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 і підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі рекламного бюро "Бум"**

Виконав: студент IV курсу, групи КІ-418

Спеціальності **123 Комп'ютерна інженерія**

(шифр і назва спеціальності)

_____ Микола РАДЬ

(ім'я та прізвище)

Керівник _____ Ігор ТХІР

(ім'я та прізвище)

Рецензент _____ _____

(ім'я та прізвище)

Тернопіль - 2025

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
" 31 " березня 2025 року

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

Радю Миколі Васильовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Розробка проєкту комп'ютерної мережі рекламного бюро "Бум"

керівник роботи Тхір Ігор Любомировтч
(прізвище, ім'я, по батькові)

Затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 28.03.2025р № 4/9-166а

2. Строк подання студентом роботи: 13 червня 2025 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, 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 проекту. Спеціальний розділ. Економічний розділ. Охорона праці, техніка безпеки та екологічні вимоги.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
- плани 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, техніка безпеки та екологічні вимоги	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	05.05	
3	Написання першого розділу	16.05	
4	Розробка технічного та робочого проекту	23.05	
5	Написання спеціального розділу	30.05	
6	Розрахунок економічної частини	2.06	
7	Написання розділу охорони праці	4.06	
8	Виконання графічної частини	9.06	
9	Оформлення проєкту	11.06	
10	Погодження нормоконтролю	12.06	
11	Попередній захист роботи	13.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 04 квітня 2025 року

Студент _____ Микола РАДЬ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Ігор ТХІР
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Радь М.В. Розробка проєкту комп'ютерної мережі рекламного бюро "Бум": кваліфікаційна робота на здобуття освітнього ступеня фаховий молодший бакалавр за спеціальністю "123 – Комп'ютерна інженерія". Тернопіль: ВСП "ТФК ТНТУ", 2025. 103 с.

Кваліфікаційна робота передбачає розробку проекту комп'ютерної мережі рекламного бюро "Бум" згідно стандартів та вимог замовника. В проектовані мережі використано сучасні стандарти Gigabit Ethernet IEEE 802.3ab, IEEE 802.11ac та Ethernet IEEE 802.3q. При цьому реалізовано розподіл мережі на віртуальні підмережі, планування та розподіл адресного простору. Розроблено інструкції з інсталяції та налаштування файлового сервера, DHCP-сервера та web-севрера, шлюзу доступу до мережі Інтернет, віртуальних підмереж та засобів захисту мережі.

Ключові слова: комп'ютерна мережа, файловий сервер, web-сервер, DHCP-сервер, маршрутизатор, комутатор, віртуальна мережа, VLAN, антивірус

ANNOTATION

Rad M.V. Development of a computer network project for the advertising agency "Boom": qualification work for the degree of professional junior bachelor in the specialty "123 – Computer Engineering". Ternopil: VSP "TFK TNTU", 2025. 103 p.

The qualification work involves the development of a computer network project for the advertising agency "Boom" according to the standards and requirements of the customer. The designed networks use modern Gigabit Ethernet IEEE 802.3ab, IEEE 802.11ac and Ethernet IEEE 802.3q standards. At the same time, the network is divided into virtual subnets, planning and allocation of address space is implemented. Instructions for installing and configuring a file server, DHCP server and web server, Internet access gateway, virtual subnets and network security tools have been developed.

Keywords: computer network, file server, web server, DHCP server, router, switch, virtual network, VLAN, antivirus

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

BIND (Berkeley Internet Name Domain) – сервер доменних імен в операційній системі FreeBSD

DNS (Domain Name System) – сервер доменних імен.

DHCP (Dynamic Host Configuration Protocol) – протокол динамічної конфігурації вузла.

HTTP (Hypertext Transfer Protocol) – протокол передачі гіпертексту.

IEEE 802.3ab – стандарт Gigabit Ethernet на витій парі UTP 5e, 6.

IEEE 802.3z – стандарт Gigabit Ethernet на оптоволоконному кабелі.

IEEE 802.3ac – стандарт, що пребачає збільшення максимального розміру фрейму до 1522 байт, яке дозволяє зберігати інформації про VLAN стандарту IEEE 802.1Q та пріоритету стандарту IEEE 802.1p.

IEEE 802.3u – стандарт Fast Ethernet 100Мбіт/с.

IP (Internet Protocol) – Інтернет-протокол;

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) – апаратна адреса ПК;

SNMP (Simple Network Management Protocol) – простий протокол мережевого управління. Протокол мережевого адміністрування.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол управління передачею/Інтернет протокол;

UTP (Unshielded Twisted Pair) - неекранована скручена пара;

ОС – операційна система.

ПК – персональний комп’ютер.

ВСТУП

Для обміну інформацією між різними цифровими пристроями можна використовувати різноманітні засоби, проте найбільш ефективним варіантом буде використання локальної комп'ютерної мережі, яка забезпечує високу швидкість обміну інформацією.

Під локальною мережею розуміють спільне підключення декількох комп’ютерів (робочих станцій) та інших мережевих пристроїв до спільного каналу передачі даних. Завдяки локальним мережам користувачі отримали можливість одночасного використання мережевих ресурсів: дискових масивів, мережевих принтерів і БФП, безперечно доступ до глобальної мережі і баз даних декількома користувачами, які не мають безпосереднього з’єднання з цими ресурсами.

Комп’ютерна мережа дозволяє об’єднати всі комп’ютери співробітників в єдину систему, що значно спрощує обмін інформацією, файлами, проєктами. Це особливо важливо для рекламного бюро, де постійно працюють з візуальними матеріалами, дизайнами, макетами, презентаціями тощо.

Завдяки мережі можна організувати централізоване зберігання файлів на сервері або у хмарі, що дозволяє кільком працівникам працювати над одним проєктом одночасно, бачити актуальні зміни та уникати дублювання роботи.

Розробка комп’ютерної мережі для рекламного бюро є не просто бажаною, а необхідною умовою ефективної, швидкої та безпечної роботи в сучасних умовах.

Отже, метою кваліфікаційної роботи є розробка локальної комп’ютерної мережі рекламного бюро “Бум” на основі вимог технічного завдання.

Завдання із проектування, інсталяції, налаштування і забезпечення безперебійного функціонування комп’ютерної мережі є актуальною і матиме практичне використання. З метою перевірки правильності прийнятих рішень варто реалізувати моделювання роботи мережі в певному програмному середовищі.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Згідно із темою кваліфікаційної роботи необхідно розробити комп'ютерну мережу для рекламного буро "Бум" стандарту Gigabit Ethernet, її проектування, встановлення, монтування, налагодження мережних служб та сервісів. В даній мережі необхідно передбачити наявність як провідного так і безпровідного сегменту для забезпечення вільного доступу до ресурсів Інтернет відвідувачів рекламного бюро.

Щоб реалізувати поставлені завдання необхідно розробити технічне завдання, в якому врахувати всі вимоги, поставлені до мережі відповідно до існуючого плану приміщення.

Мережа розробляється для рекламного буро "Бум", яке надає послуги у сфері розробки дизайну і поліграфічного друку різноманітної рекламно-інформаційної та сувенірної продукції, зовнішньої реклами, а також створення рекламних електронних web-ресурсів. Дане підприємство крім розробки дизайну друкованої продукції має власні потужності для цифрового, поліграфічного та флексографічного друку, виготовлення вивісок, рекламних білбордів, об'ємних букв.

У зв'язку з розширенням сфери діяльності рекламного бюро "Бум" змінило своє місцезнаходження в іншій двоповерховій будівлі, тому виникла необхідність впровадження комп'ютерної мережі за новою локацією.

При цьому проектована мережа повинна забезпечити:

- швидкий обмін інформацією між працівниками (макетами, текстами, відео);
- централізований доступ до файлів і проєктів, щоб уникнути плутанини з версіями;

- захист важливої комерційної інформації. Наявність внутрішньої мережі забезпечує вищий рівень контролю за доступом до конфіденційної інформації (бази клієнтів, брифів, комерційних пропозицій, рахунків тощо);

- спрощення рутинних процесів і підвищення продуктивності праці за рахунок автоматизація багатьох процесів (розсилка, звітність, збереження архівів) за допомогою внутрішньої мережі дозволяє зменшити кількість рутинної роботи та зосередитися на творчій діяльності;

- розмежування доступу різних підрозділів підприємства до окремих інформаційних ресурсів;

- централізоване керування підключенням до ресурсів Інтернет;

- спільне використання мережевого програмного забезпечення.

1.1.2 Призначення розробки

При проектуванні комп'ютерної мережі рекламного бюро "Бум" необхідно реалізувати наступні комунікаційні вимоги, встановлені замовником:

- сукупні витрати на проєктування, інсталяцію та впровадження мережі мають залишатися в межах бюджету, визначеного замовником;

- поєднати всю цифрову комп'ютерну техніку бюро в єдину систему для швидкого обміну інформацією та спільного використання ресурсів із поділом на логічні групи;

- забезпечити спільний доступ всіх кінцевих вузлів до ресурсів Інтрнет;

- забезпечити спільний доступ комп'ютерів до засобів друку документів;

- гарантувати обмін між кінцевими вузлами мережі із швидкістю 1 Гбіт/с;

- забезпечити можливість безпровідного доступу до ресурсів Інтернет для відвідувачів сервісного центру та самих працівників;

- забезпечити можливість легко масштабування мережі при розширенні бюро, додаванні нових робочих місць та обладнання;

- забезпечити можливість безпровідного доступу до мережі із безпровідних пристрої.

1.1.3 Вимоги до апаратного і програмного забезпечення

Для реалізації проекту комп'ютерної мережі рекламного бюро "Бум" необхідно використання як пасивного так і активного мережевого обладнання.

Згідно з технічним завданням замовника, мережа має підтримувати швидкість передачі даних до 1 Гбіт/с між кінцевими вузлами. Для реалізації цієї вимоги вирішено використати стандарти технології Gigabit Ethernet. Крім цього, замовник також поставив вимогу забезпечення безпровідний доступ до мережевих ресурсів, тому в проектованій мережі слід також передбачити безпровідний сегмент. Враховуючи вимоги замовника щодо швидкість передачі даних 1 Гбіт/с, вирішено використати стандарти технології Wi-Fi стандарту IEEE-802.11ac.

Для мінімізації витрат на розробку мережі, згідно з вимогами замовника, в якості фізичного середовища передачі даних доцільно використовувати кабель категорії 6 (1000Base-T).

В загальному для проектування мережі рекламного бюро "Бум" необхідно використати наступне пасивне мережеве обладнання:

- мережевий кабель категорії Cat 6;
- мережеві роз'єми 8P8C;
- патч-корди;
- мережеві розетки Cat 6;
- комутаційна шафа.

До переліку активного мережевого обладнання необхідного для проектованої мережі входить:

- маршрутизатор, який повинен забезпечити доступ до ресурсів Інтернет та виконувати функції міжмережевого екрану, для захисту комп'ютерної мережі рекламного бюро "Бум" від зовнішніх загроз із Інтернет та створення демілітаризованої DMZ-зони web-сервера;

- головний комутатор третього рівня OSI-моделі, який буде здійснювати маршрутизацію між окремими віртуальними підмережами всередині ЛОМ рекламного бюро “Бум”;

- сегментуючі комутатори робочих груп зі швидкістю портів 1Гбіт/с на 24 портів та підтримкою стандартів 802.3ab Gigabit Ethernet, 802.1p QoS, 802.1Q VLAN;

- сервер для організації файлового, DNS- та web-сервера;

- точки доступу стандарту IEEE-802.11ac для безпровідного підключення кінцевих пристроїв зі швидкістю 1 Гбіт/с.

До програмного забезпечення проектованої мережі відносяться:

- операційні системи робочих станцій, що забезпечують роботу стеку протоколів TCP/IP та підтримують використовуване на підприємстві прикладне програмне забезпечення;

- операційна система сервера, яка повинна бути надійною, регулярно оновлюватись, підтримувати файловий, DNS- та web- сервери.

1.1.4 Вимоги до документації

Після розробки та впровадження локальної комп'ютерної мережі необхідно підготувати пакет документації, який допоможе у вирішенні експлуатаційних проблем, а також у майбутній модернізації, моніторингу та зборі статистичних даних.

Для мережі рекламного бюро “Бум” необхідно розробити наступну технічну документацію:

- план приміщення;
- логічна топологія;
- схема прокладання кабелів на плані приміщення;
- таблиця IP-адрес.
- інструкції з налаштування базових мережевих пристроїв ;
- інструкції з тестування мережі та звіт по тестуванню.

1.1.5 Техніко-економічні показники

Основні техніко-економічні показники рекламного бюро “Бум”:

- топологія мережі – гібридна топологія, що поєднує провідну ієрархічну розширену зірку та безпровідну комірчасту;
- специфікації мережі – IEEE 802.3ab та IEEE-802.11ac;
- кількість робочих станцій – 60;
- кількість мережевих принтерів – 5;
- фізичне середовище передачі даних – скручена пара категорії 6;
- типи серверів – файловий сервер;
- вартість мережі до 300 тис.грн.

1.1.6 Стадії та етапи розробки

Створення комп'ютерної мережі, як і будь-який проєкт, потребує попереднього розроблення чіткого плану впровадження. Загалом, процес розробки локальної мережі складається з трьох основних етапів [3]:

- створення та затвердження технічного завдання на розробку мережі;
- написання робочого проекту;
- розробка технічної документації до проекту.

Створення робочого проекту мережі рекламного бюро “Бум” складається із наступних етапів [3]:

- вивчення комунікаційних вимог до створюваної мережі;
- розробка плану проекту комп’ютерної мережі сервісного центру;
- вибір та розробка логічної топології мережі;
- вибір та розробка фізичної топології мережі;
- побудова плану прокладання кабелів;
- практичне прокладання кабельної інфраструктури;
- термінування кабельних сегментів;
- підключення пасивного та активного мережевого обладнання;

- тестування підключеного пасивного та активного обладнання;
- налаштування активного мережевого обладнання;
- тестування розробленої мережі на фізичному рівні;
- тестування конфігурацій мережевого обладнання та сервісів.

На етапі розробка технічної документації до проекту необхідно [3]:

- оформити технічну документацію;
- розробити інструкції з експлуатації мережі.

1.1.7 Порядок контролю та прийому

Тестування основних технічних характеристик розробленої мережі на відповідність технічному завданню є наступним кроком після налаштування мережевого обладнання. Для цього застосовуються апаратні засоби, такі як сертифікований кабельний тестер 1000 Base-T, а також програмні інструменти.

Успішне завершення тестування передбачає введення мережі в експлуатацію спеціальною комісією, що складається з представників замовника та виконавця, з оформленням відповідних актів прийому-передачі.

1.2 Формулювання завдання на розробку проєкту мережі. Загальна характеристика рекламного бюро “Бум”

Основним завданням діяльності рекламного бюро “Бум” є створення, розповсюдження та просування інформації про товари, послуги, бренди або ідеї з метою впливу на цільову аудиторію та досягнення маркетингових цілей клієнтів..

Рекламне бюро “Бум” надає послуги із розробки дизайну макетів як електронної так і друкованої рекламної продукції, створення фірмового стилю, друку різних рекламно-інформаційних матеріалів, сувенірної продукції (брендовані ручки, брелоки, календарі, блокноти, кружки, текстильні вироби та ін.). Окремим напрямком діяльності бюро є виготовлення зовнішньої реклами,

а саме вивісок, об’ємних букв, рекламних щитів, білбордів, реклами на будівельних елементах.

Крім цього, в рекламному бюро “Бум” існує підрозділ web-розробки, який займається створенням електронних рекламних лендінгів, блогів, web-порталів та просуванням реклами в соціальних мережах.

Таке різноманіття напрямків роботи дозволяє рекламному бюро “Бум” бути конкурентоспроможним та займати на ринку рекламних послуг стабільне становище та сприяє його розвитку та розширенню.

У штаті підприємства 74 співробітників, які розподілені по структурних підрозділах, зображених на рисунку 1.1.

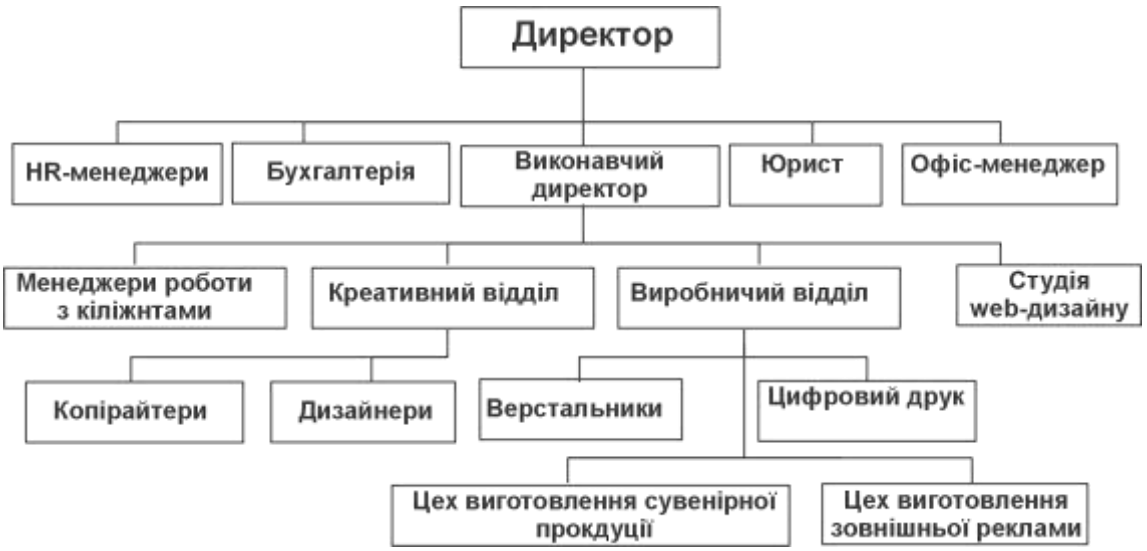


Рисунок 1.1 – Структура рекламного бюро “Бум”

Керівником рекламного бюро є директор, якому безпосередньо підпорядковується працівники адміністрації, загальною кількістю 10 осіб:

- офіс-менеджер (1 особа) здійснює забезпечення ефективної роботи офісу, управління адміністративним персоналом, документообіг, організація зустрічей, логістика, підтримка співробітників;
- юрист (1 особа);
- виконавчий директор (1 особа);
- відділ HR-менеджерів із 3 осіб, які займаються підбором кадрів рекламного бюро;

- бухгалтерія із 3 працівників, один із них головний бухгалтер;

- виконавчий директор визначає загальне креативне бачення, натхнення команди, контроль якості креативу на рівні бюро. Йому підпорядковуються чотири відділи підприємства:

- менеджери роботи із клієнтами (8 осіб) здійснюють ведення проєктів, комунікація з клієнтами, контроль бюджетів та термінів, розуміння бізнес-цілей клієнті;

- креативний відділ (18 осіб) включає команду копірайтерів (7 осіб), які здійснюють написання текстів для різних рекламних матеріалів, сценаріїв, слоганів, контенту та дизайнери (11 осіб), які займаються розробкою макетів, графічних елементів, бренд-айдентики та інше;

- студія web-дизайну (10 осіб) включає колектив Front end та Back end розробників;

- виробничий відділ (28 осіб) загальною кількістю, який складається із 10 верстальників друкованої продукції, цеху виготовлення сувенірної продукції із 7 працівників, цеху виготовлення зовнішньої реклами (10 осіб) та операторів цифрового друку (5 осіб).

Для виконання своїх щоденних професійних обов'язків співробітники рекламного бюро активно використовують комп'ютерну техніку, зокрема для таких завдань, як розробка реклами, web-контенту, підготовка фінансової звітності, ведення бухгалтерського обліку та нарахування заробітної плати.

Щоб усунути ці недоліки та підвищити продуктивність праці співробітників локального бюро пропонується впровадити локальну комп’ютерну мережу, яка надасть наступні переваги:

- швидкий доступ до файлів та ресурсів. Мережа дозволить всім авторизованим працівникам миттєво отримувати доступ до необхідних файлів, проєктної документації, креативних матеріалів, баз даних клієнтів та інших важливих ресурсів, незалежно від їхнього фізичного розташування в офісі;

- централізоване зберігання даних. Мережеві сховища (сервери) забезпечить централізоване зберігання всіх робочих файлів, що полегшить їхнє

резервне копіювання, керування версіями та спільний доступ, мінімізуючи ризик втрати важливої інформації;

- миттєвий обмін повідомленнями. Внутрішні мережеві месенджери та системи електронної пошти забезпечать швидку та зручну комунікацію між співробітниками, прискорюючи обговорення проєктів, узгодження рішень та вирішення поточних питань;

- забезпечить спільну робота над проєктами. Мережеві інструменти для спільної роботи (наприклад, хмарні сервіси, системи управління проєктами) дозволять кільком співробітникам одночасно працювати над одним документом, макетом або презентацією, підвищуючи ефективність командної роботи та скоротити час на узгодження;

- обмін креативними ідеями. Мережеві платформи та інструменти для брейнштормінгу полегшать обмін ідеями між креативними командами, незалежно від їхнього фізичного розташування, сприяючи генерації більш інноваційних та оригінальних рішень;.

- інтеграції робочих процесів. Мережа дозволяє інтегрувати різні програмні забезпечення та сервіси, що використовуються в бюро (наприклад, CRM, системи управління проєктами, графічні редактори), забезпечуючи більш злагоджений та ефективний робочий процес;

- спільне використання периферійних пристроїв. Мережа дозволить кільком користувачам спільно використовувати принтери, сканери, плотери та інше обладнання, що знизить витрати на придбання окремих пристроїв для кожного працівника;

- ефективне використання інтернет-з'єднання. Мережа забезпечить спільний доступ до інтернет-ресурсів для всіх співробітників, оптимізуючи використання пропускної здатності та знижуючи витрати на окремі підключення.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Аналіз та обґрунтування вибору топології та технології мережі

Для забезпечення ефективності та безпеки мережі, згідно з технічним завданням, буде реалізовано принцип сегментації за допомогою віртуальних локальних мереж (VLANs). Мережа буде поділена на шість віртуальних сегментів, як показано на плані приміщення (Додаток А). Маршрутизатор виконуватиме функції міжсегментної маршрутизації та шлюзу доступу до Інтернету, використовуючи віртуальні порти для взаємодії з кожним VLAN:

- Net1 – перша віртуальна підмережа повинна об’єднувати комп’ютери керівництва підприємства, а саме директора, офіс-менеджера, юриста, виконавчого директора, HR-менеджерів (разом 6 вузлів);
- друга підмережа Net2 – комп’ютери працівників бухгалтерії (3 вузли);
- Net3 – третя VLAN – менеджери роботи із клієнтами (8 осіб);
- Net4 – четверта VLAN об’єднує 7 комп’ютерів копірайтерів
- Net5 – п’ята VLAN об’єднує 11 вузлів дизайнерів друкованої продукції;
- у шосту підмережу Net6 повинні увійти 10 ПК студії web-дизайну;
- Net7 – сьома підмережа об’єднує 10 комп’ютерів верстальників;
- Net8 – восьма підмережа об’єднує 9 комп’ютерів виробничого відділу по 2 у цехах зовнішньої реклами та сувенірної продукції та 1 операторів цифрового друку та 5 мережевих принтерів.

Окрім віртуальних підмереж, проєкт мережі передбачає підключення файлового, web та DNS-серверів. Ці сервери будуть розміщені в окремому мережевому сегменті, що гарантує підвищений рівень безпеки, оскільки він не матиме прямого логічного з'єднання з VLANs робочих станцій.

Враховуючи розташування підприємства на двох поверхах будівлі, логічна сегментація мережі відображена у фізичному розміщенні: віртуальні підмережі Net3, Net4, та Net6 розгорнуті на першому поверсі будівлі, а Net2, Net5 та VLAN7 – на другому.

Крім цього, підмережа керівництва підприємства Net1 об’єднує ПК директора, офіс-менеджера, HR-менеджерів (2 вузли) розташовані на 2 поверсі та юриста і виконавчого директора на першому поверсі. Так само підмережа Net8 об’єднує 1 ПК із цеху виготовлення сувенірної продукції, 1 ПК та 5 мережевих принтерів операторів цифрового друку, розташованих на другому поверсі будівлі і 1 ПК із цеху виготовлення сувенірної продукції, 1 ПК із цеху виготовлення зовнішньої реклами та 1 ПК із цеху лазерної різки та гравіювання розташовані на 1 поверсі.

Щоб ефективно здійснити задуманий логічний поділ мережі на віртуальні підмережі, для її провідної частини (ядра мережі) буде використано фізичну топологію "ієрархічна розширена зірка". Цей вибір є найбільш прийнятним для такої архітектури.

Згідно із технічним завданням, для відвідувачів рекламного бюро у приміщені менеджерів для роботи із клієнтами слід забезпечити доступ до мережі за допомогою безпровідного середовища WiFi. Отже, мережа повинна поєднувати провідний та безпровідний сегменти. Тому в цілому фізичною топологією мережі буде гібридна топологія.

Загалом мережа нараховуватиме 60 робочих станцій та 5 мережевих принтерів, розподілених по віртуальних сегментах, деталізовано у таблиці 2.1.

Таблиця 2.1 – Кількісний розподіл робочих станцій по сегментах

Назва логічного сегменту мережі	Структурний підрозділ підприємства	Разом
1	2	3
Net1	Директор	1
	Офіс-менеджер	1
	Юрист	1
	Виконавчий директор	1
	HR-менеджери	2
Net2	Бухгалтерія	3

Продовження таблиці 2.1

1	2	3
Net3	Менеджери роботи із клієнтами	8
Net4	Копірайтери	7
Net5	Дизайнерів друкованої продукції	11
Net6	Студії web-дизайну	10
Net7	Верстальники	10
Net8	Цех зовнішньої реклами	1
	Цех лазерної порізки та гравіювання	1
	Оператори цифрового друку	1
	Цех виготовлення сувенірної продукції	2
	Мережеві принтери	5
Разом		65

Фізичне об'єднання пристроїв в одну віртуальну мережу досягається за допомогою комутаторів другого рівня OSI (Layer 2) з підтримкою VLAN, по два таких пристрої розташовані на кожному поверсі.

Виходячи з кількісного розподілу вузлів у Net1 (таблиця 2.1), стає можливим консолідувати функції центрального комутатора мережі (див. рис. 2.1) з комутатором Net1. Це досягається шляхом використання частини його 24 портів для підключення комутаторів Net2 Net8 у транковому режимі, що забезпечує економію ресурсів. Крім цього, один з портів цього центрального комутатора буде виділений для підключення до маршрутизатора, який виконуватиме маршрутизацію між усіма віртуальними мережами та

слугуватиме шлюзом для доступу в Інтернет. Файловий, DNS та web-сервери, з міркувань безпеки, будуть підключені до окремого порту маршрутизатора. Логічна схема мережі детально показана на рисунку Б.1, додатку Б.

Побудова мережевої інфраструктури базуватиметься на стандарті Gigabit Ethernet. Обґрунтуванням такого рішення є його висока поширеність на ринку, що спрощує інтеграцію. Крім того, швидкості, які надає Gigabit Ethernet, є цілком достатніми для задоволення сучасних потреб, а також забезпечується повна сумісність з раніше встановленим мережевим обладнанням, що робить цей вибір економічно доцільним та ефективним [2].

Будучи одним із провідних стандартів для локальних мереж, Gigabit Ethernet дозволяє передавати дані зі швидкістю до 1 Гбіт/с. Ця технологія широко використовується для забезпечення потреб у високій пропускній здатності, зокрема для швидкісного доступу до Інтернету та передачі відео. Стандарт базується на основі Ethernet, але включає ряд оптимізацій, що значно покращують швидкість, знижують затримки пакетів та підвищують загальну ефективність мережі. [3].

Технології Ethernet базуються на методі CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Цей принцип дозволяє кільком пристроям спільно використовувати одне середовище передачі, де кожен "слухає" мережу перед відправкою даних і при виявленні колізії, всі учасники припиняють передачу та повторюють спробу пізніше.

CSMA/CD – це набір протоколів, розроблених для ефективного використання спільного мережевого середовища. Їхня ключова функціональність полягає у "прослуховуванні" мережі перед передачею, виявленні будь-яких колізій та, за потреби, плануванні повторної передачі після випадкової затримки. [7].

Gigabit Ethernet пропонує гнучкість у виборі середовища передачі, підтримуючи як оптоволоконні кабелі (одномодові та багатомодові), так і кручену пару. Для передачі даних на великі відстані, від 550 м до 70 км, застосовується оптоволокно, що відповідає специфікаціям стандарту IEEE

802.3z, таким як 1000BaseSX, 1000BaseLX, 1000BaseLX10, 1000BaseLH, 1000BaseZX та 1000BASE-BX10.

Для створення мереж на короткі відстані (до 100 м) у межах офісу чи будівлі економічно вигіднішим є використання крученої пари. Ці рішення регламентуються специфікаціями 1000BASE-T та 1000BASE-TX. З-поміж них, 1000BASE-T є кращим вибором з точки зору вартості, оскільки, на відміну від 1000BASE-TX (що вимагає дорожчих кабелів Cat-6 та Cat-7), вона підтримує більш доступні кабелі категорій Cat-5, Cat-5e та Cat-6.

Проаналізувавши план приміщення рекламного бюро “Бум”, було встановлено, що довжина кабельних сегментів структурованої кабельної системи не перевищуватиме 100 м. Ця обставина, у поєднанні з прагненням до економічної ефективності, стала вирішальним фактором для вибору специфікації 1000BASE-T як основи мережевої інфраструктури..

Специфікація 1000BASE-T, що регулюється стандартом IEEE 802.3ab, забезпечує повнодуплексну передачу даних одночасно по всіх чотирьох парах провідників, причому кожен провідник передає сигнал в обох напрямках. Це рішення для високочастотної передачі стало можливим завдяки застосуванню сучасних сигнальних процесорів, які можуть виділяти необхідні сигнали із суміші.

2.2 Вибір кабельного середовища та розташування вузлів мережі

При розробці структурованої кабельної системи, схеми розміщення кабельних сегментів створювалися у повній відповідності до вимог замовника та загальноприйнятих стандартів СКС. Детальна схема всіх мережевих вузлів та їх взаємозв'язок та розташування на першому і другому поверхах будівлі візуалізовані відповідно на рисунках В.1 та В.2 додатку В.

У проєкті, розроблюваному в кваліфікаційній роботі, локальна мережа побудована на основі таких взаємопов'язаних компонентів:

- мережеві розетки слугують точками доступу для підключення робочих станцій та периферійних пристроїв (принтери) до локальної мережі. слід розмістити на стінах поруч із мережевими вузлами;

- комутаційна шафа є центральним пунктом для організації та розміщення активного мережевого обладнання;

- комутатори сегментів мережі виконують функцію об'єднання пристроїв у межах визначених підгруп або окремих мережевих сегментів, наприклад, для різних офісів на одному поверсі;

- головний комутатор локальної мережі виступає основним пристроєм, що з'єднує всі вузли ЛМ через відповідні комутатори сегментів. Як вже відмічалось в розділі 2.1 з метою економії коштів на розробку та враховуючи розміщення інших мережевих пристроїв головний комутатор буде інтегровано із комутатором першого сегменту мережі, куди входять пристрої підмережі керівництва підприємства;

- маршрутизатор – ключовий компонент міжмережевої взаємодії, який виконує три основні функції: маршрутизує трафік між віртуальними підмережами, слугує шлюзом для доступу до Інтернету та забезпечує надання відповідних мережевих сервісів;

- сервер, який виконують критично важливі завдання. Він надає файловий сервіс, що слугує централізованим сховищем для документів та підтримує їх обмін за протоколом FTP серед співробітників підприємства. Крім цього, на базі даного фізичного сервера слід розгорнути web-сервер для розташування web-сайту рекламного бюро “Бум” та внутрішнього тестування розробок web-студії. Ще одну функцію, яку слід встановити на фізичному сервері – роль DNS-сервера для внутрішньої адресації пристроїв в середині докальної мережі.

Загальна схема мережі з усіма її вузлами та їх взаємозв'язками представлена на рисунках В.1 та В.2 додатку В. Для побудови локальної мережі було обрано неекрановану кручену пару категорії 6.

З метою дотримання стандартного обмеження в 100 метрів між кінцевим пристроєм та мережевим комутатором, довжина основного кабельного сегмента (від розетки до патч-панелі) не повинна перевищувати 90 метрів. Залишок у 10 метрів призначений для коротких патч-кордів, що з'єднують розетку з робочою станцією та патч-панель з комутатором. Після детального аналізу схеми розміщення мережевих вузлів на плані приміщення (рисунки В.1 та В.2) можна зробити висновок, що ця схема цілком відповідає даній вимозі.

Інсталяція кабельних сегментів усередині кімнат передбачає їхнє прокладання у настінних кабельних коробах розміром 50Х40 мм, з підключенням до мережевих розеток стандарту RJ-45. Розетки слід встаноини на зручній висоті, відповідній рівню робочого столу користувача. Кабельні магістралі у коридорах будуть інтегровані у підвісні гофровані лотки з внутрішньою розділювальною перегородкою над підвісною стелею.

З метою захисту кабелю та забезпечення безпечного прокладання, перетин стін виконуватиметься в ПВХ трубках діаметром 16 мм. Місця розташування та необхідні діаметри отворів детально вказані на монтажній схемі кабельних мереж (Додаток В).

Прокладання вертикальної кабельної система між поверхами приміщення планується реалізувати у вентиляційних шафах приміщення у гофрованому ПВХ шланзі діаметром 24 мм і довжиною 6 м..

Для ефективного впорядкування мережевих кабелів, все активне мережеве обладнання серверної буде встановлено у комутаційній шафі, де також будуть задіяні патч-панелі та відповідні патч-корди.

Сегментуючі комутатори робочих груп, розташовані в приміщеннях дизайнерів, верстальників другого поверху та менеджерів для роботи із клієнтами, студії web-дизайну першого поверху (рисунки В.1 та В.2) слід розмістити на поличках закріплених на стіні.

2.3 Обґрунтування вибору комунікаційного обладнання

2.3.1 Вибір пасивного обладнання

Мережева інфраструктура включає такі пасивні компоненти:

- структуровану кабельну систему, що охоплює горизонтальні та вертикальні ділянки (з'єднання між поверхами);
- мережеві розетки RJ-45, які є точками підключення для кінцевих користувачів;
- патч-корди – короткі кабельні сегменти, що забезпечують з'єднання між розетками та портами комутаторів;
- патч-панель на 24 порти категорії 6 (висота 1U), що використовується для кросування;
- комутаційна шафа висотою 6U, призначена для розміщення мережевого обладнання;
- джерело безперебійного живлення.

При виборі кабельної системи враховуються тип і топологія мережі. Необхідні для стандарту фізичні властивості кабелю закладаються під час його виготовлення та відображаються у маркуванні. З огляду на це, сьогодні більшість мереж будуються з використанням UTP-кабелів та волоконно-оптичних ліній.

Інфраструктура локальної мережі базується на неекранованій крученій парі категорії 6. Однак, як і будь-який інший мережевий компонент, цей кабель володіє певними технічними характеристиками, а його правильне функціонування залежить від дотримання встановлених правил монтажу та експлуатації. Істотне порушення цих вимог загрожує швидким виходом кабельної системи з ладу.

Вибір кабелю для побудови горизонтальних і вертикальних сегментів мережі (що забезпечують зв'язок між поверхами) зупинено на U/UTP Cat.6 4Pr виробництва "Одескабель". Його конструктивні особливості включають [14]:

– струмопровідна жила: мідний м'який провідник;

– діаметр: 0,57 мм (23 AWG);

– діаметр провідника: 1,05 мм.;

– ізоляція: поліетилен;

– відповідність вимогам: EN 50173-1:2002, ISO/IEC 11801:2002, IEC 61156-5:2002, ANSI/TIA/EIA-568-B.2-1-2002.

Кабелі будуть горизоентальної СКС будуть під'єднуватись до мержевих розеток, характеристики яких представлено в таблиці 2.2.

Таблиця 2.2 – Розетка з екраном Cablexpert RJ-45, 6 cat, зовнішня (NCAC—HS—SMB2) [17]

Характеристика	Значення
Тип розетки	Зовнішня
Матеріал	пластик
Габарити	50x50x30мм

У якості магістрального кабелю для підключення локальної мережі до глобальної мережі Інтернет був обраний ОПТ-24А4, виготовлений фірмою "Південкабель". Цей кабель відрізняється такими конструктивними особливостями [15]:

– тип оптичного волокна: одномодовий з розширеним діапазоном хвиль;

– кількість волокон – 24;

– діаметр кабеля: 10x19±0.5 мм.

Важливим елементом мережевої інфраструктури є також блок безперебійного живлення (ДБЖ), який забезпечує безперервну роботу всіх мережевих вузлів у разі збоїв в електромережі. Для цього проєкту обрано модель APC Back-UPS Pro 1500VA. Детальні технічні характеристики даного ДБЖ можна знайти у таблиці 2.3 [12].

Таблиця 2.3 – Технічні характеристики APC Back-UPS Pro 1200VA

Кількість вихідних розеток	4
Діапазон вхідної напруги	175 - 295 В
Ефективна потужність	1200 Вт
Потужність	1500 Вт
Індикація	Так
Звукова індикація	Так
Захист телефонної лінії	Так
Час зарядки батареї	8 год
Час роботи від батареї	При повному навантаженні 15 хв
Габарити	301 x 112 x 382 мм

Для встановлення зв'язку маршрутизатора з провайдером послуг Інтернет за допомогою оптичних каналів, необхідно придбати оптичний конектор SC одномодового типу (Single-mode) з діаметром 3 мм.

Все мережеве обладнання серверної буде компактно розміщено у комутаційній шафі висотою 22U (див. рис. 2.1), що має габарити 600x600x1196 мм. Для забезпечення належної структури та функціональності, шафа включатиме патч-панелі, необхідний комутатор, блок безперебійного живлення APC 1500VA, а також кабельні організатори для зручного управління кабелями.

Рисунок 2.1 – Комутаційна шафа GEAR 6U ZT-NET AL-WDR06U-64G

Для організації та кросування мережевих з'єднань буде використано патч-панелі Panduit (19-дюймові, 24-портові, категорії 6) [15]. Ці панелі легко встановлюються в серверну шафу або стійку і постачаються з конекторами RJ-45, які не потребують спеціалізованих інструментів для підключення завдяки механізму автоматичного прорізання ізоляції провідників. Комплект поставки включає кріпильні елементи та хомути Colring, а самі патч-панелі повністю відповідають стандарту EIA/TIA 568 B.2-1.

2.3.2 Вибір активного обладнання

Активне мережеве обладнання відіграє ключову роль у функціонуванні даної локальної мережі, і включає наступні компоненти:

- маршрутизатор;
- сегментуючі та центральний комутатори;
- безпровідна точка доступу.

У локальній мережі рекламного бюро "Бум" маршрутизатор є центральним елементом, що забезпечує як функцію шлюзу доступу до Інтернету, так і маршрутизацію трафіку між дев'ятьма віртуальними підмережами, включно з окремою підмережею для сервера. З огляду на планування оптичного підключення до Інтернету та потребу у складній сегментації, ключовими критеріями для вибору маршрутизатора є його здатність підтримувати понад дев'ять VLAN, наявність SFP-порту для оптичних волокон та мінімальна швидкість передачі 1 Гбіт/с. Додатково, для ефективної роботи мережі, необхідна присутність вбудованого локального DNS-сервера.

Враховуючи поставлені вимоги до мережі рекламного бюро "Бум", було прийнято рішення зупинити вибір на маршрутизаторі DrayTek Vigor2962. Його функціональність та економічна доцільність зробили цей пристрій оптимальним рішенням. Детальні технічні характеристики Vigor2962 представлені в таблиці 2.4 [7], а його зовнішній вигляд – на рисунку 2.2.

Рисунок 2.2 – Маршрутизатор DrayTek Vigor2962

Таблиця 2.4 – Специфікація маршрутизатора DrayTek Vigor2962 [7]

Характеристика	Значення
Макс. Кількість VLAN	20
Підтримувані VLAN	802.1q Tag-на основі, на основі портів
Локальний сервер DNS	+
Пропускна здатність NAT	2.2 Гбіт/с
Маршрутизація	Статична, RIP v1/v2, BGP, OSPF
Захист від атак DoS	+
Захист від спуфінгу	+
Монтаж в стійку	1U
WAN-порт	SFP – 1 шт.
LAN-порт	Gigabit Ethernet RJ-45
Розмір (мм)	273 x 171 x 45 мм
Вартість	24 488 грн.

Далі потрібно вибрати головний комутатор та комутатор робочих. Як відзначалось у розділі 2.1 для зменшення собівартості мережі та враховуючи специфіку логічної топології мережі, функції головного комутатора покласти на сегментуючий комуатор Sw1 (див. додаток Б). До цього комутатора слід під’єданти 6 пристроїв підмережі керівництва Net1 (таблиця 2.1) та чотири інших сегментуючі комутатори. Отже, для цієї мети 24 портового комутатора цілком достатньо.

Комутатор Sw2 (див. додаток Б), розташований на 2 поверсі і об’єднує 11 ПК дизайнерів друкованої продукції та 3 вузли бухгалтерії Net2 (таблиця 2.1). Разом 14 пристроїв.

Комутатор Sw3 (див. додаток Б), розташований на 2 поверсі і об’єднує 10 ПК верстальників підмережі Net7 (таблиця 2.1), по 1 ПК цеху виготовлення сувенірної продукції, операторів цифрового друку 5 мережевих пристроїв операторів цифрового друку Net8 (таблиця 2.1). Разом 17 пристроїв.

Комутатор Sw4 (див. додаток Б), розташований на 1 поверсі і об’єднує 8 ПК і одну точку безпровідного доступу менеджерів роботи із клієнтами Net3 (таблиця 2.1), 7 ПК копірайтерів із підмережі Net4 (таблиця 2.1) та по 1 ПК юриста і виконавчого директора. Разом 18 пристроїв.

Комутатор Sw5 (див. додаток Б), розташований на 1 поверсі і об’єднує 10 ПК студії web-дизайну Net6 (таблиця 2.1), та по 1 ПК цеху лазерної порізки та гравіювання, цеху зовнішньої реклами і цеху виготовлення сувенірної продукції із Net8 (таблиця 2.1). Разом 13 пристроїв.

Отже, проаналізувавши потреби в підключенні мережевих пристроїв до кожного сегментуючого комутатора можна зробити висновок, що цілком достатньо використати комутатор на 24 порти стандарту GigabitEthernet.

Комутатор сегменту мережі відіграє ключову роль у логічному об'єднанні робочих станцій, що належать до однієї групи або відділу. Таке рішення сприяє локалізації мережевого трафіку, підвищуючи ефективність та безпеку. Для подальшого розподілу мережі на віртуальні підмережі, що відповідають окремим кімнатам або відділам підприємства, необхідно використовувати керовані комутатори другого або третього рівнів, з обов'язковою підтримкою створення щонайменше шести віртуальних мереж.

Аналіз технічних вимог та співвідношення "ціна/якість" дозволив обрати комутатор DrayTek VigorSwitch P2280 (див. рис. 2.3) для сегментації мережі рекламного бюро "Бум". Його відповідність ключовим технічним параметрам, наведеним у таблиці 2.5 [8], зробила його оптимальним рішенням.

Рисунок 2.3 – Комутатор DrayTek VigorSwitch P2280x

Таблиця 2.5 – Специфікація комутатора DrayTek VigorSwitch P2280 [8]

Характеристика	Значення
Комутаційна ємність (Гбіт/с)	12
Розмір буфера	12 Мбіт
Підтримувані VLAN	VLAN на основі тегів 802.1q VLAN на основі MAC
Макс. Кількість VLAN	256
Підтримка Spanning Tree	STP, RSTP, MSTP
Стандарти Ethernet	802.3af PoE 802.3at PoE+ 802.3u 100Base-T 802.3ab 1000Base-T 802.3ae 10GBase-X Контроль потоку 802.3x Автоматичне узгодження 802.3 VLAN на основі тегів 802.1q Клас обслуговування 802.1p 802.1d STP 802.1w RSTP 802.1s MSTP 802.3ad LACP 802.1ad QinQ Контроль доступу до портів 802.1x 802.1AB LLDP 802.3az EEE
Монтаж в стійку	1U
Порти	Gigabit Ethernet RJ-45– 24 шт.
Макс. споживана потужність	499 Вт
Розмір (мм)	441 x 270 x 44 мм
Вага	4.25 кГ
Вартість	10 750 грн.

У приміщенні менеджерів у приміщенні менеджерів по роботі із клієнтами буде розгорнута бездротова точка доступу. Це рішення є оптимальним, оскільки дозволяє пристрою, що використовуватиме Wi-Fi, також підключатися по кабелю, зберігаючи при цьому ту саму статичну IP-адресу. Такий підхід виключає необхідність використання маршрутизатора чи моста, які б лише розширювали існуючий сегмент провідної мережі на бездротовий.

Для цієї мети була обрана модель TP-LINK EAP110 (див. рис. 2.4). Вона ідеально підходить для невеликого офісу завдяки оптимальному співвідношенню технічних характеристик та вартості, а також легкості встановлення на стіну чи стелю.

Рисунок 2.4 – Точка доступу TP-LINK EAP110

Завдяки своєму стильному дизайну, що нагадує світильник, TP-LINK EAP110 легко інтегрується в офісне середовище. Ця точка доступу не потребує додаткового кабелю живлення, оскільки підтримує живлення за стандартом PoE. Важливо також, що EAP110 підтримує аутентифікацію користувачів, забезпечуючи контроль доступу.

Адміністратор мережі може ефективно керувати численними точками доступу завдяки програмному забезпеченню EAP Controller, яке забезпечує централізований контроль над бездротовими мережами. Крім того, це рішення надає моніторинг у реальному часі, можливість графічного аналізу мережевого трафіку та функцію групового оновлення прошивки.

2.4 Послідовність та особливості монтажу мережі

Монтаж локальної мережі рекламного бюро "Бум" необхідно здійснювати у кілька етапів, дотримуючись встановлених стандартів та враховуючи особливості планування приміщень. Важливо забезпечити як функціональність, так і естетичний вигляд системи.

Прокладання кабельних трас та монтаж кабельних каналів здійснюється спочатку установка настінних коробів (січенням 50х40 мм) для прокладки кабельних сегментів до мережевих розеток. Важливо дотримуватися естетичності та безпеки, забезпечуючи надійне кріплення коробів.

Це забезпечує захист кабелів від механічних пошкоджень, естетичний вигляд та зручність доступу для подальшого обслуговування чи розширення.

Короби повинні бути надійно закріплені до стін, уникнення провисань та щілин. Кабелі всередині коробів мають бути акуратно укладені, без перехрещень та сильного натягу, щоб запобігти пошкодженню ізоляції та вигинам, що перевищують допустимий радіус.

У коридорах кабелі прокладаються у підвісних гофрованих лотках (під стелею). Ці лотки повинні мати розділювальну перегородку, що дозволяє розділити силові та слаботочні кабелі, або різні групи мережевих кабелів, мінімізуючи взаємні перешкоди та покращуючи організацію.

Лотки мають бути надійно закріплені до конструкцій стелі, дотримуючись безпечних інтервалів та відстаней від інших комунікацій.

Для перетину кабелями стін обов'язково використовуються ПВХ трубки діаметром 16 мм. Це забезпечує захист кабелю від гострих країв стін, вологи та механічних впливів, а також дозволяє за потреби легше замінити кабель.

Отвори для цих трубок повинні бути просвердлені строго відповідного діаметру у місцях, що позначені на монтажній схемі кабельних мереж (додаток В), для точного та безпечного прокладання.

Мережеві розетки 8Р8С встановлюються біля робочих місць користувачів, переважно на стіні. Розетки проєктуються на рівні робочого столу

користувача комп'ютера для максимальної зручності підключення та мінімізації ризику пошкодження кабелів.

Кабелі повинні бути правильно обтиснуті та підключені до розетки згідно з обраним стандартом (наприклад, T568B), що забезпечує коректну роботу мережі.

Монтаж патч-панелей (Panduit, 19", 24 порти, кат. 6) у комутаційних шафах. Підключення прокладених кабельних сегментів до патч-панелей, використовуючи конектори з автоматичним прорізанням ізоляції провідників.

Після прокладання кабельних систем та монтажу розеток здійснюється встановлення в комутаційні шафи маршрутизатора (DrayTek Vigor2962), сегментуючого комутатора Sw1 (DrayTek VigorSwitch P2280), блоку безперебійного живлення (APC Back-UPS Pro 1500VA) та кабельних організаторів.

На наступному етапі відбувається комутація кабельних систем, яка включає:

- з'єднання портів патч-панелей з відповідними портами комутаторів за допомогою патч-кордів;
- підключення комутаторів сегментів до центрального комутатора;
- з'єднання центрального комутатора з маршрутизатором для між-VLAN маршрутизації та доступу до Інтернету;
- підключення сервера до окремого порту маршрутизатора;
- встановлення одномодового оптичного конектора SC (3 мм) на маршрутизатор для підключення до провайдера;
- розміщення бездротової точки доступу TP-LINK EAP110 у приміщенні менеджерів на стелі з використанням живлення по PoE.

Дотримання цих детальних вимог до прокладання кабелів є запорукою створення надійної, високопродуктивної та легко керованої мережевої інфраструктури для рекламного бюро "Бум".

2.5 Обґрунтування вибору програмного забезпечення

Програмне забезпечення, задіяне в проєкті локальної мережі та для виконання завдань на ПК користувачів, категоризується наступним чином:

- серверні операційні системи, що керують функціонуванням мережевих серверів;
- операційні системи для робочих станцій, які забезпечують взаємодію користувачів з ПК.
- прикладне програмне забезпечення, призначене для вирішення конкретних робочих завдань.

Для забезпечення всіх необхідних мережевих сервісів у рекламному бюро "Бум" буде потрібно встановити на сервери відповідні операційні системи. Додатково, для їхньої повноцінної роботи необхідно інтегрувати програмне забезпечення для файлового сервера (для файлового обміну), web-сервера (для розміщення web-ресурсів) та DNS-сервера.

Вибір серверної операційної системи вимагає врахування таких ключових критеріїв, як вартість, надійність, безпека систем захисту від кібератак (що є найважливішим аспектом) та періодичність оновлень. На відміну від серверних ОС, з якими працюють підготовлені адміністратори, для операційних систем робочих станцій пріоритетом є простота та зручність використання, оскільки ними користуються рядові співробітники без глибоких знань в адмініструванні. Серед найбільш поширених серверних ОС виділяються продукти на платформах: Microsoft Windows Server, Ubuntu, Debian, Red Hat Enterprise Linux та FreeBSD.

Microsoft Windows Server вирізняється насамперед універсальністю своїх серверних служб і ролей, включно з додатками, поштовими та файловими серверами. Історично його проблемним місцем була безпека, оскільки більшість вірусів розробляються саме для ПЗ Microsoft. Проте, останні версії системи значно покращили цей аспект. Головним недоліком залишається висока комерційна вартість продукту.

Debian – один з найстаріших дистрибутивів Linux, відомий своєю винятковою стабільністю. Ця ОС підтримує практично всі архітектури процесорів і може бути встановлена на більшості серверів. Ще однією перевагою є велика кількість доступних репозиторіїв (програмних пакетів) для різноманітних служб. Сама система розповсюджується безкоштовно, проте технічна підтримка є платною. Основним недоліком є дуже тривалі періоди між оновленнями, що пов'язано з ретельним і тривалим тестуванням, тому нові технології впроваджуються повільно.

Red Hat Enterprise Linux (RHEL) є лідером серед комерційних дистрибутивів Linux і є кращим вибором для багатьох великих підприємств та критично важливих інфраструктур. Його переваги зосереджені на забезпеченні стабільності, безпеки та професійної підтримки, що робить його ідеальним для серйозних бізнес-завдань.

Дана ОС розроблений спеціально для корпоративного використання. Він проходить ретельне тестування та сертифікацію, що забезпечує неперевершену стабільність і надійність, критично важливі для бізнес-додатків, що працюють 24/7. Це виражається у значному скороченні незапланованих простоїв.

Кожен реліз RHEL має передбачуваний 10-річний життєвий цикл підтримки. Це означає, що компанії можуть розгортати системи і бути впевненими, що вони отримуватимуть оновлення безпеки, виправлення помилок та технічну підтримку протягом тривалого періоду, що спрощує довгострокове планування та знижує потребу в частих міграціях.

RHEL має вбудовані, передові функції безпеки, такі як SELinux (Security-Enhanced Linux) для контролю доступу, регулярні оновлення безпеки та інструменти для дотримання нормативних вимог. Це дозволяє підприємствам відповідати суворим стандартам безпеки та ефективно захищати свої дані та системи від кіберзагроз.

Хоча RHEL є платним дистрибутивом, його стабільність, підтримка та інструменти управління можуть призвести до значної економії коштів у

довгостроковій перспективі за рахунок зменшення операційних витрат, простоїв та потреб у ручному втручанні.

Ubuntu Server є одним з найпопулярніших виборів для розгортання серверних рішень, пропонуючи значний набір переваг, особливо для компаній, що шукають баланс між функціональністю, зручністю та вартістю. Дана ОС відома своєю відносною легкістю у встановленні та налаштуванні, навіть для адміністраторів, які не мають глибокого досвіду роботи з Linux. Це досягається завдяки інтуїтивно зрозумілому інсталятору та добре документованим процесам.

Ubuntu Server має доступ до величезної кількості програмних пакетів та репозиторіїв. Це дозволяє легко встановлювати та налаштовувати різноманітні сервіси, такі як веб-сервери (Apache, Nginx), бази даних (MySQL, PostgreSQL), файлові сервери (Samba, NFS), а також спеціалізоване програмне забезпечення, що може знадобитися рекламному бюро (наприклад, для FTP-сервера, як зазначено у вашому випадку).

Canonical (компанія, що стоїть за Ubuntu) випускає регулярні оновлення, що забезпечують актуальність системи та усувають вразливості. Особливо цінними є LTS (Long Term Support) релізи, які отримують підтримку та оновлення безпеки протягом п'яти років. Це забезпечує стабільність та довгострокову надійність, що є критично важливим для серверних систем.

Сам дистрибутив Ubuntu Server є безкоштовним, що дозволяє значно заощадити на ліцензійних витратах у порівнянні з комерційними ОС. Хоча комерційна підтримка від Canonical доступна, її використання не є обов'язковим для початкового розгортання та експлуатації.

Завдяки активному співтовариству та швидкому реагуванню на виявлені вразливості, Ubuntu Server є достатньо безпечною платформою. Регулярні оновлення безпеки допомагають захистити систему від нових загроз.

Ubuntu Server може бути використаний для широкого спектру завдань – від невеликого файлового сервера до складних кластерних рішень. Його

гнучкість дозволяє адаптувати систему під конкретні потреби рекламного бюро та масштабувати її в міру зростання бізнесу.

FreeBSD є потужною, стабільною та безпечною операційною системою, яка базується на BSD-ядерній архітектурі. Вона має довгу історію розвитку та відзначається певними унікальними перевагами, що роблять її привабливим вибором для певних серверних задач.

Дана ОС відома своєю винятковою стабільністю та надійністю в роботі. Системи на FreeBSD можуть працювати роками без перезавантажень, що є критично важливим для серверів, які вимагають максимального часу безвідмовної роботи. Це досягається завдяки ретельному тестуванню та інтегрованій розробці всього стеку операційної системи (ядра та користувацьких утиліт).

На відміну від Linux, де ядро та "userland" (користувацькі утиліти) розробляються окремими проєктами, FreeBSD є цілісною операційною системою. Ядро, системні утиліти та базова система розробляються та випускаються однією командою. Це забезпечує кращу інтеграцію, узгодженість та спрощує оновлення системи.

FreeBSD має вбудовані, передові функції безпеки. Завдяки меншій "поверхні атаки" (меншій кількості компонентів у базовій системі) та ретельній розробці, вона вважається дуже безпечною платформою. Вона включає такі інструменти, як Capsicum (розширена ізоляція процесів) та інтегровані механізми аудиту безпеки.

FreeBSD пропонує потужну та гнучку систему управління програмним забезпеченням – "Ports Collection" (для компіляції з вихідного коду) та "pkg" (для встановлення бінарних пакетів). Це забезпечує доступ до тисяч додатків та сервісів, які можна легко встановити та налаштувати.

В цілому, FreeBSD є чудовим вибором для серверів, що вимагають максимальної стабільності, високої продуктивності в мережевих завданнях та надійних функцій безпеки. Вона ідеально підходить для розгортання файлових

серверів, веб-серверів, поштових серверів, брандмауерів та спеціалізованих мережевих рішень, де цілісність системи та передбачуваність є пріоритетом.

Проаналізувавши переваги та недоліки кожної розглянутої ОС прийнято рішення в якості серверної операційної системи використати FreeBSD 14.0.

FreeBSD, будучи універсальною серверною операційною системою, не має "вбудованого" або єдиного рекомендованого файлового чи веб-сервера. Натомість, вона надає користувачам гнучкість у виборі з широкого спектра програмного забезпечення, доступного через її систему портів (Ports Collection) або бінарні пакети (pkg).

В якості файлового сервера вирішено вибрати Samba. Це найпопулярніше рішення для забезпечення сумісності файлових служб з клієнтами Windows. Samba дозволяє FreeBSD серверу виступати як контролер домену, файловий сервер, сервер друку для Windows-мереж, дозволяючи користувачам Windows легко отримувати доступ до файлів. Доступний через порти (net/samba).

Для забезпечення функціоналу web-сервера вирішено використати Nginx. Останнім часом Nginx набирає популярність як високопродуктивний веб-сервер, зворотний проксі та балансувальник навантаження. Він відомий своєю ефективністю використання ресурсів та здатністю обробляти велику кількість одночасних з'єднань. На FreeBSD Nginx також доступний через порти (www/nginx).

Створення DNS-сервера на FreeBSD зазвичай включає встановлення та налаштування програмного забезпечення, що реалізує службу DNS. Найпопулярнішим DNS-сервером є BIND (Berkeley Internet Name Domain), який є стандартом де-факто для більшості Unix-подібних систем. Також можна використовувати Unbound (рекурсивний кешуючий DNS-сервер) або DNSmasq (легкий DNS/DHCP-сервер).

Вирішено використати BIND як на найбільш повнофункціональне рішення для створення авторитетного DNS-сервера.

Для робочих станцій необхідно обрати операційну систему, яка буде максимально зручною для рядових співробітників видавництва, а також гарантуватиме повну сумісність та ефективну роботу зі спеціалізованим прикладним програмним забезпеченням, що є критично важливим для видавничого процесу.

Ще одним ключовим фактором при виборі операційної системи для робочих станцій є рівень володіння нею персоналом. Важливо оцінити кількість співробітників, які мають практичні навички роботи на різних платформах ОС, щоб забезпечити ефективність та мінімізувати потребу в додатковому навчанні.

Проаналізувавши ці критерії, було вирішено використовувати платформу Windows для операційних систем робочих станцій. Враховуючи характеристики апаратного забезпечення та терміни підтримки оновлень [12], пропонується 64-розрядна версія Microsoft Windows 11 Pro.

2.6 Розподіл адресного простору та поділ мережі на віртуальні підмережі

Відповідно до технічного завдання замовника, для мережі рекламного бюро "Бум" надається IP-адреса 192.168.1.0/24, яка передбачає використання до 254 мережевих адреси, що для даної мережі із 65 кінцевих вузлів цілком достатньою. Цю адресу необхідно сегментувати на дев'ять віртуальних підмереж, з урахуванням виділення окремої підмережі для сервера. В таблиці 2.6 представлено потреби у виділенні IP-адрес мережевих вузлів із врахуванням необхідності однієї додаткової адреси для мережевого шлюзу.

Таблиця 2.6 – Необхідна кількість IP-адрес в підмережах

Net1	Net2	Net3	Net4	Net5	Net6	Net7	Net8	Serv
6+1=7	3+1=4	8+1=9	7+1=8	11+1=12	10+1=11	10+1=11	10+1=11	1+1=2

Крім представленого в таблиці переліку підмереж необхідно створити ще одну, десяту, підмережу для гостьової Wi-Fi зони, яку згідно із технічним завданням слід організувати у приміщенні відділу менеджерів для роботи із клієнтами. Враховуючи пропускну здатність приміщення відділу та забезпечення усіх потенційних клієнтів окремою адресою вирішено виділити 20 IP-адрес для гостьової підмережі із назвою WiFi.

Для ефективного управління адресним простором та його економії, поділ мережі на підмережі буде виконано за допомогою маски змінної довжини (VLSM). Таке рішення передбачає використання методу безкласової міждоменної маршрутизації (CIDR).

Щоб ефективно використовувати адресний простір і запобігти перекриттю підмереж, маски змінної довжини визначатимуться, починаючи з тих підмереж, які потребують найбільшої кількості вузлів. Згідно із даними таблиці 2.6 та аргументованим виділення IP-адрес для гостьової Wi-Fi-підмережі найбільша за кількістю адрес підмережа саме WiFi і становить 21 адресу (включаючи шлюз). Для забезпечення такої кількості потрібно із частини мережевої адреси, що відповідає за адресацію вузлів виділити 5 бітів, оскільки $2^5 = 32$ найближче число більше за необхідну максимальну кількість IP-адрес. Отже, на адресу мережі залишається 27 бітів. Відповідно маска такої мережі в бітовому представлені буде:

11111111. 11111111. 11111111.11100000,

або в десяткових числах:

255.255.255.224

Отже, адресу підмережі WiFi можна записати у вигляді 192.168.1.0/27. Адресний простір для безпровідних пристроїв буде 192.168.0.1 до 192.168.0.30, а широкосмугова адреса 192.168.1.31/27. В таблиці 2.7 представлено інформацію про IP-адресу підмережі WiFi, діапазон допустимих адрес для вузлів та бродкест запитів.

Таблиця 2.7 – Розрахунок адресного простору для підмереж

Назва підме-режі	Необхід. к-сть адрес	Обчислення останнього октету	Доступ к-сть адрес	Адреса підмережі	Діапазон адрес для вузлів	Широкосму-гова адреса
1	2	3	4	5	6	7
WiFi	21	256-32=224	30	192.168.1.0/ 27	192.168.1.1 – 192.168.1.30	192.168.1.31
Net5	12	256-16=240	14	192.168.1.32/ 28	192.168.1.33 – 192.168.1.46	192.168.1.47
Net6	11	256-16=240	14	192.168.1.48/ 28	192.168.1.49 – 192.168.1.62	192.168.1.63
Net7	11	256-16=240	14	192.168.1.64 /28	192.168.1.65 – 192.168.1.78	192.168.1.79
Net8	11	256-16=240	14	192.168.1.80 /28	192.168.1.81 – 192.168.1.94	192.168.1.95
Net3	9	256-16=240	14	192.168.1.96 /28	192.168.1.97– 192.168.1.110	192.168.1.111
Net4	8	256-16=240	14	192.168.1.112 /28	192.168.1.113 – 192.168.1.126	192.168.1.127
Net1	7	256-16=240	14	192.168.1.128 /28	192.168.1.129 – 192.168.1.142	192.168.1.143
Net2	4	256-8=248	6	192.168.1.144 /29	192.168.1.145 – 192.168.1.150	192.168.1.151
Serv	2	256-4=252	2	192.168.1.152 /30	192.168.1.153 – 192.168.1.154	192.168.1.155

Відповідно до даних таблиці 2.6 наступна за кількістю адрес буде підмережа Net5 із 12 адрес. Найближчий мінімальний блок адрес становить 2^4=16. Шляхом віднімання 16 від 256 отримуємо останній октет маски підмережі, що дорівнює 240. Отже, маска підмережі: 255.255.255.240. Це

означає, що в останньому октеті маски підмережі чотири старших біти використовуються для підмережі, а не для адреси хоста. Отже, адреса підмережі Net5 буде 192.168.1.32/28. Адресний простір для мережевих вузлів буде 192.168.1.33 до 192.168.1.46, а широкосмугова адреса 192.168.1.47/28.

Згідно із даними таблиці наступними за кількістю вузлів є відразу три підмережі Net6, Net7 та Net8 із 11 адрес. Найближчий мінімальний блок адрес, щоб забезпечив цю кількість теж 2^4=16. Відповідно в останньому октеті маски теж число 256-16=240, і маски цих підмереж 255.255.255.240. Тобто, для маски в останньому октеті буде забрано чотири біти. Оскільки, кількості IP-адрес в них однакова, то встановимо адреси цих підмереж в порядку слідування їх номерів, тому мережі Net6 буде 192.168.1.48/28, Net7 – 192.168.1.64/28 та Net8 – 192.168.1.80/28. Результати розрахунку розподілу адресного простору для мережевих вузлів цих мереж та широкосмугових адрес відображено в таблиці 2.7. Подібним чином слід розрахувати адресний простір для решту підмереж, що представлені в таблиці 2.6.

Наступна за кількістю вузлів, згідно із таблицею 2.6 є підмережа Net3 із 9 IP-адрес. Найближчий мінімальний блок адрес, щоб забезпечив цю кількість теж 2^4=16. Відповідно в останньому октеті маски теж число 256-16=240, і маски цих підмереж 255.255.255.240. Отже, адреса підмережі Net5 буде 192.168.1.96/28/ Розподіл адресного простору для мережевих вузлів представлено в таблиці 2.7.

Далі за кількістю вузлів, згідно із таблицею 2.6 є підмережа Net1 із 7 IP-адрес. Найближчий мінімальний блок адрес, щоб забезпечив цю кількість теж 2^4=16, оскільки, враховуючи резервування двох IP-адрес для самої підмережі та бродкесту 2^3=8 не достатньо. Отже, адреса підмережі Net1 буде 192.168.1.128/28, розподілу адресного простору для мережевих вузлів представлено в таблиці 2.7.

Наступною за кількістю вузлів, згідно із таблицею 2.6 є підмережа Net2 із 7 IP-адрес. Найближчий мінімальний блок адрес, щоб забезпечив цю

кількість 2^3=8. Отже, адреса підмережі Net2 буде 192.168.1.144/29, розподілу адресного простору для мережевих вузлів представлено в таблиці 2.7.

Останньою за кількістю необхідний IP-адрес є підмережа сервера рівна 2 адресам. Найближчий мінімальний блок адрес, щоб забезпечив цю кількість теж 2^2=4. Шляхом віднімання 4 від 256 отримуємо останній октет маски підмережі, що дорівнює 252. Отже, маска підмережі: 255.255.255.252 Це означає, що в останньому октеті маски підмережі шість старших бітфі використовуються для підмережі, а не для адреси хоста. Отже, адреса підмережі Serv буде 192.168.1.152/30. Розподіл адресного простору для мережевих вузлів представлено в таблиці 2.7.

Адресний простір від 192.168.1.157 до 192.168.1.254 (разом 98 адрес) не використовується і буде зарезервований на випадок розширення мережі.

2.7 Тестування та налагодження мережі

Ефективне функціонування локальної мережі залежить від бездоганного налаштування та відповідності стандартам усіх її компонентів: від мережевих пристроїв до робочих станцій і серверів. Проте, навіть при ідеальній конфігурації, несподівані чинники можуть впливати на продуктивність, не обов'язково викликаючи очевидні помилки. Для запобігання таким явищам і підтримки оптимальної роботи мережі необхідна систематична діагностика, тестування та профілактичне обслуговування.

Причини збоїв і проблем у мережі зазвичай зводяться до чотирьох основних категорій:

- несправності фізичного підключення (кабелі);
- помилки у роботі мережевих протоколів;
- надмірне навантаження на мережу;
- дефекти в програмному забезпеченні..

Несправності в кабельній системі стосується фізичного рівня мережі – кабелів, конекторів, патч-панелей та іншого обладнання, що забезпечує

фізичне з'єднання між пристроями. Проблеми на цьому рівні є одними з найпоширеніших і часто найпростіших для діагностики, але можуть викликати повну відсутність зв'язку.

Пошкодження кабелю може бути пов’язане:

- повне переривання кабельного з'єднання, спричинене механічними пошкодженнями (перегин, розтягнення, перерізання, пошкодження гризунами) або виробничими дефектами. Призводить до повного відключення пристрою або сегмента мережі;

- пошкодження ізоляції може призвести до коротких замикань або перехресних перешкод (cross-talk), що викликає зниження швидкості, нестабільність з'єднання або помилки передачі даних;

- перевищена довжина: кабелю, можуть призвести до ослаблення сигналу (затухання) та втрати пакетів, що проявляється у нестабільній роботі або зниженій швидкості.

- проблеми з конекторами (RJ-45):

- порушення стандарту обтискання (T568A або T568B) або неправильний контакт жил у конекторі. Це може призвести до відсутності з'єднання, зниження швидкості (наприклад, працює тільки на 100 Мбіт/с замість 1 Гбіт/с) або періодичних обривів;

- поганий контакт пов’язаний із забрудненням, окислення, деформацією або ослаблення контактів у роз'ємі призводить до нестабільного з'єднання.

Несправності патч-панелей та розеток:

- неправильне забивання кабелю в роз'єм патч-панелі або розетки, що створює поганий контакт;

- фізичні пошкодження портів на комутаторах, маршрутизаторах, мережевих картах або патч-панелях.

Діагностика несправностей в кабельній системі:

- перевірка фізичних пошкоджень кабелів та конекторів;

- використання спеціальних пристроїв для перевірки цілісності кабелю, правильності обтискання, наявності обривів або коротких замикань. Деякі

тестери можуть вимірювати довжину кабелю та визначати відстань до несправності;

- перевірка світлодіодних індикаторів на мережевих картах, комутаторах та роутерах – вони повинні світитися, вказуючи на фізичне з'єднання (Link) та активність (Activity);

- використання команд ping та ipconfig для перевірки наявності IP-адреси та базового зв'язку з іншими пристроями в мережі.

Проте слід відзначити, що навіть при ідеальному фізичному з'єднанні, неправильна конфігурація або збої в роботі протоколів можуть повністю паралізувати мережу або її частину.

Некоректне функціонування мережевих протоколів може бути спричинене:

- неправильною IP-адресацією. Дублювання IP-адрес (коли два пристрої мають однакову IP-адресу в одній мережі), використання IP-адреси поза допустимим діапазоном підмережі, або призначення недійсної адреси призводить до конфліктів IP-адрес, відсутності зв'язку або нестабільної роботи;

- неправильна маска може призвести до того, що пристрої не зможуть зв'язуватися з іншими пристроями в тій же підмережі або з пристроями в інших підмережах;

- неправильно вказаний шлюз за замовчуванням (Default Gateway) приводить до того , що пристрої не зможуть вийти за межі своєї локальної підмережі;

- неправильні DNS-сервери призводять до того що пристрої не зможуть розпізнавати доменні імена, хоча доступ за IP-адресою може працювати. Це робить використання багатьох сервісів неможливим;

- Неправильно налаштовані маршрути у таблицях маршрутизації. В цьому випадку маршрутизатори направляють трафік неправильним шляхом, що призводить до втрати пакетів або затримок.

Перевантаження виникає, коли обсяг трафіку в мережі перевищує її пропускну здатність. Це не обов'язково призводить до повного відключення,

але значно знижує продуктивність мережі, викликаючи затримки, втрату пакетів та повільну роботу додатків.

Причиною перевантаження може бути надмірна кількість широкомовного трафіку в мережі, спричинена несправним мережевим адаптером, програмною помилкою, петлею в мережі без протоколу STP (Spanning Tree Protocol) або DoS-атакою. Також таке явище може бути спричинене масовою передачею великих файлів, потокового відео високої якості, інтенсивне використання хмарних сервісів, програм для резервного копіювання або синхронізації файлів, дія в мережі вірусів черв’яків та шкідливих програм.

Проблеми можуть виникнути на рівні операційних систем, мережевих драйверів, додатків або системного програмного забезпечення, що працює в мережі.

Додатки, які інтенсивно використовують мережу, можуть мати помилки, що призводять до витоків пам'яті, надмірного споживання ресурсів або неправильного форматування даних, що викликає проблеми в мережі. Додаток неправильно налаштований для роботи з мережевими сервісами або базами даних.

Віруси, черв'яки або ботнети, які генерують великий обсяг мережевого трафіку для атак або поширення.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування мережевих серверів

3.1.1 Інструкції з налаштування файлового сервера

Встановлення файлового сервера Samba на FreeBSD 14 дозволяє обмінюватися файлами між комп'ютерами з різними операційними системами (в даному випадку клієнтськими машинам Windows) у локальній мережі.

Перед встановленням сервера потрібно оновити індекси пакетів, щоб переконатися, що адміністратор отримує останні доступні версії. Для цього слід ввести команду:

admin@server:~ % sudo pkg update

Далі потрібно встановити Samba 4 за допомогою менеджера пакетів pkg командою [10]:

admin@server:~ % sudo pkg install samba419

де samba419 – це назва встановлюваного пакету (Samba 4) та його поточна версія – 19.

Після успішного встановлення пакету сервера, необхідно відредагувтаи його конфігураційний файл. Файл конфігурації Samba зазвичай знаходиться за адресою /usr/local/etc/smb4.conf. Якщо його немає після встановлення, він може бути згенерований автоматично при першому запуску програми, або можна створити його вручну командою:

admin@server:~ % sudo nano /usr/local/etc/smb4.conf

В даному випадку для редагування конфігураційного файлу використовується текстовий редактор nano.

У файлі слід перейти до розділу [global] і ввести наступні налаштування [10]:

[global]

workgroup = Bum; назва робочої групи, яка буде відображатися в мережі Windows

security = admin; використовувати аутентифікацію за користувачами

passdb backend = tdbsam; спосіб зберігання паролів Samba (tdbsam - рекомендовано)

load printers = yes ; увімкнути спільний доступ до принтерів

log file = /var/log/samba/log.%m ; аайл журналу для Samba

max log size = 50 ; максимальний розмір файлу журналу (в МБ)

dns proxy = no; Вимкнути проксі DNS;

interfaces = re0 192.168.1.153/30; sказати мережевий інтерфейс та мережу (див. таблиця 2.7)

;bind interfaces only = yes; прив'язати Samba тільки до вказаних інтерфейсів.

Також в конфігураційному файлі слід створити окремий розділ для спільного каталогу де будуть зберігатися файли користувачів мережі рекламного бюро “Бум”. Наприклад, для каталогу /home/samba_share потрібно ввести наступну інформацію [10]:

[myshare]

comment = My Samba Share

path = /home/samba_share

browseable = yes

read only = no

guest ok = no; вимкнути гостьовий доступ

valid users = user1, @sambagroup; дозволити доступ тільки певним користувачам або групі

create mask = 0664; права доступу для нових файлів

directory mask = 0775; права доступу для нових каталогів

На наступному кроці потрібно створити відповідний спільний каталог і і вказати відповідні права доступу для користувачів. Для цього вводимо команди [10]:

admin@server:~ % sudo mkdir -p /home/samba_share

admin@server:~ % sudo chown -R root:wheel /home/samba_share #

Або іншого користувача/групи, якій належить папка [10]:

admin@server:~ % sudo chmod -R 775 /home/samba_share

На четвертому етапі необхідно створити системних користувачів Samba:

Користувачі Samba повинні існувати як системні користувачі на FreeBSD. Якщо користувач user1 вже існує, т цей крок слід пропустити. Якщо ні, то необхідно ввести команду [10]:

admin@server:~ % sudo adduser user1

Далі необхідно слідувати підказкам і ввести його пароль та інші персональні дані.

Після створення системних користувачів, їх потрібно додати до бази даних користувачів Samba командою [10]:

admin@server:~ % sudo smbpasswd -a user1

Буде запропоновано ввести та підтвердити пароль для Samba. Цей пароль може відрізнятися від пароля системного користувача.

На п’ятому етапі потрібно увімкнення Samba в автозавантаження. Для цього слід відкрити конфігураційний файл rc.conf [10]:

admin@server:~ % sudo nano /etc/rc.conf

Тоді додати наступний рядок:

samba_server_enable="yes"

Для завантаження служби Samba вручну необхідно ввести [10]:

admin@server:~ % sudo service samba_server start

Щоб переконатися, що Samba запущена та працює слід ввести:

admin@server:~ % sudo service samba_server status

Якщо увімкнений фаєрвол (IPFW або PF), то потрібно дозволити трафік Samba Для IPFW слід додати правила для портів Samba (137/udp, 138/udp, 139/tcp, 445/tcp) в конфігураційному файлі rc.conf слід ввести [10]:

firewall_enable="yes" firewall_script="/etc/ipfw.rules"

Створити або відредагуйте файл /etc/ipfw.rules командою

admin@server:~ % sudo nano /etc/ipfw.rules

У файлі слід ввести наступний скрипт [10]:

#!/bin/sh # Дозволити loopback інтерфейс

/sbin/ipfw -q add 10 allow all from any to any via lo0

Дозволити Samba

/sbin/ipfw -q add 100 allow udp from any to any dst-port 137,138

/sbin/ipfw -q add 101 allow tcp from any to any dst-port 139,445

Дозволити вихідні з'єднання

/sbin/ipfw -q add 500 allow tcp from any to any out via ${ext_if} setup keep-state

/sbin/ipfw -q add 501 allow udp from any to any out via ${ext_if} keep-state

Заборонити все інше

/sbin/ipfw -q add 65535 deny all from any to any

Далі необхідно зробити скрипт виконуваним:

admin@server:~ % sudo chmod +x /etc/ipfw.rules.

Після цього запустити фаєрвол:

admin@server:~ % sudo service ipfw start.

На цьому налаштування файлового севрера Samba завершено.

3.1.2 Інструкції з налаштування DNS-сервера

Налаштування DNS-сервера на FreeBSD 14 передбачає використання BIND, який є найпопулярнішою реалізацією протоколу DNS. Можна налаштувати BIND як кешуючий DNS-сервер, авторитетний DNS-сервер (для домену рекламного бюро “Бум”), або комбінацію.

Хоча базова система FreeBSD містить деяку функціональність BIND, рекомендується встановити повний пакет BIND з Ports або pkg для найновішої версії та всіх необхідних інструментів. Для цього спочатку рекомендується обновити індекси пакетів командою:

admin@server:~ % sudo pkg update

Після цього слід встановити пакет BIND ввівши команду;

@server:~ % sudo pkg install -y bind919 bind-tools

де bind919 – основний пакет сервера BIND;

bind-tools – містить утиліти, такі як dig, host, nslookup, rndc для тестування та керування DNS.

Після встановлення пакету необхідно здійснти базові налаштування сервера.

На першому кроці необхідно переконатися, що сервер має правильне ім'я хоста. Для цього слід відкрити для редагування файл rc.conf:

@server:~ % sudo nano /etc/rc.conf

У файлі слід знайти запис hostname і додати або змінити ім’я сервера:

hostname="server.bum.com.ua"

Далі потрібно налаштувати файлу /etc/hosts ввівши команду редагування:

@server:~ % sudo nano /etc/hosts

У файлі необхідно додати IP-адресу та ім'я хоста сервера:

127.0.0.1 localhost localhost.bum.com.ua

192.168.1.153 server.bum.com.ua server

На наступному етапі необхідно налаштувати параметри у файлі /etc/resolv.conf, що визначає DNS-сервери, які система буде використовувати для визначення імен. Щоб BIND міг запускатися та вирішувати завдання DNS слід вказати спочатку сторонні кореневі сервери (наприклад, Google Public DNS або DNS провайдера). Після успішного налаштування BIND, можна змінити їх, на локальний DNS-сервер (127.0.0.1).

Отже, необхідно ввести команду

@server:~ % sudo nano /etc/resolv.conf

Та у файлі, що відкриється ввести наступні параметри:

nameserver 8.8.8.8

nameserver 8.8.4.4

search boom.com.ua

Основний файл конфігурації BIND — /usr/local/etc/namedb/named.conf. BIND зазвичай запускається в chroot-середовищі за замовчуванням для безпеки. Конфігураційні файли розташовані в /usr/local/etc/namedb/.

Стандартний файл named.conf, що створює BIND слід скопіювати та відредагувати:

@server:~ % sudo cp /usr/local/etc/namedb/named.conf.sample /usr/local/etc/namedb/named.conf

@server:~ % sudo chown bind:bind /usr/local/etc/namedb/named.conf

Відкриваємо файл для редагування:

sudo nano /usr/local/etc/namedb/named.conf

Конфігураційному файл named.conf в якості кешуючого DNS-сервера слід ввести наступний текст [10]:

```
options {
    directory "/usr/local/etc/namedb";      // Каталог для файлів зон
    pid-file "/var/run/named/named.pid";   // Шлях до PID-файлу
    dump-file "/var/dump/named_dump.db";   // Файл для дампів бази даних
    statistics-file "/var/stats/named.stats"; // Файл статистики
    allow-query {127.0.0.1; 192.168.1.0/30; };// Дозволити запити з будь-лише з локальної мережі
   listen-on {127.0.0.1; 192.168.1.152; }; // Слухати на локальному та зовнішньому IP-адресах // 192.168.1.143 – IP-адреса даного сервера
    recursion yes;  // Дозволити рекурсивні запити (для кешуючого сервера)
    forwarders {
      8.8.8.8;    // DNS-сервер Google (або ваш провайдер)
      8.8.4.4;
    };
    forwarders {}; // Сервер сам вирішуватиме імена;
    dnssec-enable yes;  // Увімкнути DNSSEC (рекомендується для безпеки)
    dnssec-validation auto; // Автоматична перевірка DNSSEC
    managed-keys-directory "/usr/local/etc/namedb/keys";
};
// Оголошення кореневих серверів (named.root)
zone "." IN {
```

```
    type hint;
    file "named.root";
};
// Зона для localhost (пряма)
zone "localhost" IN {
    type master;
    file "master/localhost.rev"; // Файл зони для localhost
    allow-update { none; };
};
// Зона для 127.0.0.1 (зворотна)
zone "127.in-addr.arpa" IN {
    type master;
    file "master/127.0.0.1.rev"; // Файл зворотної зони для 127.0.0.1
    allow-update { none; };
};
```

BIND потребує файлів зон для вирішення імен. Файл named.root містить список кореневих DNS-серверів. Цей файл вже є у /usr/local/etc/namedb/. Можна оновити його, якщо він застарілий командою:

@server:~ % sudo dig @a.root-servers.net . NS > /usr/local/etc/namedb/named.root

@server:~ % sudo chown bind:bind /usr/local/etc/namedb/named.root

Файли зон localhost та 127.0.0.1 переважно вже існують або їх потрібно створити в каталозі master всередині /usr/local/etc/namedb/[10]:

@server:~ % sudo mkdir -p /usr/local/etc/namedb/master

@server:~ % sudo chown bind:bind /usr/local/etc/namedb/master

Після налаштування вищеописаних конфігураційних файлів слід замінbти власника файлів зон на bind:bind:

@server:~ % sudo chown bind:bind /usr/local/etc/namedb/master/*

Для того щоб сервер був авторитетним для власного домену (наприклад, boom.com.ua), потрібно додати відповідні зони до named.conf та створити файли зон.

До файлу named.conf потрібно додати пряму зону [10]:

```
zone "boom.com.ua" IN {
   type master;
   file "master/db.your_domain.com";
   allow-update { none; };
};
```

До файлу named.conf потрібно додати зворотну зону [10]:

```
zone "1.168.192.in-addr.arpa" IN {
   type master;
   file "master/db.192.168.1";
   allow-update { none; };
};
```

1.168.192.in-addr.arpa є зворотним записом для мережі 192.168.1.0/24.

Далі потрібно змінити власника файлів зон:

@server:~ % sudo chown bind:bind /usr/local/etc/namedb/master/db.boom.com.ua

@server:~ % sudo chown bind:bind /usr/local/etc/namedb/master/db.192.168.1

Після налаштування конфігурації потрібно прописати автоматичне завантаження BIND при запуску системи. Для цього слід відкрити для редагування файл /etc/rc.conf [10]:

@server:~ % sudo nano /etc/rc.conf

І додати в ньому наступний рядок до /etc/rc.conf:

named_enable="YES"

Для запуску служби BIND в ручному режимі слід ввести команду [10]:

@server:~ % sudo service named start

Перевірка статусу:

@server:~ % sudo service named status

Ви повинні побачити, що named запущено.

Якщо у системі увімкнений фаєрвол, то потрібно дозволити трафік для DNS (порт 53 UDP/TCP).

Для цього слід відредагувати конфігураційних файл фаєрвола []:

@server:~ % sudo nano /etc/ipfw.rules

І ввести наступний текст [10]:

add 100 allow udp from any to any dst-port 53

add 101 allow tcp from any to any dst-port 53

Перезавантажити фаєрвол [10]:

@server:~ % sudo service ipfw restart

3.1.3 Інструкції з налаштування web-сервера

Для розгортання web-сервера Nginx у FreeBSD спочаткук його потрібно проінтсалювати командою [10]:

@server:~ % sudo pkg update

@server:~ % sudo pkg install -y nginx

Після встановлення Nginx потрібно відредагувати основний файл конфігурації Nginx, що знаходиться за адресою /usr/local/etc/nginx/nginx.conf.

Для цього слід його відкрити у редакторі nano [10]:

@server:~ % sudo nano /usr/local/etc/nginx/nginx.conf

У файлі що відкриється потрібно ввести наступні налаштування [10]:

worker_processes auto; # Кількість робочих процесів (auto - за кількістю ядер CPU)

events {

worker_connections 1024; # Максимальна кількість одночасних з'єднань

}

http {

include mime.types; # Типи MIME файлів

default_type application/octet-stream;

```
sendfile        on;          # Використовувати sendfile для оптимізації
keepalive_timeout  65;       # Час утримання з'єднання
# Конфігурація для віртуального хоста (сервера)
server {
   listen       80;          # Слухати на порті 80 (HTTP)
   server_name  boom.com.ua;   # Ім'я домену сервера
   # Кореневий каталог для веб-сайту
   root   /usr/local/www/nginx; # Де будуть розміщені веб-файли
   # Індекси файлів (файли, які Nginx шукатиме, якщо запит на каталог)
   index  index.html index.htm;
   # Блокування доступу до прихованих файлів (наприклад, .htacess)
   location ~ /\. {
      deny all;
   }
   # Конфігурація для помилок
   error_page   500 502 503 504  /50x.html;
   location = /50x.html {
    root   /usr/local/www/nginx-dist; # Каталог для сторінок помилок
   }
```

Щоб Nginx запускався автоматично при завантаженні системи, слід відкрити для редагування файл /etc/rc.conf [10]:

@server:~ % sudo nano /etc/rc.conf

І додати в ньому наступний рядок до /etc/rc.conf:

nginx_enable="YES"

Далі необхідно запустити службу Nginx в ручному режимі [10]:

@server:~ % sudo service nginx start

Якщо у увімкнений фаєрвол, то потрібно дозволити вхідний трафік на порт 80 (HTTP) та порт 443 (HTTPS, для використання SSL/TLS). Потрібно виконати дії аналогічні для додавання порту 53 для DNS описаного у розділі 3.1.2.

3.2 Інструкції з налаштування комутаторів та маршрутизації між VLAN

Після налаштування сервера необхідно здійснити налаштування активного мережевого обладнання. Цей процес розпочнемо з налаштування комутаторів, що обслуговують окремі сегменти мережі.

Процес налаштування комутаторів передбачає визначення їхніх унікальних імен, конфігурацію інтерфейсів для ефективної взаємодії з VLAN-ами, а також імплементацію надійних заходів безпеки, таких як паролі для аутентифікації.

Налаштування комутаторів DrayTek VigorSwitch P2280 зазвичай здійснюється через веб-інтерфейс (GUI) або командний рядок (CLI) за допомогою Telnet або SSH.

Спочатку необхідно підключити комп'ютер до будь-якого порту комутатора DrayTek VigorSwitch P2280. За замовчуванням VigorSwitch P2280 має IP-адресу 192.168.1.224. Отже, слід ввести команду

telnet 192.168.1.224

Автоматично потрапляємо в користувацький режим комутатора. Щоб вказати його ім’я потрібно ввести наступні команди [10]:

p2280>enable

p2280#configure terminal

p2280(config)#hostname Sw1

Sw1(config)#

Далі потрібно створити самі VLAN-и. Кожен VLAN ідентифікується унікальним ID (VLAN ID).

Спочатку необхідно створити базу даних. Для цього у DrayTek VigorSwitch необхідно ввести наступні команди [8]:

Sw1(config)#vlan database

Sw1(config-vlan)#vlan 101 name Net1

Sw1(config-vlan)#vlan 102 name Net2

```
Sw1(config-vlan)#vlan 103 name Net3
Sw1(config-vlan)#vlan 104 name Net4
Sw1(config-vlan)#vlan 105 name Net5
Sw1(config-vlan)#vlan 106 name Net6
Sw1(config-vlan)#vlan 107 name Net7
Sw1(config-vlan)#vlan 108 name Net8
Sw1(config-vlan)#vlan 109 name Serv
Sw1(config-vlan)#vlan 109 name WiFi
Sw1(config-vlan)#exit
Sw1(config)#exit
Sw1#write memory
```

Процес створення VLAN на комутаторі Sw1 починається з переходу в режим глобального конфігурування vlan. Для цього слід ввести команду “vlan database”. Далі для кожної віртуальної мережі необхідно ввести команду “vlan <номер> name <назва>”, де <номер> та <назва> відповідають даним з таблиці 3.1.

Таблиця 3.1 Назви та номери підмереж VLAN

Підрозділ	Під’єднано до комутатора	Назва VLAN	Номер VLAN
Керівництво	Sw1, Sw4	Net1	101
Бухгалтерія	Sw2	Net2	102
Менеджери роботи із клієнтами	Sw4	Net 3	103
Копірайтери	Sw4	Net4	104
Дизайнери	Sw2	Net5	105
Студії web-дизайну	Sw5	Net6	106
Верстальники	Sw3	Net7	107
Виробничий відділ	Sw3	Net8	108
Сервер	R1	Serv	109
Гостьова	Sw4	WiFi	110

Наступний крок – вибір типів портів комутатора, задіяних у функціонуванні VLAN. Інтерфейси, що прямо підключаються до комп'ютерів, які належать до певного VLAN, конфігуруються як access-порти. Це пов'язано з тим, що вони призначені для прийому та відправлення нетегованого трафіку лише однієї віртуальної мережі. Водночас, для з'єднання комутаторів між собою або з маршрутизатором, порти слід визначити як trunk-порти, оскільки вони необхідні для передачі тегованих пакетів з усіх VLAN-ів.

Для конфігурації портів комутатора Sw1 слід увійти в режим глобального конфігурування. Зважаючи на те, що всі комп'ютери віртуальної підмережі 101 (як показано на Рисунку Б.1) входять до єдиного VLAN, інтерфейси GigabitEthernet, що з'єднують їх з ПК, слід налаштувати як access-порти для VLAN 101 [8]:

```
Sw1(config)# interface range ethernet 1/1 - 1/4
Sw1(config-if-range)# switchport mode access
Sw1(config-if-range)# switchport access vlan 101
Sw1(config-if-range)#exit
Sw1(config)# interface range  ethernet 1/11 - 1/14
Sw1(config-if-range)# switchport mode trunk
Sw1(config-if-range)#exit
Sw1(config)# interface ethernet 1/24
Sw1(config-if)# switchport mode trunk
Sw1(config-if)#exit
```

Завершальним кроком у налаштуванні комутатора після конфігурації портів є встановлення парольної аутентифікаці

Використовується три рівні парольного захисту це паролі на консольний доступ до пристрою, віддалений доступ по SSH або TelVLAN і пароль на вхід до привілейованого режиму.

Для введення паролю на комутатор слід ввести комана:

```
Sw1(config)# username admin password <пароль> level 15
```

де, level 15 – встановлює рівень привілеїв. 15 є найвищим рівнем (адміністратор).

Далі можна переходити до налаштування конфігурації інших комутаторів робочих груп. Відрізнятись буду лише номери access-портів та транкових портів та номери і назви підмереж VLAN, відповідно до структурно-функціональна схема мережі представленої на рисунку Б.1, додатку Б та таблиці 3.1.

Деякі комутатори можуть вимагати окремої команди для встановлення пароля enable (пароля для переходу в привілейований режим, якщо він відрізняється від пароля admin). Для DrayTek це інтегровано.

Завершальним етапом є конфігурація маршрутизатора. Цей пристрій виконуватиме подвійну функцію: слугуватиме шлюзом для виходу в Інтернет та забезпечуватиме маршрутизацію трафіку між віртуальними підмережами.

Для досягнення цих цілей, на його фізичному інтерфейсі, з'єднаному з головним комутатором, потрібно створити й налаштувати віртуальні порти для кожної VLAN. Проте, перед цим кроком необхідно призначити маршрутизатору ім'я, використовуючи відповідні команди.

Для під’єднання до маршрутизатора необхідно використати консольний кабель для підключення комп'ютера до консольного порту маршрутизатора. При цьому слід використати програму-термінал (наприклад, PuTTY на Windows) з такими налаштуваннями: 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

Після успішного входу в командний рядок керування маршрутизатором, відкриється режим користувача або привілейований режим. Потрібно перейти в режим глобальної конфігурації. При введені команди

Vigor2962> enable

З’явиться пропозиція ввести ім’я користувача та пароль. За замовчуванням логін/пароль admin/admin.

Після успішної авторизації необхідно перейти в режим глобального конфігурування командою:

Vigor2962# configure terminal

У режимі глобальної конфігурування слід ввести команду hostname для встановлення імені маршрутизатора:

Vigor2962(config)# hostname R1

Для того щоб змінити пароль за замовчуванням для для користувача admin слід ввести команду:

R1(config)# username admin password <новий_пароль> level 15

де level 15 забезпечує найвищий рівень привілеїв.

Після встановлення налаштувань безпеки слід зберегти конфігурацію командою:

R1(config)# end

R1# write memory

Налаштування інтерфейсів маршрутизатора DrayTek Vigor2962, включаючи призначення IP-адрес і конфігурацію віртуальних портів (VLAN-інтерфейсів або Sub-interfaces) для маршрутизації між VLAN, є ключовим кроком. Це дозволяє маршрутизатору виступати як шлюз для кожної віртуальної мережі та забезпечувати маршрутизацію між ними, а також до Інтернету.

DrayTek Vigor2962 підтримує багато підмереж на одному LAN-інтерфейсі за допомогою VLAN Tagging. Для кожної віртуальної мережі (VLAN) необхідно створити логічний інтерфейс (VLAN Interface), якому призначаєте IP-адресу, що буде шлюзом для цієї VLAN.

Принцип "Router-on-a-Stick" полягає у налаштовуванні одного фізичного LAN-інтерфейс (наприклад, LAN1) як транковий порт. На цьому фізичному інтерфейсі створюватимуться віртуальні інтерфейси (sub-interfaces) для кожного VLAN. Кожен sub-interface матиме IP-адресу, яка буде шлюзом за замовчуванням для пристроїв у відповідному VLAN.

У мережі рекламного буро “Бум” слід створити 10 віртуальних підмереж представлених в таблиці 3.1. IP-адреси цих підмереж представлені в таблиці 2.7. Для зручності як адресу шлюзу буде використано останню адресу діапазону IP-адрес вузлів представлений в таблиці 2.7.

DrayTek Router OS відрізняється від Cisco CLI. В цій ОС VLAN-и налаштовуються в розділі LAN, а потім здійснюється прив'язування їх до фізичних або віртуальних інтерфейсів.

На відміну від Cisco, де створюються sub-interface на фізичному інтерфейсі, DrayTek Vigor маршрутизатори мають більш інтегрований підхід до управління VLAN. Потрібно використовувати команди, які стосуються налаштування підмереж на LAN-портах та їх зв'язку з VLAN ID. Для цього слід перейти в режим конфігурування LAN-портів, ввівши команду:

Спочатку слід увімкніть функцію VLAN командою:

R1(config)# vlan enable

Далі слід створити LAN Subnet (логічну підмережу) для кожного VLAN ID та призначити їй IP-адресу. За замовчуванням, LAN1 вже налаштований з IP 192.168.1.1. Потрібно змінити його та створити VLAN-інтерфейси (LAN2 – LAN10).

В таблиці 3.2 представлено відповідність LAN інтерфейсів вірт уальним мережам та їхнім VLAN ID.

Таблиця 3.2 Відповідність віртуальних LAN маршрутизатора VLAN ID

Назва віртуального інтерфейсу	Назва VLAN	Номер VLAN	IP-адреса шлюзу	Маска підмережі
lan 1	Net1	101	192.168.1.142	255.255.255.240
lan 2	Net2	102	192.168.1.150	255.255.255.248
lan 3	Net 3	103	192.168.1.110	255.255.255.240
lan 4	Net4	104	192.168.1.126	255.255.255.240
lan 5	Net5	105	192.168.1.46	255.255.255.240
lan 6	Net6	106	192.168.1.62	255.255.255.240
lan 7	Net7	107	192.168.1.78	255.255.255.240
lan 8	Net8	108	192.168.1.94	255.255.255.240
lan 9	Serv	109	192.168.1.154	255.255.255.252
lan 10	WiFi	110	192.168.1.30	255.255.255.224

В Vigor2962 LAN-порти за замовчуванням мають вже призначені IP-адреси. Якщо LAN1 використовується для підключення до комутатора, до якого йдуть всі VLAN-и, можете переконатися, що він активний.

Команди lan використовуються для створення віртуальних LAN-інтерфейсів (підмереж) та призначення їм IP-адрес. Ці віртуальні LAN-інтерфейси потім асоціюються з VLAN ID та фізичними портами.

Відповідно до даних таблиці 3.2 необхідно налаштувати віртуальні інтерфейси LAN [8]:

R1(config)# lan 1

R1(config-lan-1)# ip address 192.168.1.142 255.255.255.240

R1(config-lan-1)# vlan tag 101 //Призначити VLAN ID 101 цьому логічному LAN-інтерфейсу

R1 (config-lan-1)# exit

R1(config)# lan 2

R1(config-lan-2)# ip address 192.168.1.150 255.255.255.248

R1(config-lan-2)# vlan tag 102

R1 (config-lan-2)# exit

R1(config)# lan 3

R1(config-lan-3)# ip address 192.168.1.110 255.255.255.240

R1(config-lan-3)# vlan tag 103

R1 (config-lan-3)# exit

R1(config)# lan 4

R1(config-lan-4)# ip address 192.168.1.126 255.255.255.240

R1(config-lan-4)# vlan tag 104

R1 (config-lan-4)# exit

R1(config)# lan 5

R1(config-lan-5)# ip address 192.168.1.78 255.255.255.240

R1(config-lan-5)# vlan tag 105

R1 (config-lan-5)# exit

R1(config)# lan 6

R1(config-lan-6)# ip address 192.168.1.94 255.255.255.240

R1(config-lan-6)# vlan tag 106

R1 (config-lan-6)# exit

R1(config)# lan 7

R1(config-lan-7)# ip address 192.168.1.46 255.255.255.240

R1(config-lan-7)# vlan tag 107

R1 (config-lan-7)# exit

R1(config)# lan 8

R1(config-lan-8)# ip address 192.168.1.62 255.255.255.240

R1(config-lan-8)# vlan tag 108

R1 (config-lan-8)# exit

R1(config)# lan 9

R1(config-lan-9)# ip address 192.168.1.154 255.255.255.252

R1(config-lan-9)# vlan tag 109

R1 (config-lan-9)# exit

R1(config)# lan 10

R1(config-lan-10)# ip address 192.168.1.30 255.255.255.224

R1(config-lan-10)# vlan tag 110

R1(config-lan-1)# dhcp server enable // Увімкніть DHCP для цього VLAN

R1 (config-lan-10)# exit

Тепер потрібно вказати, які фізичні порти будуть пропускати ці теговані VLAN-и. Зазвичай це робиться в режимі конфігурації порту. На DrayTek маршрутизаторах це часто налаштовується в розділі LAN -> VLAN у веб-інтерфейсі, де обирають, які LAN-інтерфейси (LAN1, LAN2, LAN3...) асоціюються з певним фізичним портом та VLAN ID (Tagged/Untagged).

В командному рядку, це можна зробити командою [8]:

R1(config)# interface ethernet 1/1

R1(config-if)# switchport mode trunk

R1(config-if)# switchport trunk allowed vlan add 101, 102, 103, 104, 105, 106, 107, 108, 109, 110

Команда vlan tag <VLAN_ID> у підрежимі lan <номер> уже робить цей LAN-інтерфейс тегованим для відповідного VLAN ID на всіх портах, де цей LAN-інтерфейс активований як "tagged".

Далі потрібно вказати, щоб фізичний порт LAN1 на маршрутизаторі, до якого підключений головний комутатор, дозволяв тегований трафік для всіх VLAN-ів. У DrayTek це робиться через налаштування самого LAN-порту, де слід вказати, які "LAN підмережі" (LAN1, LAN2, LAN3 і т.д.) він буде обслуговувати, і чи буде трафік тегованим. Для цього слід ввести команди [8]:

```
R1(config)# lan port 1
R1(config-lan-port-1)# pvid 1 // встановити PVID
R1(config-lan-port-1)# allow vlan 10 tagged
R1(config-lan-port-1)# allow vlan 20 tagged
R1(config-lan-port-1)# allow vlan 30 tagged
R1(config-lan-port-1)# exit
```

Переважно, на маршрутизаторах DrayTek, WAN-інтерфейс отримує IP-адресу від провайдера (через DHCP) або йому призначається статична публічна IP. LAN-інтерфейси отримують приватні IP-адреси, які будуть шлюзами для локальних мереж. Але, оскільки провайдер надає рекламному бюро “Бум” статичну IP-адресу, 203.0.113.10/29 із шлюзом 203.0.113.9, то слід вказати наступні команди для їх призначення [8]:

```
R1(config)# wan1
R1(config-wan1)# ip address 203.0.113.10 255.255.255.248
R1(config-wan1)# ip default-gateway 203.0.113.9
R1(config-wan1)# dns server 8.8.8.8
R1(config-wan1)# exit
```

На завершення потрібно зберегти всі зміни, щоб вони не були втрачені після перезавантаження маршрутизатора:

```
R1(config)# end
R1# write memory
```

На цьому налаштування активного мережевого обладнання закінчено.

3.3 Інструкції з налаштування інструментів мережевого захисту

Оскільки в локальній мережі рекламного буро “Бум” використовується NAT для доступу до Інтернет, а всередині локальної мережі розгортається web-сервер, до якого потрібно забезпечити доступ публічними адресами. То потрібно налаштувати пере6направляенн портів Port Forwarding (Destination NAT).

На DrayTek Vigor2962, NAT для вихідного трафіку (Source NAT, або "маскарадинг") зазвичай увімкнений за замовчуванням для трафіку, що йде з приватних IP-адрес локальної мережі на WAN-інтерфейс. Вам не потрібно явно вмикати "NAT" як глобальну функцію, оскільки вона є невід'ємною частиною функціонування маршрутизатора як шлюзу. Але для перенаправлення вхідного трафіку з Інтернету на конкретний сервер у локальній мережі Port Forwarding (Destination NAT / Virtual Server) необхідно виконувати додаткові налаштування.

В розроблюваній мережі рекламного бюро “Бум” web-серверу призначено з IP-адресу 192.168.1.153/30 . хочете, щоб доступ до нього з Інтернету був за портом 80 (HTTP) та 443 (HTTPs). Для цього слід ввести команди [8]:

R1(config)# nat

R1(config-nat)# virtual-server add name WebServer wan wan1_ip_alias_0 protocol tcp public-port 80 private-ip 192.168.1.153 private-port 80

R1(config-nat)# virtual-server add name WebServer wan wan1_ip_alias_0 protocol tcp public-port 443 private-ip 192.168.1.153 private-port 443

Vigor2962(config-nat)# exit

Веб-сервер рекламного бюро "Бум" є загальнодоступним ресурсом, що вимагає гостьового доступу з Інтернету. У таких випадках для розміщення публічних ресурсів створюють демілітаризовані зони (DMZ) – ізольовані сегменти мережі. Для цього слід ввести команди:

Vigor2962(config)# nat

Vigor2962(config-nat)# dmz enable

Vigor2962(config-nat)# dmz host 192.168.1.153 // IP-адреса хоста в DMZ

Vigor2962(config-nat)# exit

Антивірусний захист та захист від шкідливого ПЗ (Antivirus/Anti-malware) не є суто "мережевий" інструмент, він є критично важливим для кінцевих точок, які підключаються до мережі, і може зупинити поширення загроз. Для цього пропонується використати ClamAV – відкритий антивірус що часто використовується на серверах або для сканування файлів.

Для встановлення антивірусу слід ввести команду:

@server:~ % sudo pkg install -y clamav

Для оновлення баз даних вірусів:

@server:~ % sudo freshclam

Для сканування каталогу:

@server:~ % sudo clamscan -r /path/to/scan # Рекурсивне сканування

Після встановлення антиірусу потрібно:

- регулярно оновлюйте антивірусні бази даних;
- запланувати регулярне сканування всіх систем.

Базові принципи мережевого захисту:

- принцип найменших привілеїв. Надавати тільки необхідні дозволи;
- сегментація мережі. Розділяти мережу на менші, ізольовані сегменти (VLAN, підмережі) для обмеження поширення атак;
- резервне копіювання. Регулярно створювати резервні копії критичних даних та конфігурацій;
- моніторинг – постійно відстежувати мережеву активність та журнали;
- навчання персоналу. Людський фактор є однією з найбільших вразливостей. Необхідно навчити користувачів основам кібербезпеки;
- план реагування на інциденти:. Розробіть чіткий план дій у випадку інциденту безпеки.

Налаштування ефективної мережевої безпеки — це безперервний процес, який вимагає постійного моніторингу, оновлення та адаптації до нових загроз.

3.4 Інструкції з налаштування безпровідної точки доступу

Існує два основні способи налаштування EAP110:

- автономний режим (Standalone Mode) – налаштування кожної точки доступу індивідуально через її власний веб-інтерфейс. Це підходить, якщо у мережі лише одна або кілька точок доступу;
- режим контролера (Controller Mode) – налаштування та управління всіма точками доступу централізовано за допомогою програмного контролера Omada SDN (на ПК, сервері або апаратному контролері OC200/OC300). Використовується для великих мереж.

Для мережі рекламного бюро “Бум”, де встановлено лише одну безпровідну точку доступу слід використати автономний режим.

Спочатку потрібно підключити EAP110 до джерела живлення. EAP110 підтримує живлення через Power over Ethernet (PoE) за стандартом 802.3af, тому її можна під’єднати через мережевих кабель до комутатора Sw4, який одночасно буде забезпечувати живлення пристрою.

За замовчуванням EAP110 отримує IP-адресу по DHCP. Якщо у мережі ще не налаштовано DHCP-сервер, точка доступу використовуватиме статичну IP-адресу за замовчуванням: 192.168.0.254.

Тепер слід під’єднати комп'ютер і налаштувати на ньому IP-адресу, щоб він знаходився в одній мережі із точкою доступу (наприклад, 192.168.0.100). Після цього на ПК слід виконати наступні дії:

- відкрити web-браузер;
- у адресному рядку ввести IP-адресу EAP110 – 192.168.0.254;
- натиснути Enter. З'явиться сторінка входу;
- ввести облікові дані: За замовчуванням логін і пароль: admin / admin;
- обов'язково змінити стандартні облікові дані. Після першого входу система запропонує негайно змінити пароль. Якщо ні, то зайти в розділ Management -> Account і змінити пароль адміністратора;
- перейти до розділу Wireless Settings;

- натиснути кнопку для додавання нового SSID;
- створити новий SSID, ввівши SSID Name –назву Wi-Fi мережі (наприклад, Guest_Boom);
- в розділі Security Mode вибрати WPA2-PSK (це найбільш поширений і безпечний варіант для домашніх/малих офісних мереж). Далі вибрати метод шифрування WPA2-PSK/AES;
- в полі Password ввести надійний пароль для Wi-Fi мережі (мінімум 8 символів, комбінація великих/малих літер, цифр і спецсимволів);
- опцію Enable SSID Broadcast рекомендовано залишити увімкненим, щоб Wi-Fi мережа була видимою для пристроїв. Якщо вимкнути, мережа буде "прихованою";
- для гостьових пристроїв вказати VLAN ID і призначити цьому SSID VLAN ID 110. Це дозволить розділити трафік на окремий VLAN для гостей і окремий для працівників;
- зберегти зміни, натиснувши "Save" або "Apply";
- у розділі "Network" -> "LAN" змінити IP-адресу EAP110 на 192.168.1.1. Після зміни IP-адреси доведеться повторно підключитися до web-інтерфейсу за новою адресою;
- у розділі "System" -> "Firmware Upgrade" перевірити, чи доступна нова версія прошивки на офіційному сайті TP-Link. Завжди рекомендується оновлювати прошивку для покращення стабільності та безпеки.

3.5 Інструкція з використання тестових наборів та тестових програм

Тестування мережі – не просто початковий етап, а безперервний процес, що є фундаментальною складовою її безпеки. Безпека мережі не обмежується лише захистом від несанкціонованого доступу; вона також полягає в забезпеченні її надійної та ефективної роботи. Адже збої та неправильна

конфігурація можуть призвести не тільки до відмов, але й до суттєвого зниження продуктивності.

Щоб мінімізувати подібні ситуації, необхідно регулярно проводити діагностику, тестування та інші профілактичні заходи. Для цього доступний широкий спектр апаратних і програмних засобів, проте найчастіше використовуються вбудовані утиліти операційних систем. У Windows для тестування мережі вам знадобляться [6]:

- ipconfig –перегляд поточної конфігурації налаштувань протоколу TCP/IP;
- netstat – моніторинг з'єднань та їх статистики;
- ping – перевірки доступності іншої робочих станцій для даного ПК;
- tracert – відстеження маршруту проходження пакетів між даним та віддаленим комп'ютерами;
- route – перегляд та редагування таблиць маршрутизації.

Процес тестування цієї мережі складається з двох основних етапів. Почніть з апаратної перевірки: оцініть фізичні з'єднання та електричні характеристики кабельної системи за допомогою кабельного тестера. Після цього перейдіть до програмного тестування мережі, використовуючи такі вбудовані утиліти, як ipconfig, ping та netstat.

Перший етап тестування передбачає використання кабельного тестера. Спершу необхідно провести візуальний огляд кабельних роз'ємів, перевіряючи їх на дефекти, правильність обтиску та цілісність контактів. Далі підключити один кінець кабелю до тестера, а інший – до його віддаленого модуля. Увімкнувши тестер, потрібно спостерігайте за індикаторами: їх послідовне світіння свідчить про справне з'єднання. Відсутність індикації для будь-якого провідника вказує на несправність, яка може вимагати заміни кабелю.

Для програмної діагностики мережі спочатку потрібно використати команду ipconfig на кожному вузлі. Це дозволить перевірити поточні налаштування TCP/IP, включаючи MAC- та IP-адреси вузла, адресу шлюзу та DNS-сервера. Якщо виникли проблеми з DNS, то можна скористатися

командою “ipconfig /flushdns” для очищення кешу DNS, а потім перезавантажте вузол.

Далі необхідно перевірити зв'язок з іншими вузлами за допомогою команди ping. Ця утиліта відправляє запит на вказану робочу станцію та очікує відповідь. Якщо з'єднання працює коректно, буде отримано пакет-відповідь та час, необхідний для його отримання. Для цієї мережі час відповіді не має перевищувати 10 мілісекунд.

Якщо відобразиться повідомлення "Request timed out" (перевищено час очікування відповіді), це може вказувати на такі проблеми:

- мережа не працює;
- невірно вказана адреса одержувача;
- час отримання пакету-відповіді перевищив допустимі 750 мілісекунд;
- вузол, з яким перевіряється з'єднання, вимкнений.

Для повної перевірки працездатності мережі необхідно перевірити доступність усіх робочих станцій.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Економічна частина кваліфікаційної роботи використовується для здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для рекламного бюро «Бум» і прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Ці розрахунки вартості наукових досліджень та розробки виконується в декілька етапів:

- описати технологічний процес розробки із зазначенням трудомісткості кожної операції;
- визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;
- визначити суму матеріальних затрат;
- обчислити витрати на електроенергію для науково-виробничих цілей;
- розрахувати транспортні витрати;
- нарахувати суму амортизаційних відрахувань;
- визначити суму накладних витрат;
- скласти кошторис та визначити собівартість НДР;
- розрахувати ціну НДР;
- визначити економічну ефективність та термін окупності мережі рекламного агентства «Бум».

4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР доцільно звести у таблицю 4.1 дані витрат часу по окремих операціях технологічного процесу. Виконавцями стадій технологічного процесу будуть: керівник, інженер, технік.

В таблиці 4.1 наводяться стадії технологічного процесу та середній час їх виконання.

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

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Постановка задачі, формування технічного завдання на проект локальної мережі. Узгодження майбутнього розміщення мережевих розеток.	Керівник проекту	15
2.	Проектування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі проектно-монтажної організації «Будсервіс». Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури проектно-монтажної організації «Будсервіс».для сегментування локальної мережі на підмережі.	Інженер	15
3.	Монтаж мережі (прокладання кабельних каналів, вертикальних та горизонтальних кабельних каналів). Здійснюється монтаж та підключення пасивного обладнання. Перевірка СКС локальної мережі на відповідність вибраній технології.	Технік	25

Продоження таблиці 4.1

1	2	3	4
4.	Конфігурування мережевого обладнання (налаштування апаратного та програмного забезпечення). Налагодження мережі. Тестування конфігурацій апаратного та програмного забезпечення служб ЛОМ.	Інженер	20
5.	Підготовка документації. Написання кабельного журналу, списку мережевого обладнання та його технічних характеристик.	Інженер	5
		Разом	80

Проєктна розробка мережі вимагає загалом 80 годин роботи. З них 15 годин припадає на діяльність керівника проєкту, 40 годин – на інженера, і 25 годин – на техніка.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Грошова винагорода, яку працівник отримує від власника підприємства за виконану роботу, становить оплату праці – вираження вартості робочої сили. Ця винагорода безпосередньо корелює з кінцевими результатами функціонування підприємства, підлягає податковому регулюванню та не обмежується максимальними розмірами.

Основна заробітна плата обчислюється за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

На підставі рекомендованих тарифних ставок встановлено наступні погодинні ставки: для керівника проєкту – 100 грн, для інженера – 90 грн, а для техніка – 60 грн.

Таким чином, основна заробітна плата для:

- керівника проекту – $З_{осн1} = 15 \cdot 100 = 1\ 500$ грн.
- інженера – $З_{осн2} = 40 \cdot 90 = 3\ 600$ грн.
- техніка – $З_{осн3} = 25 \cdot 60 = 1\ 500$ грн.

Сумарна основна заробітна плата становить

$$З_{осн}=1\ 500 +3\ 600 + 1\ 500 =6\ 600 \text{ грн.}$$

Додаткова заробітна плата становить 10 –15 % від суми основної заробітної плати.

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника $З_{дод1}=1\ 500 \cdot 0,13= 195$ грн.
- інженера $З_{дод1}=3\ 600 \cdot 0,13= 468$ грн.
- техніка $З_{дод3}=1\ 500 \cdot 0,13= 195$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод}=195 + 468 + 195= 858 \text{ грн.}$$

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

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

Звідси, загальні витрати на оплату праці становлять:

$$В_{о.п.}= 6\ 600 + 858 = 7458 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи. Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде становити:

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з}= 7458 \cdot 0,22= 1640,76 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/	Категорія працівників	Основна заробітна плата, грн.			Додатк. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тарифна ставка, грн.	К-сть відпрац. год.	Фактично нарах. з/пл., грн.			
1	Керівник	100	15	1500	195		
2	Інженер	90	40	3600	468	-	-
3	Технік	60	25	1500	195	-	-
			Разом	6600	858	1640,76	9098,76

Отже, загальні витрати на оплату праці становлять 9098,76 грн.

4.3 Розрахунок матеріальних витрат

Розмір матеріальних витрат встановлюється шляхом множення кількості використаних матеріалів та їхньої ціни:

$$M_{BI} = q_i \bullet P_i \quad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу *i*-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} \sum M_{B_i} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Кіль-кість	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа GEAR 6U ZT-NET AL-WDR06U-64G	шт.	1	2950	2950
2	Патчпанель 24 порти, кат. 6	шт.	1	1200	1200
3	Розетка зовнішня Cablexpert RJ-45 NCAC—HS—SMB2	шт.	57	79	4503
4	Розетка підлогова Cablexpert RJ-45 (Cat 6)	шт.	9	55	495
4.	Роз’єм 8P8C (пачка 100 шт)	шт.	1	631	631
5	Короб (середня ціна для різного січення)	м.	238	120	28560
6	Короб підлоговий	м.	15	159	2385
6	Гофрована трубка	м.	12	35	420
7	Кабель UTP (кат. 6) (бухта)	шт.	3	5310	15960
8	Патчкорди (кат. 6)	шт.	66	51	3366
9	Кабель опотоволоконний	м.	10	26	260
10	Конектор SC	шт.	2	35	70
11	Маршрутизатор DrayTek Vigor2962	шт.	1	24488	24488
12	Комутотар DrayTek VigorSwitch P2280x	шт.	4	10750	43000
13	Безпровідна точка доступу TP-LINK EAP110	шт.	1	1429	1429
14	Джерело безперебійного живлення APC Back-UPS Pro 1200VA	шт.	1	3650	3650
Р а з о м			-	-	133367

Отже, загальна сума матеріальних витрат на розробку мережі становить 133367 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 10 годин, споживана потужність – 0,5 кВт/год, вартість 1 кВт електроенергії - 7 грн. Тому витрати на електроенергію будуть становити::

$$З_е = 0,5 \cdot 10 \cdot 7 = 35 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8–10% від загальної суми матеріальних затрат.

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

де $Т_В$ – транспортні витрати.

Отже,

$$Т_В = 133367 \cdot 0,08 = 15344,08 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

В процесі використання основних фондів виконуються заходи що до їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації. Амортизація – це процес перенесення вартості основних фондів на вартість

новоствореної продукції з метою їх повного відновлення. Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_в \cdot Н_А}{100\%} \cdot T \quad (4.9)$$

де А – амортизаційні відрахування за звітний період, грн.;

$Б_в$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 10 год., балансова вартість ПК - 26500 грн., тому, то амортизаційні відрахування становлять:

$$A = \frac{26500 \cdot 0{,}04}{150} \cdot 10 = 70{,}67 \text{ грн}$$

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.

$$Нв = Во.п. \cdot 0{,}2...0{,}6,, \quad (4.10)$$

де H_B – накладні витрати.

$$H_B = 7458 \cdot 0{,}5 = 3729 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат – це узагальнений план всіх очікуваних витрат підприємства на майбутній період його виробничо-фінансової діяльності. Результати попередніх розрахунків будуть зведені в таблиці 4.4, яка включатиме такі види витрат: оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування та накладні витрати..

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	в % до загального
Витрати на оплату праці (основну і додаткову заробітну плату)	7458	3,39
Відрахування на соціальні заходи	1640,76	0,75
Матеріальні витрати	133367	82,51
Витрати на електроенергію	35	0,02
Транспортні витрати	*15344,08*	6,97
Амортизаційні відрахування	70,67	0,03
Накладні витрати	3729	1,69
Собівартість	161644,51	100

В таблиці 4.4 зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати, тобто собівартість ($С_в$) НДР розрахуємо за формулою:

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

Отже, собівартість дорівнює C_B=161644,51 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_в \cdot (1 + P_{рен}) + K \cdot B_{ні}}{K} \cdot (1 + ПДВ) \quad (4.12)$$

де $P_{рен.}$ – рівень рентабельності;

K – кількість замовлень, од.;

$B_{і.н}$ - вартість носія інформації, грн.;

ПДВ – ставка податку на додану вартість, (20 %).

Отже, ціна НДР становить:

$$Ц = 161644{,}51 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 252\,165{,}43 \text{ грн}$$

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 (ТОК).

$$ЧТВ = -K_В + \sum_{i=1}^{t} \frac{Г_в}{(1+i)^t} \geq 0, \quad (4.13)$$

де $K_в$ – затрати на проект;

$Г_В$ – грошовий потік за t-ий рік;

t - відповідний рік проекту;

i –величина дисконтної ставки (10-15%).

$$ЧТВ = -161644{,}51 + \frac{127681{,}29}{1 + 0{,}1} + \frac{127681{,}29}{(1 + 0{,}1)^2} = 59951{,}12 \text{ грн}$$

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

Термін окупності визначається за формулою:

$$T_{ОК} = T_{\text{ПВ}} + \frac{H_B}{\Gamma_{\text{пр}}} \quad (4.14)$$

де $T_{ПВ}$ – період до повного відшкодування витрат, років;

H_B – невідшкодовані витрати на початок року, грн.;

$Г_{ПР}$ – грошовий потік на початку року, грн..

$$T_{ОК} = 1 + \frac{25536,26}{127681,29} = 1,2$$

Всі дані внесемо в зведену таблицю 4.5 економічних показників.

Таблиця 4.5 – Економічні показники НДР

№п/п	Показник	Значення
1.	Собівартість, грн.	161644,51 грн.
2.	Плановий прибуток, грн.	90811,52 грн.
3.	Ціна, грн.	252 165,43 грн.
4.	Чиста теперішня вартість	59951,12 грн.
5.	Термін окупності, рік	1,2

Загальна вартість розробленої комп'ютерної мережі для рекламного бюро «Бум» становить 252 165,43 грн. Термін окупності становить 1,2 роки, що є хорошим показником. Таким чином, можна зробити висновок, що проведення робіт по розробці даної мережі є доцільним та економічно вигідним.

.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

Науково-технічний прогрес вніс серйозні зміни в умови діяльності працівників розумової праці. Їх праця стала інтенсивним, які вимагають значних витрат розумової, емоційної і фізичної-ческький енергії, що зажадало комплексного рішення проблем ергономіки, гігієни і організації праці, регламентації режимів праці та відпочинку. В даний час комп'ютерна техніка широко застосовується у всіх областях діяльності людини.

При роботі з комп'ютером людина піддається дії ряду небезпечних і шкідливих виробничих факторів: електромагнітних полів (діапазон радіочастот: ВЧ, УВЧ і СВЧ), інфрачервоного і іонізуючого випромінювань, шуму і вібрації, статичної електрики і ін. Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою. Велике значення має раціональна конструкція і розташування елементів робочого місця, що важливо для підтримки оптимальної робочої пози людини-оператора. У процесі роботи з комп'ютером необхідно дотримувати правильний режим праці та відпочинку [4].

5.1 Нормативні акти про охорону праці, що діють у межах рекламного бюро “Бум”

У межах рекламного бюро “Бум”, як і в будь-якому іншому підприємстві чи організації України, діють нормативно-правові акти з охорони праці, які забезпечують безпеку, гігієну праці та здорові умови праці для працівників. Навіть якщо діяльність здається «офісною» або «творчою», законодавство з охорони праці все одно обов’язкове.

Основні загальні нормативно-правові акти [4]:

- Закон України "Про охорону праці" № 2694-XII. Це основний законодавчий акт, що визначає загальні (основні) принципи державної політики

у сфері охорони праці, обов'язки роботодавця та працівників, а аткож вимоги до організації роботи з охорони праці;

- Кодекс законів про працю України. Містить положення щодо умов праці, трудових договорів, робочого часу та часу відпочинку, що також мають значення для охорони праці;

- Закон України «Про колективні договори і угоди», який містить розділ щодо заходів з охорони праці;

- типове положення про службу охорони праці, затверджене наказом Держнаглядохоронпраці від 15.11.2007 № 255. Визначає основні завдання, функції та права служби охорони праці на підприємстві;

- типове положення про порядок проведення навчання і перевірки знань з питань охорони праці, затверджене наказом Держнаглядохоронпраці від 26.01.2005 № 15, оновлений у 2019 році. Встановлює порядок організації та проведення навчання з питань охорони праці для працівників;

- порядок розслідування та обліку нещасних випадків, професійних захворювань та аварій на виробництві, затверджений постановою Кабінету Міністрів України від 17.04.2019 № 337. Визначає процедуру розслідування та обліку нещасних випадків і професійних захворювань;

- нормативно-правові акти з охорони праці (НПАОП), які є галузевими або міжгалузевими правилами, нормами, інструкціями та іншими документами, що встановлюють вимоги безпеки праці залежно від видів робіт та обладнання.

Оскільки, одним із напрямків діяльності рекламнеого бюро "Бум" є зовнішня реклама, то на підприємтсві діють настурпні специфічні нормативно-правові акти. Монтажні роботи, навіть якщо вони проводяться в межах рекламного бізнесу (наприклад, встановлення зовнішньої реклами, вивісок, банерів, конструкцій тощо), вважаються підвищено небезпечними роботами. До таких нормативних актів відносяться [7]:

- НПАОП 0.00-1.15-07 Правила охорони праці під час виконання робіт на висоті;

- Наказ Мінсоцполітики № 62 від 27.01.2005, чинний у редакції 2018 року, який втсановлює:

- вимоги до організації та виконання робіт на висоті (від 1,3 м і більше),
- вимоги до страхувальних систем, касок, поясів, огороджень
- навчання і допуск працівників до висотних робіт;

- Наказ Міністерства надзвичайних ситуацій України від 29.09.2011 № 1045 – Правила охорони праці під час монтажу, демонтажу та експлуатації металевих конструкцій

- регламентують вимоги до встановлення конструкцій, в тому числі рекламних щитів,
- вимоги до вантажопідіймальних механізмів, монтажних лебідок,
- порядок проведення навчання і перевірки знань з охорони праці – Наказ №15/45 від 26.01.2005 (оновлений у 2019 р.), який регламентує обов'язкове навчання для всіх, хто виконує монтажні (підвищено небезпечні) роботи;

- правила безпечної експлуатації електроустановок.

Крім державних нормативно-правових актів, в рекламному бюро "Бум", розроблено та затверджено власні внутрішні нормативні акти з охорони праці:

- наказ про призначення відповідального за охорону праці;
- положення про охорону праці в рекламному бюро "Бум";
- переліки робіт з підвищеною небезпекою для спеціаліста із монтажу зовнішньої реклами;
- журнал реєстрації інструктажів з охорони праці в рекламному бюро "Бум";
- програма вступного, первинного, повторного інструктажу з охорони праці;
- дозволи на виконання робіт підвищеної небезпеки (від Держпраці);
- медогляди працівників (обов'язково для висотників);
- інструкції з охорони праці для всіх груп працівників.

При цьому у рекламному бюро “Бум” розроблено інструкції для наступних груп працівників:

- офісних працівника;
- дизайнера, який працює за комп’ютером;
- спеціаліста з монтажу зовнішньої реклами;
- прибиральника.

5.2 Вимоги до розташування виробничого і офісного обладнання в реклаиному бюро “Бум”

Вимоги до розташування виробничого та офісного обладнання в рекламному бюро визначаються насамперед безпекою праці, ергономікою, ефективністю робочого процесу та пожежною безпекою. Оскільки рекламне бюро “Бум” включає як офісні приміщення, так і виробничі ділянки для друку, різки, монтажу зовнішньої реклами, вимоги для цих зон відрізняються.

Загальні вимоги для обох зон [4]:

- забезпечення достатнього вільного простору для безпечного переміщення працівників та транспортування матеріалів;
- уникнення захаращення проходів та робочих місць;
- надійне кріплення обладнання, щоб запобігти його падінню або перекиданню;
- забезпечення доступу до засобів пожежогасіння (вогнегасники, пожежні щити) та шляхів евакуації;
- розміщення електрообладнання з урахуванням вимог електробезпеки (захист від ураження струмом, правильне підключення, відсутність оголених проводів).
- врахування вагових навантажень на підлогу;
- організація робочих місць з урахуванням антропометричних даних працівників для забезпечення зручної робочої пози;

- правильне розміщення моніторів, клавіатур, мишей та іншого офісного обладнання для запобігання втомі та захворюванням опорно-рухового апарату.

- забезпечення належного освітлення робочих місць (природного та штучного);

- мінімізація шумів та вібрацій на робочих місцях.

- забезпечення можливості регулювання висоти столів та стільців.

Раніше, площу приміщень, у яких розташовували персональні комп'ютери, визначали згідно з ДСанПіН 3.3.2-007-98, але згідно з наказом Міністерства охорони здоров'я України від 15.01.2021 № 44 він втратив чинність Хоча жорсткої норми площі на ПК в новому документі немає, фахівці з охорони праці часто орієнтуються на загальні рекомендації та міжнародні практики, які передбачають щонайменше 4,5 - 6 м² на одне робоче місце в офісних приміщеннях для забезпечення комфортних та безпечних умов. Однак це є рекомендацією, а не прямою нормативною вимогою після скасування ДСанПіН 3.3.2-007-98 [4].

Заземлені конструкції, що знаходяться у приміщеннях (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном тощо), мають бути надійно захищені діелектричними щитками або сітками від випадкового дотику.

Конструкція робочого місця адміністратора має забезпечити підтримання оптимальної робочої пози офісного працівника. Конструкція робочого столу має відповідати сучасним вимогам ергономіки і забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів.

Правилами встановлюються висота робочої поверхні робочого столу, параметри ширини і глибини для робочих столів, які мають забезпечувати можливість виконання операцій у зоні досяжності моторного поля.

Згідно рекомендацій робочий стілець має бути підйомно–поворотним, регульованим за висотою, з кутом нахилу сидіння та спинки, від спинки до переднього краю сидіння поверхня сидіння має бути плоскою, передній край – заокругленим. Регулювання за кожним із параметрів має здійснюватися незалежно, легко і надійно фіксуватися [7]``.

Поверхня сидіння і спинки стільця має бути напівм’якою з нековзним, повітронепроникним покриттям, що легко чиститься і не електризується [4]

Важливе значення має безпека розміщення й оснащення робочого місця. Внутрішнє планування розподіляється на дві зони: зону праці (безпосередньо робоче місце) і зону підходу (стелажі, шухляди, шафи тощо).

Зовнішнє планування – розміщення робочого місця відносно інших робочих місць – визначається характером і кількістю його оснащення, характером виконуваних робіт. Крім того, до комплектації робочого місця входять предмети догляду за ним, засоби індивідуального захисту.

Конструкція робочого місця остнащеного комп’ютером має забезпечувати підтримання оптимальної робочої пози з наступними ергономічними характеристиками [7]:

- ступні ніг – на підлозі або на підставці для ніг стегна – в горизонтальній площині;

- передпліччя – вертикально;

- лікті – під кутом 70°-90° до вертикальної площини;

- зап’ястя зігнуті під кутом не більше 20° відносно горизонтальної площини, нахил голови – 20°відносно вертикальної площини.

Висота робочої поверхні столу для ПК має бути в межах 680-800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля.

Рекомендовані розміри столу: висота – 725 мм, ширина – 600-1400мм, глибина – 800-1000 мм.

Робочий стіл для комп'ютера повинен мати простір для ніг висотою не менше 600 мм, шириною не менше 500 мм, глибиною на рівні колін не менше 450 мм, на рівні витягнутої ноги – не менше 650 мм.

Екран монітора та клавіатура мають розташування на оптимальній відстані від очей користувача, але не ближче 600 мм, з урахування розміру алфавітно-цифрових знаків та символів.

Відстань від екрана до ока користувача комп'ютера повинна складати

при розмірі екрану до діагоналі [4]:

- 35/38 см (14"/15") – 500..600 мм

- 43 см (17") – 700..800 мм

- 48 см (19") – 800..900 мм

- 53 см (21") – 900..1000 мм

Освітленість робочої поверхні – не менше 100 лк для лампи люмінесцентні та не менше 30 лк для лампи розжарювання.

Оргтехніка (принтери, сканери, копіювальні апарати):

- розміщення в легкодоступних місцях для всіх користувачів;

- забезпечення достатньої вентиляції, особливо для лазерних принтерів та копіювальних апаратів, що можуть виділяти шкідливі речовини.

- врахування рівня шуму, що створюється оргтехнікою.

Зберігання документів та матеріалів:

- використання стелажів, шаф та полиць, що є стійкими та надійно закріпленими;

- розміщення важких предметів на нижніх полицях;

- забезпечення вільного доступу до місць зберігання.

Вимоги до розміщення виробничого друкарского обладнання:

- забезпечення достатнього простору для обслуговування та ремонту обладнання;

- врахування вібрації та шуму, що створюються обладнанням, та вжиття заходів для їх зменшення;

- наявність ефективної системи вентиляції для видалення шкідливих випарів (фарб, розчинників тощо).

- забезпечення належного освітлення робочої зони.

Розміщення обладнання з урахуванням технологічного процесу.

Вимоги до розміщення виробничого різального обладнання (плотери, гільйотинні ножі):

- забезпечення захисних пристроїв для запобігання травмуванню працівників;

- наявність достатнього вільного простору навколо обладнання для безпечної роботи.

- забезпечення належного освітлення робочої зони.

Монтажне обладнання (драбини, підйомники):

- зберігання у відведених місцях, у справному стані;

- забезпечення безпечних умов для їх використання (рівна поверхня, надійне встановлення).

5.3 Система організаційно-технічних заходів з пожежної безпеки в приміщеннях з комп’ютерною технікою

Система організаційно-технічних заходів з пожежної безпеки в приміщеннях з комп’ютерною технікою спрямована на запобігання пожежам, їх своєчасне виявлення та успішне гасіння, а також на забезпечення безпечної евакуації людей у разі виникнення пожежі.

Основні обов'язки власників підприємств [4]:

- призначення наказом керівника особи, відповідальної за пожежну безпеку в приміщеннях з комп’ютерною технікою;

- визначення обов'язків відповідальної особи щодо контролю за дотриманням правил пожежної безпеки, проведення інструктажів, навчання, перевірки стану обладнання тощо;

- розробка комплексних заходів щодо забезпечення пожежної безпеки в рекламній агенції;

- створення плану пожежної безпеки. Включає всі необхідні заходи для запобігання пожежам, виявлення та швидкого реагування на них;

- аналіз ризиків. Виявлення та оцінка потенційних джерел пожеж, визначення заходів щодо їх мінімізації;

- розробка та затвердження внутрішніх нормативних актів;

- тренінги та інструктажі. Регулярне проведення навчальних заходів, перевірка знань працівників;

- пропаганда пожежної безпеки. Інформаційні кампанії серед працівників щодо важливості дотримання правил пожежної безпеки.

- утримання в справному стані засобів протипожежного захисту;

- перевірка та обслуговування пожежної техніки у приміщеннях з комп'ютерною технікою: регулярне обслуговування, перевірка працездатності всіх засобів пожежного захисту;

- заборона використання не за призначенням: контроль за тим, щоб пожежне обладнання використовувалося виключно за призначенням.

Організаційно-технічне забезпечення пожежної безпеки повинно передбачати розробку методичних матеріалів, регламентів та стандартів виконання технологічних процесів, правил поводження з легкозаймистими та вибухонебезпечними речовинами та матеріалами.

Технічні заходи також включають встановлення пожежних сповіщувачів у всіх приміщеннях рекламного алентства та регулярний огляд і технічне обслуговування системи пожежної сигналізації.

Також важливо розміщувати вогнегасники у легкодоступних та видимих місцях, щоб кожен зі співробінтиків підприємтсва мав доступ до них при потребі, також забезпечувати їх регулярну перевірку та заправку, а також розміщувати пожежні гідранти переконатися, щоб вони належним чином функціонують.

Тому шляхи евакуації повинні бути чітко позначені, регулярно мати наявність та забезпечені світловими індикаторами та перевіреними знаками. Встановлення системи пожежної сигналізації також є технічним заходом для забезпечення справжнього інформування всіх працівників про небезпечну ситуацію. Регулярні перевірки системи сигналізації мають стати нормою.

Профілактичні заходи включають регулярні перевірки стану проводів та електрообладнання також профілактичне обслуговування електромережі. Тому важливо заборонити використання відкритого вогню в приміщеннях, щоб забезпечити належні умови для безпечного використання нагрівального обладнання. Також слід підтримувати чистоту та порядок ключовим для

запобігання накопиченню легкозаймистих матеріалів та забезпечення безпечного зберігання легкозаймистих матеріалів [4].

Регулярні перевірки та аудити включають організацію внутрішніх справ стану пожежної безпеки та ведення звітів про проведені перевірки та вжиті заходи. Важливо проводити спільні перевірки з представниками органів пожежного нагляду на виконання приписів та рекомендацій цих органів.

Організація навчання, інструктажу для приміщень із розмішеною комп'ютерною технікою та доступу персоналу з обслуговування вибухонебезпечних процесів має дуже велике значення для забезпечення пожежної безпеки.

Забезпечити пожежну безпеку неможливо без відповідного контролю та нагляду за дотриманням правил та норм, техніки безпеки, промислової гігієни та пожежної безпеки.

Для забезпечення повноцінної пожежної безпеки важливо також звернути увагу на наступні аспекти [4]:

- системи автоматичного пожежогасіння: встановлення таких систем у важливих зонах, де ризик виникнення пожежі високий, є ключовим аспектом забезпечення швидкого реагування на загрозу. Регулярне технічне обслуговування та перевірка працездатності;

- організація рятувальних робіт: розроблення та вдосконалення планів евакуації і рятувальних операцій для мінімізації потенційних втрат людських життів та майнових цінностей у випадку пожежі.

- спеціалізована пожежна техніка: забезпечення належного обслуговування та ефективного функціонування всіх видів пожежної техніки, такої як вогнегасники, пожежні сповіщувачі, гідранти тощо, щоб вони були завжди готові до використання;

- інформаційні кампанії: постійна освіта працівників щодо пожежної безпеки, включаючи навчання та інструктажі, а також регулярні тренінги з дотримання вимог і процедур безпеки.

- інтегровані системи управління безпекою: впровадження сучасних підходів до управління безпекою, які включають стандарти ISO та інші міжнародні норми для забезпечення високого рівня захисту.

- регулярні інспекції та аудити: виконання систематичних перевірок стану пожежної безпеки: включаючи перевірку відповідності пожежних систем, обладнання та процедур чинним стандартам і вимогам.

- попередні заходи: встановлення заходів щодо моніторингу і управління пожежними ризиками, таких як системи виявлення диму та системи контролю за температурою.

Розміщення обладнання [4]:

- розміщення комп'ютерної техніки на відстані від опалювальних приладів та інших джерел тепла;

- забезпечення достатнього простору навколо обладнання для його охолодження та обслуговування;

- використання негорючих або важкогорючих матеріалів для оздоблення приміщень (за можливості).

Утримання приміщень:

- регулярне прибирання приміщень від пилу та горючих відходів (папір, упаковка тощо);

- забезпечення належної вентиляції для запобігання перегріву комп'ютерної техніки;

- обмеження кількості горючих матеріалів у приміщеннях;

- заборона куріння у приміщеннях з комп'ютерною технікою.

Зважаючи на вищенаведені аспекти, також важливо [4]:

- моніторинг і управління матеріалами: перевірка та контроль за зберіганням легкозаймистих матеріалів, що можуть стати причиною пожежі. Важливо забезпечувати їх безпечне зберігання та використання відповідно до встановлених процедур.

- постійне оновлення знань і навичок: працівників підприємства з питань пожежної безпеки через систематичні тренінги та навчання. Це дозволяє

збільшити рівень обізнаності та готовності персоналу до дій у небезпечних ситуаціях.

- співпраця з місцевими органами: участь у спільних навчальних вправах та тренуваннях з місцевими пожежними службами для покращення координації і ефективності дій у разі пожежі.

- аналіз і вдосконалення процедур: регулярний аналіз ефективності пожежних заходів і процедур з метою виявлення слабких місць і вдосконалення системи управління пожежною безпекою.

Ці заходи не лише сприяють відповідності законодавчим вимогам, але й демонструють відповідальний підхід до пожежної безпеки як складової частини корпоративної культури та соціальної відповідальності підприємства.

ВИСНОВКИ

Результатом кваліфікаційної роботи є розроблений проект локальної мережі рекламного бюро «Бум». Основні технічні характеристики розробленого проекту локальної мережі:

- фізична топологія – «гібридна»;
- технології використані для розробки мережі - IEEE 802.3ab, IEEE 802.11n, IEEE 802.11 ac, IEEE 802.1Q;
- маршрутизатор-шлюз – DrayTek Vigor2962;
- комутатори робочих груп – DrayTek VigorSwitch P2280x;
- безпровідна точка доступу – TP-LINK EAP110
- стек протоколів локальної мережі - TCP/IP версії 4.

В кваліфікаційній роботі спроектовано логічну та фізичну топологію мережі. Підібрано відповідне апаратне та програмне забезпечення. При виборі апаратного забезпечення (активного) враховано можливість масштабування локальної мережі в майбутньому.

Описано процедуру налаштування файлового, DHCP- та web-севрера, активного комутаційного обладнання. Розроблено інструкцію з тестування та налагодження мережі.

Логічна та фізична топології локальної мережі подано в графічній частині.

В економічній частині зроблено розрахунком повної вартості робіт по проектуванню, встановленню і запуску в експлуатацію мережі. Отримана вартість мережі є в межах запропонованої замовником.

Останній розділ роботи описує питання охорони праці, та техніки безпеки, які є важливими для безпечної праці користувачів комп’ютерної техніки

ПЕРЕЛІК ПОСИЛАНЬ

1. Базові поняття мережевих технологій. Доступно: http://um.co.ua/8/8-17/8-1748.html. Дата звернення: 5.03.2024.
2. Буров Є., Митник М. Комп'ютерні мережі. (у 2-х томах) Львів, Магнолія, 2018.
3. Єфіменко А. А. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco : навчальний посібник. – Житомир : Житомирська політехніка, 2021. – 116 с.
4. Запорожець О. І.. Основи охорони праці. Підручник. – К.: Центр учбової літератури, 2019. – 264 с.
5. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навчальний посібник. – Вінниця: ВНТУ, 2015./МОНУ (Лист №1/11 – 8260 від 15.05 2015 р.) – 500 с.
6. Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Підприємстватво Львівської політехніки, 2021. – 188 с.
7. Охорона праці (гігієна праці та виробнича санітарія) : навч. посіб. / І. П. Пістун, В. О. Тимочко, І. М. Городецький, А. П. Березовецький; за ред. І. П. Пістуна. – Львів: Тріада плюс, 2015. — 223 с.
8. Products Vigor2962 [Електронний ресурс] - Режим доступу: URL: https://www.draytek.com/products/vigor2962#null Дата доступу: 26.05.2025.
9. Products VigorSwitch P2280x [Електронний ресурс] - Режим доступу: URL: https://www.draytek.com/products/vigorswitch-p2280x Дата доступу: 26.05.2025.
10. FreeBSD у деталях. Про плюси та мінуси системи URL: https://hyperhost.ua/info/uk/freebsd-u-detalyax-pro-plyusi-ta-minusi-sistemi. (Дата звернення: 14.05.2025)
11. FreeBSD 14 URL: https://www.freebsd.org/releases/14R/schedule/ (Дата звернення: 20.05.2025)

12. Джерело безперебійного живлення APC Back-UPS 1500 BA, авторегулювання напруги, 230 В, СНД URL: https://www.apc.com/ua/uk/product/ BR1500G-RS. (Дата звернення: 7.06.2025).

13. КПВ-ВП (250) URL: https://lantorg.com/products/odeskabel-kpv-vp-250-4h2h057-utp---cat6-vnutrenniy- korobka-305m/. (Дата звернення: 6.06.2025).

14. Одескабель Cat.6 URL: https://odeskabel.com/ua/products/katalog-lan/lan-kabeli-kategorii-6/uutp-4pr-indoor.html. (Дата звернення: 29.05.2025).

15. Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/50100109012007214 4/lang/en. (Дата звернення: 29.05.2025).

16. Поширені питання про життєвий цикл–Windows URL: https://learn.microsoft.com/uk-ua/lifecycle/faq/windows. (Дата звернення: 19.05.2025).

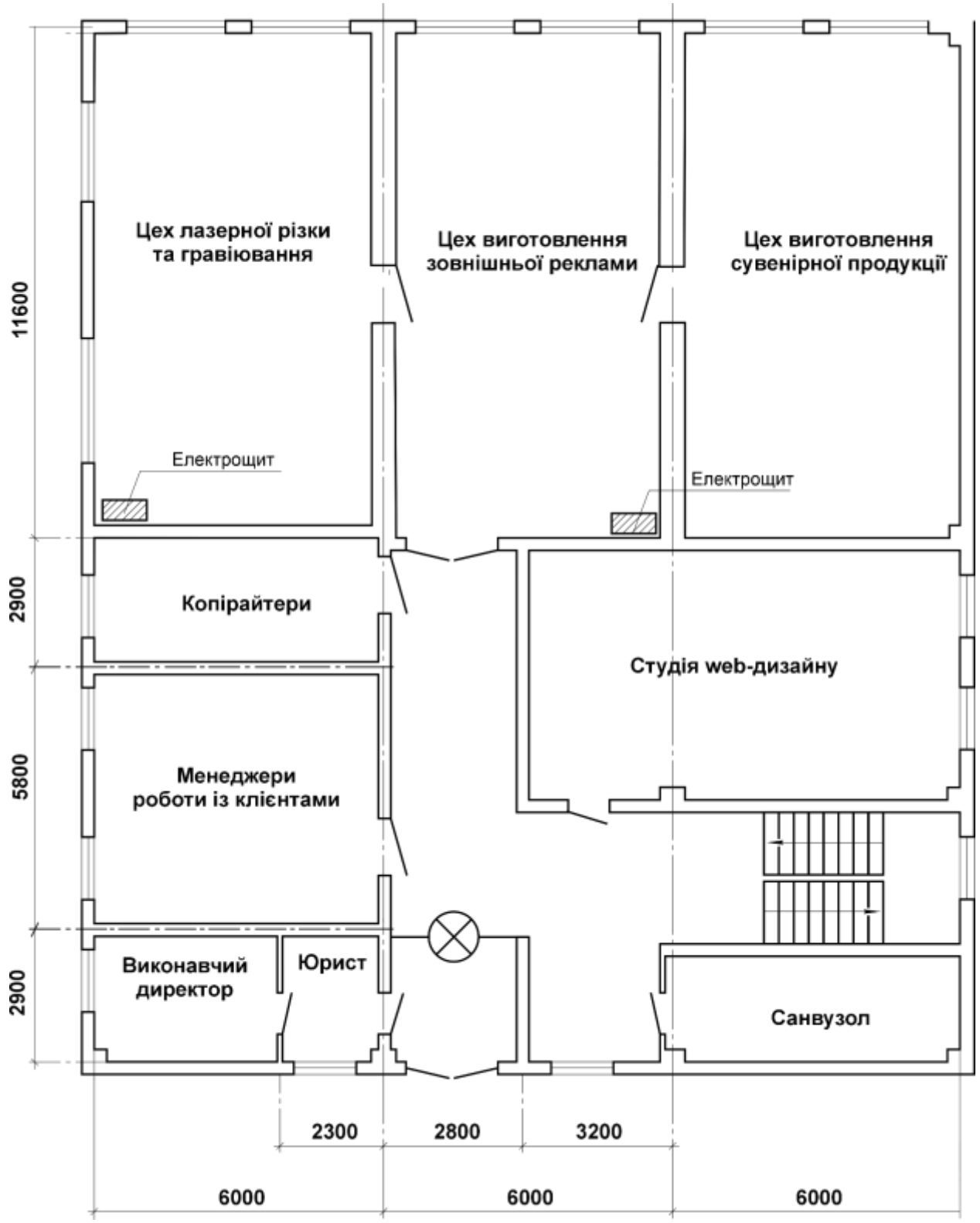
17. Сервер двопроцесорний TOWER PowerUp #51 Xeon E5 2680 v4 x2/256 GB/HDD 6 TB/SSD 512GB x2 Raid/Int Video. URL: https://powerup.ua/server-dvukhprotsessornyy-tower-powerup-51-xeon-e5-2680-v4-x2-256-gb-hdd-6-tb-ssd-480-gb-kh2-raid-int-video/. (Дата звернення: 24.05.2025)

18. Телефонна + комп'ютерна розетка RJ11 + RJ45, кат. 6, неэкр. UTP з пружинними затискачами, Алюміній, Sedna SDN5200160. URL: https://schneider.kiev.ua/telefonna--kompyuterna-rozetka-rj11--rj45-kat-6-neekr-utp-z-pruzhinnimi-zatiskachami-alyuminij-sedna-sdn5200160. (Дата звернення: 6.06.2025).

ДОДАТКИ

Додаток А. План будівлі рекламного бюро “Бум”

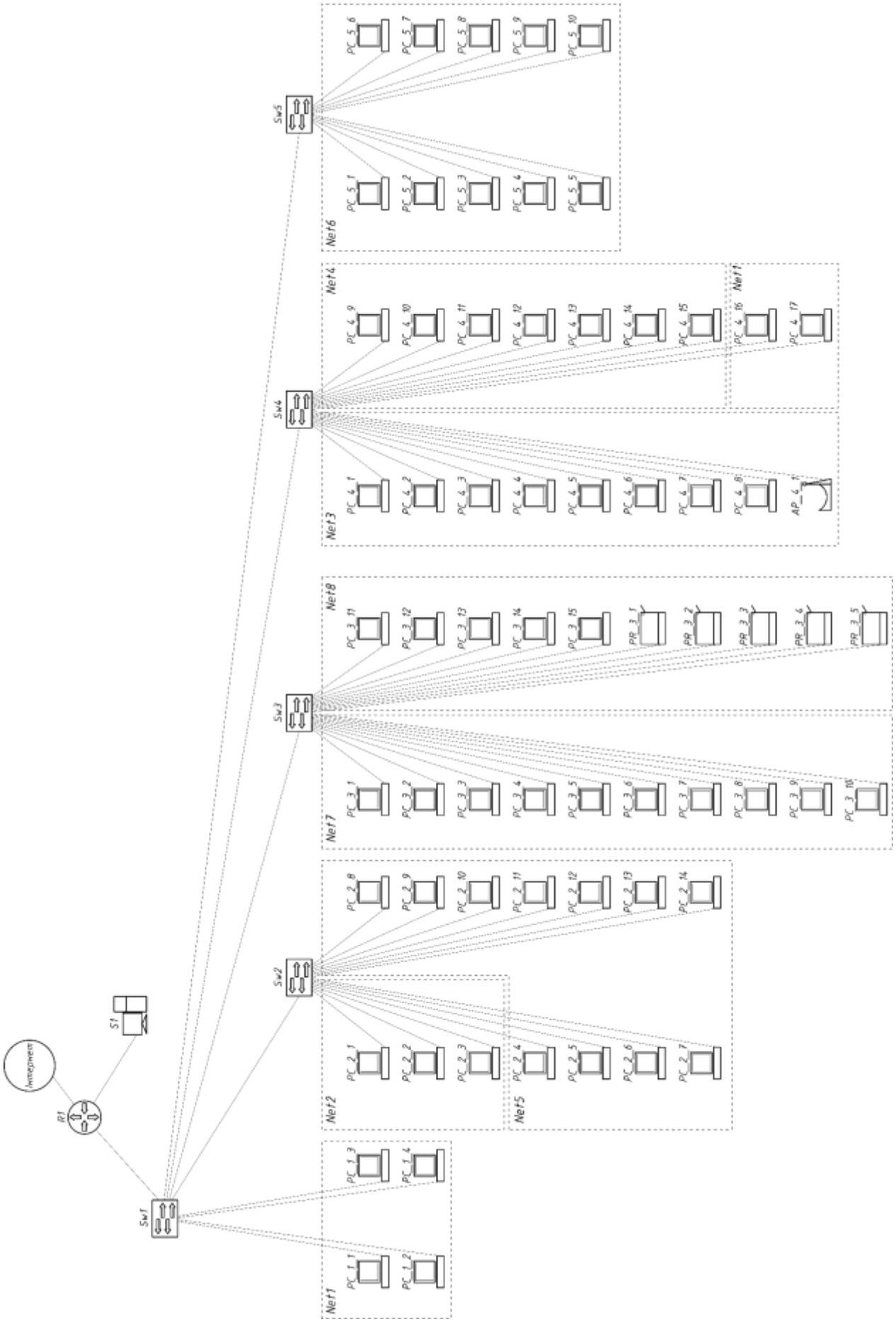
1 поверх



2 поверх

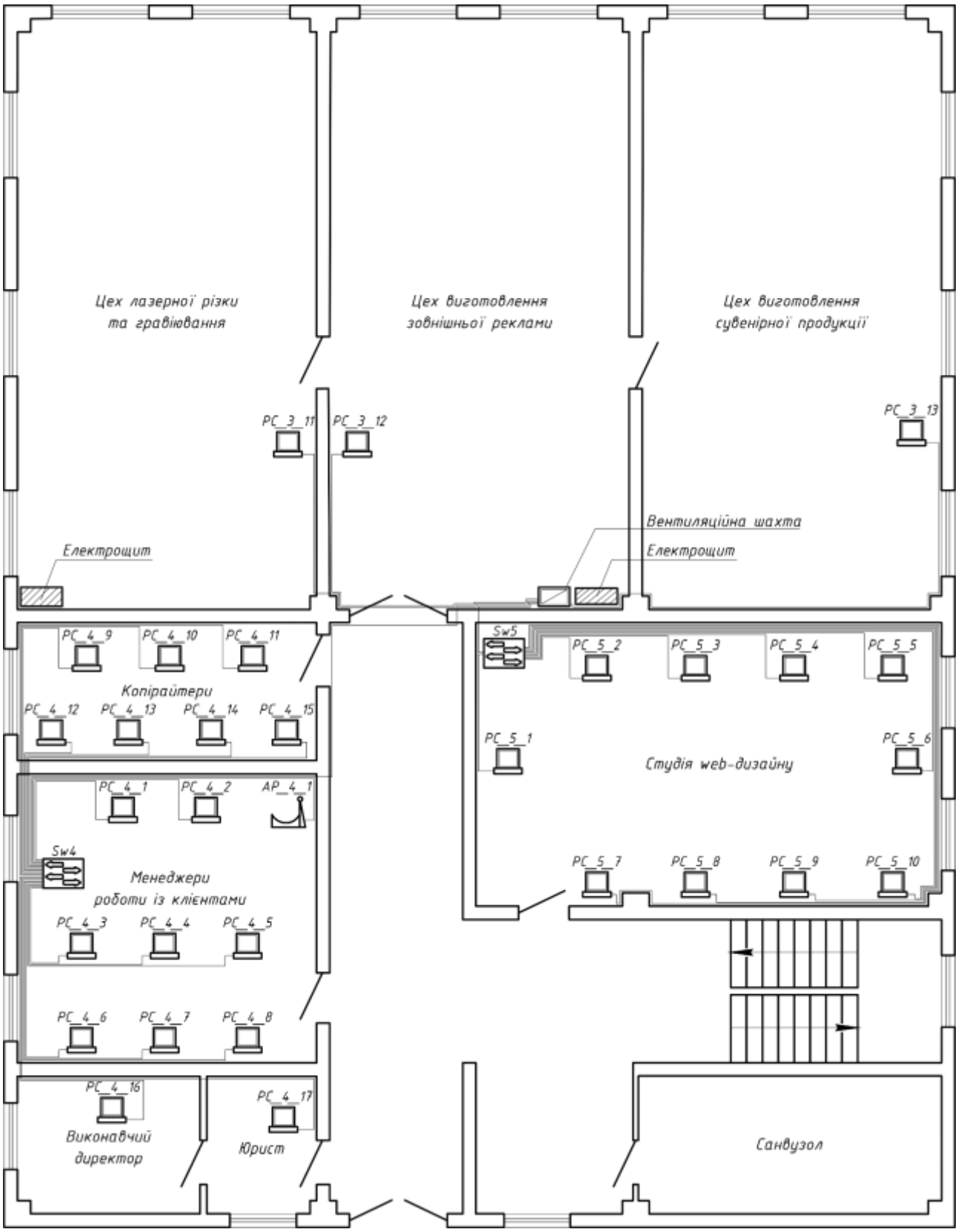

Цех виготовлення сувенірної продукції
Оператори цифрового друку
Верстальники
HR-Менеджери
Серверна
Директор
Прийомна (Офіс-менеджер)
Дизайнери
Бухгалтерія
Санвузол
11600
2900
5800
2900
6000
6000
6000

ДОДАТОК Б. Логічна топологія мережі

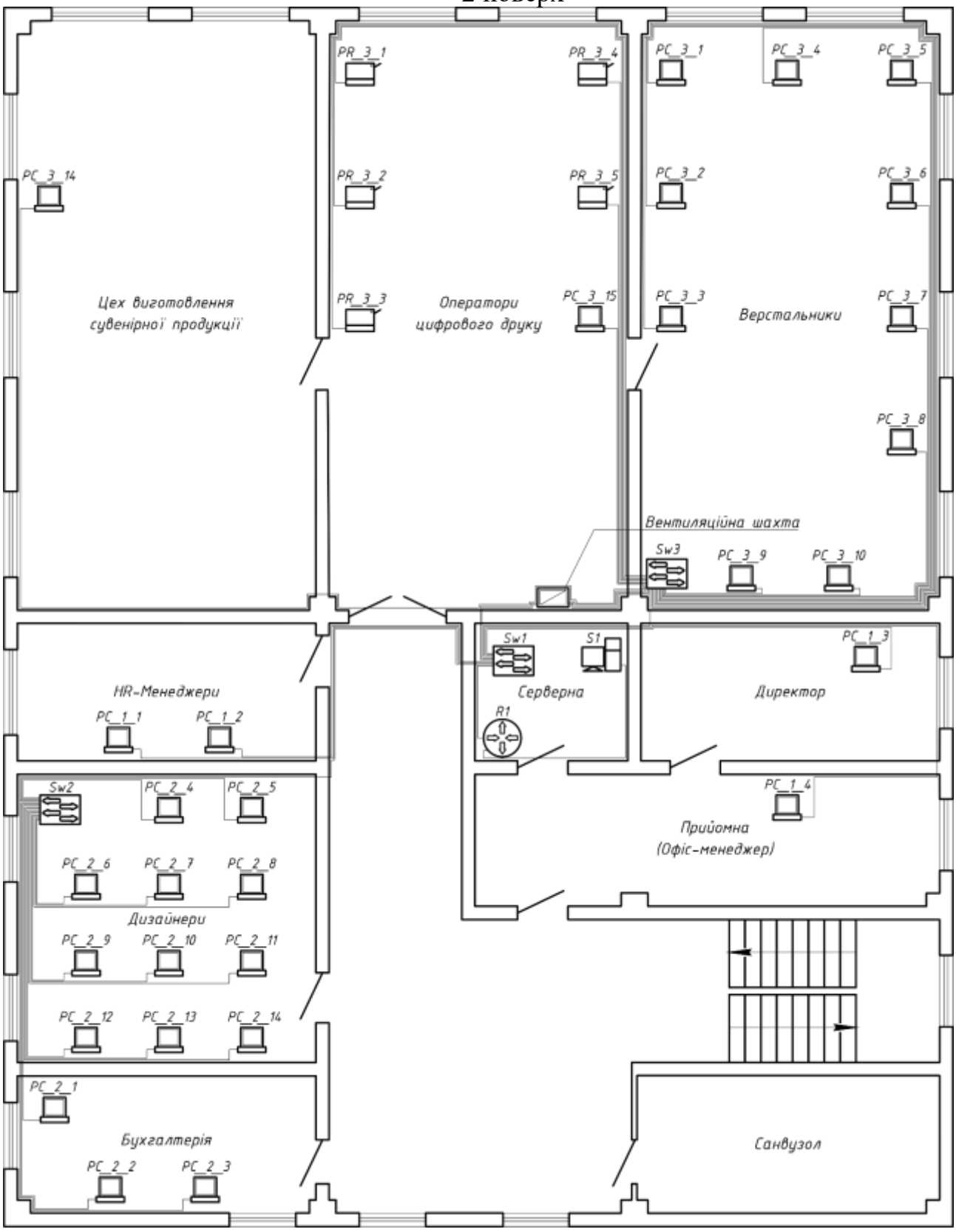


ДОДАТОК В. Горизонтальна підсистема СКС мережі

1 поверх



2 поверх


PR_3_1
PR_3_4
PC_3_1
PC_3_4
PC_3_5
PC_3_14
PR_3_2
PR_3_5
PC_3_2
PC_3_6
PR_3_3
PC_3_15
PC_3_3
PC_3_7
Цех виготовлення сувенірної продукції
Оператори цифрового друку
Верстальники
PC_3_8
Вентиляційна шахта
Sw3
PC_3_9
PC_3_10
Sw1
S1
PC_1_3
HR-Менеджери
Серверна
Директор
PC_1_1
PC_1_2
R1
Sw2
PC_2_4
PC_2_5
PC_1_4
Прийомна (Офіс-менеджер)
PC_2_6
PC_2_7
PC_2_8
Дизайнери
PC_2_9
PC_2_10
PC_2_11
PC_2_12
PC_2_13
PC_2_14
PC_2_1
Бухгалтерія
Санвузол
PC_2_2
PC_2_3