованої мережі.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проєкту комп'ютерної мережі для ТОВ «АВЕРС НК» і прийняття рішення про її подальше впровадження в роботу.

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. Виконавцями стадій технологічного процесу будуть: керівник проекту, інженер, технік. В таблиці 4.1 наводяться стадії технологічного процесу та середній час їх виконання.

Таблиця 4.1 – Середній час виконання НДР та стадії технологічного процесу

№ п/п	Назва операції	Виконавець	Середній час виконання операції, год.
1.	Передпроєктне обстеження об'єкта	керівник проекту	4
2.	Проектування мережі	інженер	24
3.	Вибір необхідного мережевого обладнання	керівник проекту	6
4.	Монтаж мережі	технік	24
5.	Тестування мережі	інженер	4
6.	Здача проекту в експлуатацію	керівник проекту	2
Разом			64

Загальний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для ТОВ «АВЕРС НК» становить 64 години.

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 власником підприємства працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів роботи підприємства, 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.

Основна заробітна плата становить:

1. Керівник проекту: $З_{осн1} = 300 \cdot 12 = 3600$ грн.;
2. Інженер: $З_{осн2} = 220 \cdot 28 = 6160$ грн.;
3. Технік: $З_{осн3} = 120 \cdot 24 = 2880$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 3600 + 6160 + 2880 = 12640 \text{ грн.}$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту: $З_{дод1} = 3600 \cdot 0,13 = 468$ грн.;

2. Інженер: $З_{дод2} = 6160 \cdot 0,13 = 800,80$ грн.;

3. Технік: $З_{дод3} = 2880 \cdot 0,13 = 374,40$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод} = 468 + 800,80 + 374,40 = 1643,20 \text{ грн.}$$

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

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

$$В_{о.п} = 12640 + 1643,20 = 14283,20 \text{ грн.}$$

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.

$$В_{с.з.} = 14283,20 \cdot 0,22 = 3142,30 \text{ грн.}$$

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.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	300	12	3600	468	-	-
2	Інженер	220	28	6160	800,80	-	-
3	Технік	120	24	2880	374,40	-	-
Разом				12640	1643,20	3142,20	17425,50

Загальні витрати на оплату праці становлять 17425,50 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються за формулою 4.5 як добуток кількості витрачених матеріалів та їх ціни:

$$M_{Bi} = q_i \cdot p_i, \tag{4.5}$$

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:

$$З_{м.в.} = \sum M_{Bi}, \tag{4.6}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

Обладнання	Одиниці виміру	Фактично витрачено матеріалів	Ціна одиниці, грн.	Загальна сума витрат, грн.
1	2	3	4	5
Комутатор D-Link DGS-1520-52	шт.	1	49999	49999
Міжмережевий екран TP-LINK Omada ER7406	шт.	1	6804	6804
Сервер Dell PowerEdge R750xs	шт.	3	109505	328515

Продовження таблиці 4.3

1	2	3	4	5
SSD диск CUSU C300 2TB 2.5" SATAIII	шт.	6	8499	50994
Точка доступу TP-Link EAP653	шт.	1	3959	3959
PoE-інжектор 2E PowerLink PSE801G (1xGE, 1xGE PoE, 802.3af/at	шт.	1	629	629
Мережевий принтер HP Color LaserJet Pro 3202dn	шт.	7	13632	95424
ДБЖ Smart-UPS LogicPower 6000 PRO RM	шт.	1	73000	73000
LAN кабель Cablexpert CAT6, 305м	шт.	5	9999	49995
Шафа монтажна настінна CMS MGSWA 21U	шт.	1	15040	15040
Патч-панель 19" 24xRJ-45 UTP Pipo 1U cat.6	шт.	2	1434	2868

Продовження таблиці 4.3

1	2	3	4	5
Кабельний організатор Digitus 19' 1U, перфорований	шт.	2	579	1158
Подовжувач до серверної шафи Qoltec RACK 1.8м 4 розетки	шт.	1	859	859
Розетка однопортова Cablexpert RJ-45, 6 cat, зовнішня	шт.	36	94	3384
Патч-корд Cablexpert CAT6 UTP 3 м	шт.	36	99	3564
Патч-корд литий RITAR UTP RJ45 Cat.6 0.5м	шт.	40	73	2920
Короб пластиковий АСКО STEP 25x16x2000мм	шт.	35	63,89	2236,15
Сітчастий лоток Ardic 100x50 мм, оцинкований,	м	110	213,97	23536,70
Разом				714884,85

Загальна сума матеріальних витрат становить 714884,85 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою 4.7:

$$З_е = W \cdot T \cdot S \text{ ,} \quad (4.7)$$

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

Час роботи ПК над даним проєктом становить 34 години, споживана потужність - 0,7 кВт/год., вартість 1 кВт електроенергії – 15,94 грн. Тому витрати на електроенергію будуть становити:

$$З_е = 0,7 \cdot 34 \cdot 15,94 = 379,37 \text{ грн.}$$

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.

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

де $Т_В$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_В = 714884,85 \cdot 0,08 = 57190,79 \text{ грн.}$$

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:

$$A = \frac{Б_В \cdot Н_А}{100\%} \cdot \text{Т}, \tag{4.9}$$

де А – амортизаційні відрахування за звітний період, грн. $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; $Н_А$ – норма амортизації, %? Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК використовується при роботі над даним проектом 34 год., балансова вартість ПК – 38000 грн., тому:

$$A = \frac{38000 \cdot 0{,}04}{150} \cdot 34 = 344{,}53 \text{ грн.}$$

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.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6\,, \tag{4.10}$$

де $Н_В$ – накладні витрати.

$$Н_В = 14283,20 \cdot 0,3 = 4284,96 \text{ грн.}$$

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, де зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати.

Таблиця 4.4 – Кошторис витрат НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	14283,2	1,8
Відрахування на соціальні заходи	3142,3	0,4
Матеріальні витрати	714884,85	89,97
Витрати на електроенергію	379,37	0,05
Транспортні витрати	57190,79	7,2
Амортизаційні відрахування	344,53	0,04
Накладні витрати	4284,96	0,54
Собівартість	794510	100

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

$$C_B = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + Т_в + А + Н_в, \quad (4.11)$$

Собівартість дорівнює $С_В$ = 794510 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

$$Ц = Св \cdot (1+Р_{рен}) \cdot (1+ПДВ), \quad (4.12)$$

де $Р_{рен.}$ – рівень рентабельності; ПДВ – ставка податку на додану вартість.

$$Ц = 794510 \cdot (1+0,3) \cdot (1+0,2) = 1239435,60 \text{ грн.}$$

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.

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності ($T_{ОК}$), який можна визначити за формулою 4.13.

$$ЧТВ = -K_B + \sum_{i=1}^{t} \frac{ГП}{(1+i)^t}, \quad (4.13)$$

де $К_В$ – затрати на проект; $Г_п$ – грошовий потік за t – ий рік; t – відповідний рік проекту; i - величина дисконтної ставки (10…15%).

Якщо ЧТВ ≥ 0, то проект може бути рекомендований до впровадження.

$$ЧТВ = -794510 + \frac{597099,35}{(1+0,1)} + \frac{597099,35}{(1+0,1)^2} = 241778,13$$

Термін окупності визначається за формулою 4.14:

$$T_{ОК} = T_{ПВ} + \frac{H_В}{Г_{ПР}}, \quad (4.14)$$

де $T_{ПВ}$ – період до повного відшкодування витрат, років; $H_В$ – невідшкодовані витрати на початок року, грн.; $Г_{ПР}$ – грошовий потік на початок року, грн.

$$T_{ок} = 1 + \frac{251692,41}{597099,35} = 1,4$$

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

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1	Собівартість, грн.	794510
2	Плановий прибуток, грн.	444925,6
3	Ціна, грн.	1239435,6
4	Чиста теперішня вартість, грн.	241778,13
5	Термін окупності, рік	1,4

Загальна вартість розробленої мережі для ТОВ «АВЕРС НК» становить 1239435,60 грн. Термін окупності становить 1,4 роки.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1 Завдання та функції служби охорони праці щодо профілактики виробничого травматизму в ТОВ «АВЕРС НК»

Діяльність служби охорони праці в логістичній компанії ТОВ «АВЕРС НК» є ключовим елементом системи забезпечення безпеки працівників та ефективної профілактики виробничого травматизму. Відповідно до чинних нормативно-правових актів, служба охорони праці створюється на підприємстві як самостійний підрозділ, що підпорядковується безпосередньо керівнику, і має на меті організацію виконання комплексу організаційно-технічних, санітарно-гігієнічних та соціально-економічних заходів [11].

Головним завданням цієї служби в умовах інтенсивної логістичної діяльності є створення та підтримання ефективної системи управління охороною праці, орієнтованої на превентивне виявлення загроз, пов'язаних із транспортними перевезеннями, роботою складських комплексів та виконанням вантажно-розвантажувальних операцій. До пріоритетних завдань належить організація безперервного процесу навчання персоналу (водіїв, комірників, операторів навантажувачів) безпечним методам роботи, проведення всіх видів інструктажів, а також координація забезпечення працівників специфічними засобами індивідуального захисту (сигнальними жилетами, захисним взуттям, касками) та суворий контроль за проходженням обов'язкових передрейсових і періодичних медичних оглядів.

Функціонал служби охорони праці логістичного підприємства охоплює широкий спектр організаційних, контролюючих та аналітичних напрямів. Працівники служби здійснюють постійний аудит та нагляд за дотриманням норм охорони праці під час механізованого та ручного переміщення вантажів, складування товарів на стелажних системах та маневрування транспорту на території бази. Важливою функцією є проведення експертизи технічного стану робочих місць, перевірка наявності дозвільної документації на експлуатацію

вантажопідіймальних механізмів та контроль за дотриманням швидкісних режимів складської техніки. У разі виявлення порушень, які можуть призвести до наїзду на працівника, падіння вантажу чи іншої аварії, спеціалісти служби мають повноваження видавати обов'язкові до виконання приписи, а в критичних ситуаціях — вимагати негайного зупинення експлуатації несправного навантажувача чи заборонити виконання робіт на аварійній ділянці складу.

Окрім того, служба охорони праці ТОВ «АВЕРС НК» веде облік і детальний аналіз причин мікротравм та ДТП на території підприємства, розробляє схеми безпечного руху транспорту і пішоходів, а також бере безпосередню участь у роботі комісій з розслідування нещасних випадків на виробництві для недопущення подібних інцидентів у майбутньому [7; 5].

5.2 Система захисного заземлення та занулення комп'ютерного обладнання в ТОВ “АВЕРС НК”

Система захисного заземлення та занулення комп’ютерного обладнання в ТОВ «АВЕРС НК» має розглядатися як складова електробезпеки офісних, серверних і складських приміщень підприємства. У комп’ютерній мережі підприємства використовуються персональні комп’ютери, сервери, комутатори, міжмережевий екран, мережеві принтери, точки доступу Wi-Fi, джерела безперебійного живлення та інше електронне обладнання. Усе це обладнання живиться від електричної мережі та в разі пошкодження ізоляції, пробою блока живлення або порушення цілісності кабелю може створювати небезпеку ураження працівника електричним струмом [6].

Для комп’ютерного обладнання особливо важливим є захист від появи небезпечної напруги на металевих корпусах системних блоків, серверних шаф, джерел безперебійного живлення, мережевих комутаторів і периферійних пристроїв. У нормальному режимі ці частини не перебувають під напругою, однак у разі пошкодження ізоляції вони можуть стати небезпечними для дотику. Саме для цього застосовуються захисне заземлення, захисне занулення,

захисні провідники, автоматичне вимкнення живлення, пристрої захисного вимкнення та вирівнювання потенціалів. ДСТУ EN 61140:2019 визначає загальні принципи захисту від ураження електричним струмом для установок та обладнання, тобто є базовим нормативним джерелом для обґрунтування таких заходів.

Захисне заземлення полягає в навмисному електричному з'єднанні відкритих провідних частин обладнання із заземлювальним пристроєм. Його призначення — зменшити напругу дотику до безпечного рівня у випадку пошкодження ізоляції та відвести струм замикання на землю.

Занулення застосовується в електромережах із глухозаземленою нейтраллю і полягає в приєднанні відкритих провідних частин електрообладнання до нульового захисного провідника. У разі пробою ізоляції на корпус виникає струм короткого замикання, який має спричинити спрацювання автоматичного вимикача або іншого апарата захисту та швидке вимкнення пошкодженої ділянки мережі. У сучасних системах електроживлення замість побутового терміна «занулення» частіше використовують поняття захисний провідник PE або PEN-провідник залежно від типу системи заземлення.

Для приміщень ТОВ «АВЕРС НК» доцільно передбачити застосування трипровідної однофазної мережі живлення L–N–PE для робочих місць і серверного обладнання. У такій схемі фазний провідник L подає напругу, робочий нульовий провідник N забезпечує робочий струмовий контур, а захисний провідник PE призначений лише для електробезпеки та приєднується до металевих корпусів обладнання. Захисний провідник не повинен використовуватися як робочий нуль, оскільки це може створити небезпечну ситуацію при його обриві або неправильному підключенні.

У серверній кімнаті підприємства вимоги до заземлення мають бути особливо суворими, оскільки там зосереджене критично важливе обладнання: сервери, комутатор, міжмережевий екран, джерела безперебійного живлення, патч-панелі та телекомунікаційна шафа. Металеві корпуси серверів, шаф і ДБЖ

повинні бути приєднані до захисного провідника. Це знижує ризик ураження електричним струмом під час обслуговування, заміни кабелів, встановлення модулів, підключення мережевих пристроїв і виконання діагностики. Крім того, наявність якісного заземлення сприяє зменшенню впливу електростатичних розрядів на електронні компоненти.

Для робочих місць працівників, де встановлені ПК, монітори, мережеві принтери або інші периферійні пристрої, потрібно використовувати справні розетки із захисним контактом. Підключення комп'ютерного обладнання через подовжувачі без заземлювального контакту, саморобні перехідники, пошкоджені мережеві фільтри або розетки з відсутнім PE-провідником є неприпустимим.

У системі електробезпеки комп'ютерного обладнання важливо застосовувати не лише заземлення, а й автоматичне вимкнення живлення. Для групових ліній живлення комп'ютерних робочих місць слід передбачати автоматичні вимикачі відповідного номіналу, а для розеткових груп — пристрої захисного вимкнення або диференційні автомати. Їхнє призначення полягає в тому, щоб швидко вимкнути живлення при струмі витоку, короткому замиканні або іншому аварійному режимі. Захисне заземлення без справного апарата автоматичного вимкнення не забезпечує повного рівня безпеки, оскільки небезпечна напруга на корпусі може зберігатися до моменту відключення пошкодженої лінії.

Важливим є також організаційний контроль. Відповідальні працівники або залучені електротехнічні спеціалісти повинні проводити огляд електромережі, фіксувати результати перевірок, не допускати експлуатації обладнання з пошкодженими кабелями, вилками, корпусами або розетками. Працівникам необхідно заборонити самостійне втручання в електромережу, використання несправних подовжувачів, підключення великої кількості пристроїв до однієї розетки та від'єднання захисного контакту [3; 6].

5.3 Вплив стресу на безпеку праці персоналу ТОВ “АВЕРС НК”

Стрес є важливим психофізіологічним чинником, який може безпосередньо впливати на безпеку праці персоналу логістичного підприємства. У ТОВ «АВЕРС НК» працівники виконують різні види робіт: офісне адміністрування, диспетчеризацію, логістичне планування, роботу з клієнтами, керування транспортними потоками, складські операції, роботу з документами та комп’ютерними системами. Для такої діяльності характерні підвищена відповідальність, необхідність швидкого прийняття рішень, робота з великим обсягом інформації, взаємодія з водіями, клієнтами й постачальниками, а також дотримання строків доставки [3].

У логістичній компанії стрес може виникати через дефіцит часу, затримки транспорту, конфліктні ситуації з клієнтами, термінові зміни маршрутів, перевантаження інформацією, відповідальність за збереження вантажу, монотонну роботу за комп’ютером або нічні й понаднормові зміни. Для складського персоналу додатковими стресовими чинниками можуть бути інтенсивний темп роботи, шум, рух навантажувачів, ризик падіння вантажу, необхідність постійної концентрації уваги під час вантажно-розвантажувальних операцій. Для водіїв і диспетчерів особливо небезпечними є втома, емоційне напруження, поспіх і потреба швидко реагувати на зміну дорожньої або виробничої ситуації [5].

Найбільш небезпечним наслідком стресу для безпеки праці є зниження уваги й самоконтролю. Працівник у стані нервового напруження може швидше втомлюватися, гірше сприймати інструкції, пропускати важливі сигнали, неправильно оцінювати виробничу ситуацію або діяти поспіхом. У логістичному підприємстві це може призвести до помилок під час оформлення документів, неправильного направлення вантажів, порушення порядку руху складської техніки, недотримання безпечної відстані, неправильного складування товарів або нехтування засобами індивідуального захисту. Тому

стрес слід розглядати не лише як психологічну проблему, а як реальний фактор ризику виробничого травматизму.

Для адміністративного та офісного персоналу ТОВ «АВЕРС НК» стрес може проявлятися у зниженні працездатності, дратівливості, помилках під час роботи з електронними документами, CRM-системами, логістичними базами даних і фінансовими матеріалами. Помилки диспетчера або менеджера з логістики можуть мати не тільки організаційні, а й безпекові наслідки: неправильне планування маршруту, несвоєчасне інформування водія, неузгоджене переміщення транспорту на території підприємства або порушення графіка вантажно-розвантажувальних робіт. У таких умовах стрес може опосередковано створювати небезпечні ситуації для водіїв, комірників, вантажників та інших працівників.

Для складського персоналу вплив стресу є ще більш безпосереднім. Якщо працівник виконує вантажно-розвантажувальні операції в умовах поспіху або емоційного напруження, зростає ризик неправильного захоплення вантажу, падіння предметів, зіткнення з навантажувачем, травмування рук, ніг або спини. Стрес також може призводити до нехтування простими правилами безпеки: працівник може не одягнути сигнальний жилет, не перевірити стійкість вантажу, пройти в небезпечній зоні руху техніки або виконувати роботу без погодження з відповідальним працівником. Саме тому профілактика стресу має бути частиною загальної системи управління охороною праці.

Профілактика негативного впливу стресу повинна включати організаційні, технічні та соціально-психологічні заходи. До організаційних заходів належить раціональне планування робочого часу, уникнення надмірного понаднормового навантаження, чіткий розподіл обов’язків між диспетчерами, менеджерами, водіями та складським персоналом, а також запровадження зрозумілих алгоритмів дій у разі аварійних або конфліктних ситуацій. Важливим є також періодичне навчання персоналу безпечним методам роботи, адже навчання й інструктажі є одним із базових елементів системи охорони праці.

До технічних заходів можна віднести належне освітлення робочих місць, справність складської техніки, наявність розмітки руху транспорту й пішоходів, використання засобів сигналізації, відеоспостереження, автоматизацію обліку вантажів і зменшення ручних операцій. Чим зрозуміліша й безпечніша організація робочого простору, тим менше працівник перебуває в ситуації невизначеності, а отже — менший рівень стресу під час виконання завдань.

Соціально-психологічні заходи передбачають підтримання нормального морально-психологічного клімату в колективі, попередження конфліктів, недопущення грубого стилю керівництва, можливість повідомляти про небезпечні ситуації без страху покарання, а також своєчасне реагування керівництва на скарги працівників щодо перевантаження або небезпечних умов праці. Працівники мають розуміти, що повідомлення про втому, небезпечний інцидент, помилку або конфлікт є не проявом слабкості, а частиною профілактики травматизму.

Окрему увагу потрібно приділяти водіям, диспетчерам і працівникам складу, оскільки їхня діяльність пов’язана з підвищеною відповідальністю й ризиком аварійних ситуацій. Для них доцільно передбачати регулярні інструктажі, контроль дотримання режиму праці та відпочинку, недопущення роботи у стані вираженої втоми, а також аналіз причин помилок і небезпечних ситуацій. Якщо стресові фактори повторюються систематично, служба охорони праці разом із керівниками підрозділів повинна розробляти коригувальні заходи: перегляд графіка, перерозподіл навантаження, уточнення інструкцій, покращення комунікації між відділами [3].

ВИСНОВКИ

У кваліфікаційній роботі було розроблено проєкт комп'ютерної мережі для ТОВ «АВЕРС НК», яка забезпечить об'єднання всіх структурних підрозділів підприємства в єдине інформаційне середовище, стабільний доступ до локальних і хмарних сервісів, ERP/CRM-систем, файлових ресурсів, засобів резервного копіювання та сервісів моніторингу. Для логістичної компанії це має особливе значення, оскільки від стабільності комп'ютерної мережі залежить цілодобовий контроль рейсів, координація роботи водіїв, взаємодія з клієнтами, митними органами та оперативне опрацювання транспортної документації.

У процесі виконання роботи було розроблено логічну та фізичну структуру мережі, виконано адресацію підмереж, визначено склад активного та пасивного мережевого обладнання, а також обґрунтовано вибір серверів, комутатора, міжмережевого екрана, точки доступу, джерела безперебійного живлення та кабельної інфраструктури.

Для серверної частини мережі запропоновано використання трьох окремих серверів на основі апаратної платформи Dell PowerEdge R750xs. Такий підхід дозволяє розподілити навантаження між окремими функціональними вузлами та уникнути взаємного впливу критичних служб.

У роботі реалізовано сегментацію мережі на шість VLAN на керованому L3-комутаторі D-Link DGS-1520-52. Такий поділ не є надмірним для офісної мережі, але забезпечує чітке розмежування доступу між підрозділами, зменшує широкомовний трафік, підвищує рівень безпеки та спрощує подальше адміністрування мережі.

Для забезпечення стабільного доступу до Інтернету передбачено підключення двох незалежних інтернет-провайдерів за схемою Dual-WAN через міжмережевий екран TP-Link Omada ER7406. На міжмережевому екрані передбачено правила Firewall Access Control, які дозволяють лише необхідний

трафік між VLAN, обмежують доступ до критичних серверів і блокують небажані з’єднання.

Для бездротового доступу у переговорній кімнаті передбачено використання точки доступу TP-Link EAP653 із підключенням через PoE-інжектор.

У межах проєкту також розроблено рекомендації щодо налаштування захисту серверів і робочих станцій. Для серверів S_1, S_2 і S_3 передбачено використання Windows Defender Firewall, Microsoft Defender Antivirus, журналювання подій, обмеження доступу до адміністративних сервісів і контроль дозволених портів.

У роботі було розглянуто питання тестування, налагодження та експлуатації мережі. Запропоновано використовувати стандартні засоби діагностики, зокрема ping, tracert, nslookup, ipconfig, журнали подій Windows Server, вебінтерфейси мережевого обладнання, засоби моніторингу комутатора, міжмережевого екрана та точки доступу.

В економічній частині кваліфікаційної роботи виконано розрахунок повної вартості проєктування, закупівлі обладнання, монтажу, налаштування та введення комп’ютерної мережі в експлуатацію. Загальна вартість розробленої мережі для ТОВ «АВЕРС НК» становить 1 239 435,60 грн. Розрахований термін окупності становить 1,4 роки, що підтверджує економічну доцільність впровадження запропонованого рішення. Очікуваний ефект досягається за рахунок підвищення продуктивності працівників, зменшення простоїв, централізації управління ресурсами, зниження ризику втрати даних і покращення контролю бізнес-процесів.

У п’ятому розділі кваліфікаційної роботи було розглянуто питання охорони праці та безпеки життєдіяльності під час експлуатації комп’ютерної мережі. Зокрема, проаналізовано завдання та функції служби охорони праці щодо профілактики виробничого травматизму в ТОВ «АВЕРС НК», розглянуто систему захисного заземлення та занулення комп’ютерного обладнання, а також вплив стресу на безпеку праці персоналу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Комп'ютерні мережі: підручник. Вінниця: ВНТУ, 2020. 378 с.
2. Волосюк Ю. В. Комп'ютерні мережі: курс лекцій. Миколаїв: МНАУ, 2019. 203 с.
3. Грибан В. Г., Фоменко А. Є., Казначеєв Д. Г. Безпека життєдіяльності та охорона праці: підручник. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2022. 388 с.
4. Жураковський Б. Ю., Зенів І.О. Комп'ютерні мережі. Частина 1. Навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем». Київ: КПІ ім. Ігоря Сікорського, 2020. 336 с.
5. Курепін В. М. Основи охорони праці: навчальний посібник для студентів закладів вищої освіти аграрної галузі. Миколаїв: МНАУ, 2022. 347 с.
6. Панченко С.В., Акімов О.І., Бабаєв М.М. та ін. Електробезпека: Підручник. Харків: УкрДУЗТ, 2018. 295 с.
7. Пожарова О.В. Охорона праці: навч.-метод. посібник. Одеса. 2021. 80 с.
8. Челомбитько В.В. Структуровані кабельні системи: конспект лекцій з дисципліни «Структуровані кабельні системи» для підготовки студентів за спеціальністю 172 «Телекомунікації та радіотехніка». Львів: ЛННЦ ОНАЗ, 2019. 38 с.
9. Telecommunications Distribution Methods Manual (TDMM). 15th ed. Tampa: BICSI, 2024. 1993 p.
10. АВЕРС НК, ТОВ. URL: https://goldenpages.rv.ua/avers (дата звернення: 02.05.2026).

11. Закон України «Про охорону праці». URL: https://zakon.rada.gov.ua/laws/show/2694-12#Text (дата звернення: 28.05.2026).

12. Інформаційні потоки у логістиці. URL: https://hub.nmcbook.com.ua/3-2-informatsijna-lohistyka/ (дата звернення: 12.04.2026).

13. Мережеві утиліти діагностики: ping, tracert, traceroute і mtr. URL: https://thehost.ua/ua/wiki/administration/ping-tracert (дата звернення: 24.05.2026).

14. Порівнюємо бездротові точки доступу. URL: https://rozetka.com.ua/ua/comparison/c80195/ids=416843811,460986784,365056479/ (дата звернення: 19.05.2026).

15. Порівнюємо бфп/принтери. URL: https://rozetka.com.ua/ua/comparison/c80007/ids=450153851,568514956,455653159/ (дата звернення: 19.05.2026).

16. Порівнюємо маршрутизатори. URL: https://rozetka.com.ua/ua/comparison/c80193/ids=500637439,374362566,577375759/ (дата звернення: 13.05.2026).

17. Порівняння. Керовані комутатори L2, L2+, L3. URL: https://e-server.com.ua/uk/my-account/compare (дата звернення: 08.05.2026).

18. Порівняння. Сервери Rack (стійкові). URL: https://e-server.com.ua/uk/my-account/compare (дата звернення: 14.05.2026).

19. Цимбалістова, О., Черніхова, О. С. Роль і значення інформаційних технологій у впровадженні логістичної методики управління. URL: https://doi.org/10.32782/2524-0072/2024-70-117 (дата звернення: 06.04.2026).

20. Як вибрати ОС для сервера. Вирішення завдань бізнесу. URL: https://xserver.cloud/uk/blog/reviews/yak-vibrati-os-dlya-servera-naykraschi-rishennya-dlya (дата звернення: 28.05.2026).

21. Як побудувати хорошу корпоративну мережу Wi-Fi? — Керівництво для підприємств. URL: https://e-server.com.ua/uk/poradi/jak-pobuduvati-horoshu-korporativnu-merezhu-wi-fi-kerivnictvo-dlja-

pidpriiemstv?srsltid=AfmBOop60CAGGe3R44FJaSY6yva1IrMeWuKLVC66hhad8KNHS3hndJH5 (дата звернення: 26.04.2026).

22. Яку ОС обрати для свого сервера? URL: https://unihost.com/blog/uk/os-to-choose/ (дата звернення: 28.05.2026).

23. D-Link. DGS-1520-52 Layer 3 Stackable Smart Managed Switch. URL: https://www.dlink.com/en/products/dgs-1520-52-layer-3-stackable-smart-managed-switch (дата звернення: 10.05.2026).

24. D-Link Web UI Reference Guide. Product Model: DGS-1520 Series Gigabit Ethernet Smart Managed Switch. URL: https://ftp.dlink.com/pub/Switch/DGS-1520-52/Description/DGS-1520%20Series_A1_Web%20UI%20Manual_v1.1(WW).pdf (дата звернення: 30.05.2026).

25. HP Color LaserJet Pro 3202dn. URL: https://support.hp.com/au-en/product/details/hp-color-laserjet-pro-3201-3204,-3288-printer-series/model/2102048004 (дата звернення: 20.05.2026).

26. HP Color LaserJet Pro 3202dn. User Guide. URL: https://kaas.hpcloud.hp.com/pdf-public/pdf_7795476_en-US-1.pdf (дата звернення: 21.05.2026).

27. Network Topologies. URL: https://networklessons.com/network-fundamentals/network-topologies? (дата звернення: 14.04.2026).

28. Omada Gigabit VPN Router/Gateway. User Guide. URL: https://static.tp-link.com/upload/manual/2024/202404/20240412/ER7206(UN)2.0_UG.pdf (дата звернення: 28.05.2026).

29. Roles, Role Services, and Features included in Windows Server - Server Core. URL: https://learn.microsoft.com/uk-ua/windows-server/administration/server-core/server-core-roles-and-services? (дата звернення: 26.05.2026).

30. Routing Between VLANs Overview. URL: https://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_rtng_vlan_ovw_ps6350_TSD_Products_Configuration_Guide_Chapter.html (дата звернення: 15.04.2026).

31. Setting Up Active Directory, DHCP, and DNS on Windows Server 2022. URL: https://github.com/jwnfld3/active-directory-network-lab? (дата звернення: 25.05.2026).

32. Star Topology. URL: https://www.sciencedirect.com/topics/ mathematics/ star-topology? (дата звернення: 14.04.2026).

33. TP-Link Omada. EAP653 | AX3000 Ceiling Mount WiFi 6 Access Point. URL: https://www.omadanetworks.com/us/business-networking/omada-wifi-ceiling-mount/eap653/ (дата звернення: 19.05.2026).

34. TP-Link Omada EAP653 інструкція користувача. URL: https://www.інструкціїкористувача.com.ua/tp-link/omada-eap653/інструкція-користувача?p=35 (дата звернення: 31.05.2026).

35. TP-Link Omada. ER7406 Omada Gigabit Rackmount/Desktop VPN Gateway. URL: https://www.omadanetworks.com/uy/business-networking/omada-router-wired-router/er7406/ (дата звернення: 13.05.2026).