Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра

(освітній ступінь)

на тему: **Розробка проекту комп'ютерної мережі Івано-Франківського відділення ТзОВ «ВНС Group**

Виконав: студент VI курсу, групи КІб-602

Спеціальності **123 Комп'ютерна інженерія**

(шифр і назва спеціальності)

_____ Віталій ЗВІРИШИН

(ім'я та прізвище)

Керівник Ігор ГЕНИК

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

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"06" травня 2025 року

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

Звіришину Віталію Тадейовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи **Розробка проекту комп'ютерної мережі Івано-Франківського відділення ТзОВ «ВНС Group**

керівник роботи Геник Ігор Степанович
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 05.05.2025 р №4/9-217.

2. Строк подання студентом роботи: 23 червня 2025 року.

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

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

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

- План приміщень
- Логічна топологія
- Фізична топологія
- Таблиця IP-адрес
- Таблиця техніко-економічних показників
- Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА заст. директора з НВР		
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	06.05	
2	Збір і узагальнення інформації	19.05	
3	Написання першого розділу	23.05	
4	Розробка технічного та робочого проекту	28.05	
5	Написання спеціального розділу	3.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	12.06	
9	Оформлення проекту	16.06	
10	Погодження нормоконтролю	18.06	
11	Попередній захист роботи	20.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 06 травня 2025 року

Студент _____ Віталій ЗВІРИШИН
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Звіришин В.Т. Розробка проєкту комп'ютерної мережі Івано-Франківського відділення ТзОВ «BHC Group»: кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2025. -86с.

Кваліфікаційна робота присвячена проєктуванню комп'ютерної мережі. На основі аналізу сучасних стандартів мережевої інфраструктури було обґрунтовано вибір логічної та фізичної топології, активного і пасивного мережевого обладнання, серверного устаткування та програмного забезпечення. Розроблено схему IP-адресації, реалізовано сегментацію мережі за допомогою VLAN, а також обґрунтовано вибір операційної системи, засобів тестування та захисту мережевої інфраструктури.

Описано процес встановлення й налаштування мережевого обладнання та серверів. Проведено моделювання функціонування мережі для оцінки її ефективності

Ключові слова: локальна комп'ютерна мережа, віртуальна мережа, сервер, комутатор.

ANNOTATION

Zviryshyn V.T. Computer Network Project Development of Ivano-Frankivsk Branch of "BHC Group" LLC: qualification work for obtaining a bachelor's degree, specialty 123 Computer Engineering. Ternopil: Separate Structural Subdivision "Ternopil Professional College of Ivan Puluj National Technical University", 2025. -86p.

The qualification thesis is devoted to the design of a computer network. Based on the analysis of modern networking infrastructure standards, the selection of logical and physical topologies, active and passive network equipment, server hardware, and software is substantiated. An IP addressing scheme was developed, network segmentation using VLANs was implemented, and the choice of operating system, testing tools, and network security measures was justified. The process of installing and configuring network equipment and servers is described. Network modeling was conducted to assess its efficiency.

Keywords: Local Area Network, Virtual Network, Server, Switch.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

802.3ad (Link Aggregation) – технологія об’єднання каналів зв’язку;

802.3ae - 10 GbE;

DNS (Domain Name System) - сервер доменних імен;

EIA (Electronic Industries Association) – асоціація електронної промисловості;

IEEE 802.3 - 10BASE-T Ethernet;

IEEE 802.3ab - 1000BASE-T Gigabit Ethernet;

IEEE 802.3u - 100BASE-TX Fast Ethernet;

IP (Internet Protocol) – Інтернет-протокол;

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) - апаратна адреса ПК;

NAT (Network Address Translation) – мережева трансляція адес;

OSI (Open System Interface) – модель з’єднання відкритих систем;

QoS – технологія пріоретизації пакетів, що проходять через мережене обладнання;

SNMP (Simple Network Management Protocol) – протокол керування мережею;

Spanning Tree Protocol – алгоритм покриваючого дерева, використовується для прокладання резервних зв’язків між вузлами;

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

UTP (Unshielded Twisted Pair) – кабель типу неекранована скручена пара;

КМ – комп’ютерна мережа;

ОС - операційна система;

ПК - персональний комп’ютер;

СКС – структурована кабельна система.

ВСТУП

Комп'ютерна мережа (КМ) **-** це організована система, призначена для спільного використання інформаційних ресурсів, апаратних засобів і програмного забезпечення [1]. Доцільність впровадження комп'ютерних мереж обґрунтовується не лише технічними потребами, а й значними економічними перевагами. Зокрема, використання локальних обчислювальних мереж (ЛОМ) сприяє скороченню витрат на інформаційно-комунікаційне обладнання та зменшенню непродуктивних витрат робочого часу персоналу.

У сучасних підприємствах комп'ютерні мережі забезпечують надійну основу для ефективної внутрішньої взаємодії між підрозділами, зокрема завдяки можливості спільного доступу до інформації, баз даних і програмних сервісів. Особливо важливу роль мережеві рішення відіграють у діяльності компаній, що спеціалізуються на оптовій і роздрібній торгівлі, де необхідна чітка координація між складами, торговими залами, офісами та пунктами доставки. У таких організаціях безперервний і швидкий обмін даними є критично важливим для забезпечення належного рівня обслуговування клієнтів, управління залишками продукції та ведення обліку.

Головною метою цієї кваліфікаційної роботи є проєктування локальної комп'ютерної мережі для Івано-Франківського філіалу ТзОВ «ВНС Group». У межах проєкту заплановано застосування таких сучасних технологій і стандартів, як фіксована маршрутизація (Static Routing), IEEE 802.1Q (VLAN), IEEE 802.3ab Gigabit Ethernet, а ще IEEE 802.3p (QoS). Відповідно до технічного завдання, потрібно обґрунтувати вибір фізичної та логічної топології мережі, здійснити підбір пасивного й активного мережевого обладнання, а також розробити настанови щодо встановлення та конфігурації шлюзу доступу до мережі Інтернет, файлового сервера , служби OpenVPN та інших компонентів інфраструктури.

Проєкт ґрунтується на застосуванні високопродуктивного та надійного обладнання, яке відповідає вимогам щодо стабільності, швидкості та здатності до масштабування мережі. Своєчасність роботи обумовлена впровадженням новітніх технологій і стандартів, які забезпечують ефективне вирішення завдань.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Назва роботи - Кваліфікаційна робота на тему: Розробка проекту комп’ютерної мережі Івано-Франківського відділення ТзОВ «ВНС Group».

Ця компанія здійснює свою діяльність у галузі мережевої та дрібнооптової торгівлі побутовою хімією, дитячої гігієни,тощо. Компанія активно співпрацює як з окремими торговцями, так і з національними мережами. ТзОВ «ВНС Group» має філії в більшості обласних центрів України.Івано-Франківський філіал, в інформаційному контексті, повинний здійснити допуск до всіх мережевих ресурсів фірми, незалежно де вони знаходяться.

Проект матиме практичне застосування як в межах цієї філії, так і в тих випадках, де необхідно буде створити об'єднану мережу кількох віддалених філій з захищеними каналами зв'язку.

1.1.2 Призначення розробки

Проєкт повинен відповідати наступним основним вимогам:

- Гарантування зв'язку між усіма робочими станціями в мережі;
- Забезпечення колективного доступу до ресурсів мережі та підключення до Інтернету;
- Закладення можливості подальшого масштабування мережевої інфраструктури (у випадку зростання кількості працівників) та зміни на більш сучасні стандарти передавання даних;

- Налагодження захищеної передачі інформації між віддаленими користувачами через безпечні канали з метою забезпечення конфіденційності даних.;

- Гарантування безперебійної роботи основних елементів мережі, уразливих до помилок;

- Конфігурація базових служб локальної мережі підприємства.

1.1.3 Вимоги до апаратного і програмного забезпечення

Для практичного втілення теми кваліфікаційної роботи необхідне підходяще апаратне та програмне забезпечення.

Мережевий шлюз (сервер для організації доступу в Інтернет). Виконує функції сервера для підключення працівників віддалених підрозділів компанії та забезпечує доступ офісних робочих станцій до мережі Інтернет. Конфігурація обов'язково повинна включати апаратний RAID-масив. Системні ресурси серверів слід обирати з урахуванням можливого збільшення навантаження в перспективі.

Головний комутатор повинен реалізовувати основні функції канального рівня моделі OSI та гарантувати стабільну швидку передачу даних 1000 Мбіт/с:

- 802.3ad Link Aggregation;
- 802.1D Spanning Tree;
- 802.1s Multiple STP;
- 802.1w Rapid Spanning Tree;
- Зеркалювання потрів.

Комутатори відділів мають підтримувати швидкість передавання даних на рівні 1000 Мбіт/с. Необхідною умовою є наявність реалізованої функції автоматичного узгодження швидкості. Кількість портів має бути не меншою за 8.

Серверне програмне забезпечення. Програмне забезпечення сервера доступу має підтримувати функціональність для створення захищених каналів зв'язку між офісами, використовуючи протокол SSL.

Програмне забезпечення комп'ютерів філії. В якості програмного забезпечення робочих комп'ютерів використано операційну систему Windows 10.

1.1.4 Вимоги до документації

У межах проєкту мережі планується така технічна документація: схема об'єднаної мережевої інфраструктури, інструкції з налаштування мережевих пристроїв та серверів, схема мережевої інфраструктури Івано-Франківського філіалу, фізична структура локальної мережі філії, план приміщення філії.

До технічної документації висуваються такі основні вимоги:

1. Повнота - документація повинна охоплювати всі компоненти мережевої інфраструктури, включаючи маршрутизатори, комутатори, сервери, кінцеві пристрої, кабельну систему та засоби захисту.

2. Актуальність - усі дані та конфігурації мають відповідати фактичному стану реалізованої мережі, з урахуванням останніх змін, оновлень та оновлень безпеки.

3. Структурованість - документи мають бути логічно впорядкованими: кожен розділ повинен чітко описувати окремий аспект проєкту (логічна структура, фізичне розташування, параметри налаштування тощо).

4. Деталізованість - кожна інструкція або схема має містити достатньо технічної інформації для відтворення або обслуговування налаштувань без потреби в додаткових джерелах.

5. Уніфікованість - уся документація має бути виконана в єдиному форматі (відповідно до вимог організації або стандартів, наприклад, ГОСТ чи ISO), з єдиним стилем позначень, скорочень, термінів та оформлення.

6. Наявність візуальних матеріалів - для зручності сприйняття та кращого розуміння необхідно включати схеми, діаграми, топологічні карти, плани приміщень з розміщенням обладнання.

7. Зручність обслуговування - документація повинна містити розділ із вказівками для обслуговування та модернізації мережі: резервні копії конфігурацій, дані для відновлення, опис типових збоїв і способів їх усунення.

8. Безпека доступу - доступ до конфіденційних частин документації (наприклад, облікові записи, паролі, IP-адресація серверів) має бути обмеженим і захищеним відповідно до політик інформаційної безпеки організації.

Наявність такої документації є критично важливою для забезпечення керованості, безперервної роботи, а також подальшого масштабування або супроводу створеної мережевої інфраструктури.

1.1.5 Техніко-економічні показники

Техніко-економічні параметри проєкту відображають ключові технічні та економічні аспекти локальної мережі. Розглянемо ключові з них: програмне втілення технології VPN – OpenVPN,основна технологія об'єднаної мережі – VPN, технологія організації локальної мережі – 1000 Base-TX, фізична топологія – розширена зірка, локальна мережа, що використовує технологію комутації пакетів, технологія з’єднання з Інтернетом – NAT, програмний файрвол - ipfw, ОС робочих станцій – Windows 10 Prof, ОС шлюзового сервера – FreeBSD 13, ціна мережі – до 450 тис грн., очікуваний прибуток - не нижчий за 50 тис. грн.

1.1.6 Стадії та етапи розробки

Проєкт комп’ютерної мережі для фірми включає такі основні етапи:

- Створення логічної структури мережі філії фірми.
- Створення фізичної структури мережі філії фірми.

- Визначення складу пасивного і активного обладнання, необхідного для реалізації мережі.
- Створення логічної структури об’єднаної мережі.
- Конфігурація серверів підрозділів фірми.
- Тестування мережі.

1.1.7 Порядок контролю та прийому

На фінальному етапі проєктування комп’ютерної мережі слід провести тестування ключових технічних параметрів мережі. Вони мають відповідати встановленим вимогам.

Передусім перевіряється функціональність мережевої інфраструктури, зокрема доступність основних вузлів, стабільність маршрутизації, відповідність VLAN-сегментації та правильність розмежування доступу. Використовуються утиліти типу ping, traceroute, netstat, а також інструменти аналізу трафіку для виявлення потенційних затримок або втрат пакетів.

Особливу увагу приділяють тестуванню швидкості передачі даних, як усередині сегментів LAN, так і між віддаленими підмережами. Застосовуються сервіси на кшталт iPerf або NetIO для вимірювання пропускної здатності та виявлення вузьких місць.

Крім цього, перевіряється стабільність роботи серверних служб (DNS, DHCP, VPN, файлових сервісів), а також відмовостійкість інфраструктури, зокрема працездатність у разі відключення окремих вузлів або портів.

Також тестується дотримання політик безпеки, наприклад, обмеження доступу між VLAN, фільтрація трафіку через міжмережеві екрани (firewall), коректність NAT, наявність відповідних правил фільтрації та журналювання подій.

У разі виявлення недоліків або невідповідностей проводиться доопрацювання конфігурацій та повторне тестування, до моменту досягнення

стабільної та відповідної до технічного завдання роботи мережі. Завершення цього етапу засвідчується підписанням акту введення системи в експлуатацію.

Для контролю за технічними параметрами мережі будуть використовуватися інструменти, описані в розділі 3.2 «Інструкція з використання тестових наборів та тестових програм».

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі

Основним завданням цієї кваліфікаційної роботи є розробка комп'ютерної мережі для Івано-Франківської філії ТзОВ «ВНС Group». Мережа має відповідати таким вимогам:

- Надійність. З підвищенням залежності співробітників від мережі, її простої матимуть високі витрати. Важливо знайти рішення, що гарантують підвищену надійність, належну гарантію та ефективні стратегії обслуговування.
- Планування мережі. З ростом чисельності працівників вимоги до мережі також збільшуватимуться. Це зумовлено двома аспектами: збільшенням складності мережевого ПЗ та збільшенням ролі мережі у роботі кожного працівника фірми. Ключове питання при проектуванні будь-якої мережі Це забезпечення збереження інвестицій в обладнання: апаратне забезпечення, що застосовується зараз, повинно бути придатним для використання і в майбутньому, коли мережа розшириться.
- Масштабованість. З часом постане потреба в додаткових робочих станціях, а також у введенні нового мережевого ПЗ та сервісів. Мережа повинна бути спроектована з урахуванням резерву пропускної здатності.
- Захист. Будь-яка мережа потребує певної форми захисту. застосування захищеного протоколу SSL дозволить уникнути витоку важливих даних. До того ж, ефективним буде використання фільтрування мережевого трафіку та технологію для формування адміністративних груп користувачів [8].

ТзОВ, для якого створюється проект, має кілька підрозділів (і в майбутньому їх число може бути змінена), серед яких один є головним. Треба розробити мережу для Івано-Франківського філіалу фірми та об’єднати всі корпуси в єдину корпоративну мережу. Процес об’єднання всіх віддалених корпусів передбачає їх підключення до Інтернету (як таке під’єднання відсутнє), під час підключення важливо звернути увагу на пропускну здатність Інтернет-каналу та його симетричність.

Потрібно здійснити конфігурацію сервера для кожної філії (інсталювати ОС FreeBSD, OpenVPN), Провести налаштування міжмережевого екрану для кожного сервера згідно з вимогами IPFW та OpenVPN. Інструкції з конфігурації зазначених програмних продуктів можна знайти в розділі 3.1 «Інструкція з інсталяції програмного забезпечення серверів та активного комутаційного обладнання».

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

У локальній мережі Івано-Франківської філії фірми застосовується технологія Gigabit Ethernet. Вибір цієї технології пояснюється тим, що вона забезпечує необхідний запас пропускної здатності для майбутнього розширення мережі. Зокрема, технологія Gigabit Ethernet має перевагу завдяки своїй відносно низькій ціні порівняно з іншими технологіями.

Gigabit Ethernet функціонує на основі технології комутації пакетів. Принцип функціонування цієї технології зводиться до того, що дані, що передаються від абонента, розбиваються на маленькі частини – пакети (packet), за допомогою передавального вузла. Зазвичай розмір пакету складає одиниці кілобайт. Кожен пакет містить заголовок, що містить адресу отримувача та порядковий номер пакету в потоці даних [5].

Суть передачі пакетів у тому, що маршрути для передавання даних є незалежними та не повторюються. Тому, коли один пакет випадково втрачається, всі інші зберігаються, а втрачені пакети передаються повторно за допомогою альтернативного маршруту.

Щоб уникнути коливаь трафіку в каналах передачі даних, застосовується проміжна пам'ять комутатора чи маршрутизатора, де пакети зберігаються тимчасово для їх подальшого збирання в єдину одиницю. Пакети даних інколи також називають дейтаграмами (datagram).

Спочатку може здатися, що мережі з комутацією пакетів можуть знижувати швидкість передачі даних між хостами, Оскільки пакети даних можливо будуть «затримуватися» в буферній пам'яті, чекаючи на отримання решти частин пакетів, поки не буде здійснено збирання даних. Проте аналіз математичної статистики довів , що загальна ефективність (Об'єм переданих

даних за певний період часу) комутації пакетів значно перевищує ефективність технології комутації каналів [1].

Головний недолік мереж, побудованих за протоколом Ethernet, заключається в тому, що при спробі одночасного доступу до каналу зв'язку збільшується кількість конфліктів (зіткнень пакетів). У такому випадку одразу значно знижується пропускна здатність мережі.

Логічна топологія локальної мережі щільно взаємопов'язана з поняттям фізичної топології. Пояснення вибору фізичної топології представлено в розділі 2.2.

Якщо компанія має кілька відділень, розташованих на значній відстані одна від одної, виникає проблема створення з'єднаної корпоративної мережі підприємства. Для цього застосовують декілька методів: Найбільш витратним з фінансової точки зору є створення виділених каналів зв'язку (переважно оптичних) між локальними мережами підрозділів фірми, другий варінат – застосування мережі Інтернет як каналу передачі даних для корпоративного трафіку. При застосуванні другого варіанту виникає проблема гарантування безпеки та цілісності даних, що передаватимуться через публічні мережі. Прийняття одного з варіантів об'єднання підрозділів у корпоративну мережу залежить від цілей компанії та обсягу інвестицій, необхідних для цього [4].

У цьому випадку для здійснення з'єднання віддалених відділень між собою буде налаштована віртуальна особиста мережа (Virtual Private Network, VPN). Це сукупність технологій, які забезпечують передавання даних через мережу Інтернет, але забезпечують конфіденційність, захист та нерозривність даних, що поширюються через публічну мережу.

Ураховуючи всі стандарти створення VPN та враховуючи недоліки і переваги для побудови розподіленої мережі фірми застосуємо технологію на основі OpenVPN, схема застосування показана на рисунку 2.1.

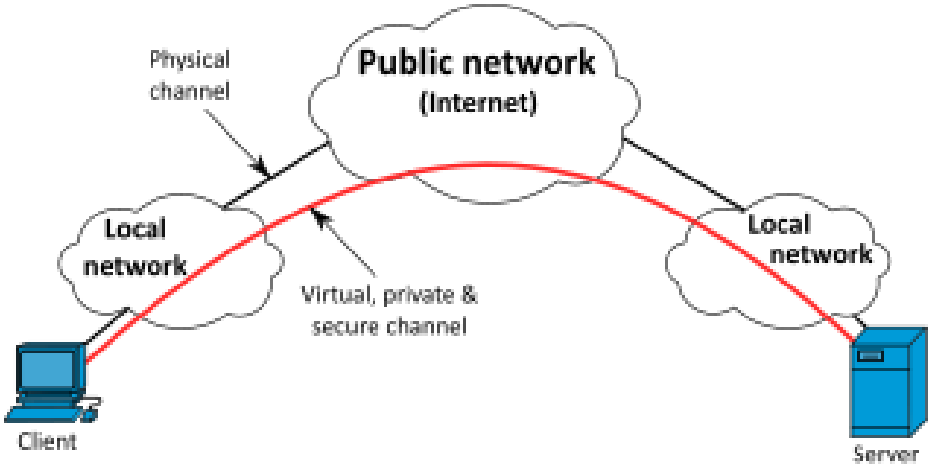

Рисунок 2.1 – Схема використання VPN

Як зазначалося раніше, локальна мережа філії фірми організована з застосуванням технології Gigabit Ethernet. Для розподілу широкомовного домену ЛОМ буде застосовано технологію VLAN стандарту Gigabit Ethernet.

За допомогою VLAN можна досягти таких результатів [6]:

- Створити мережу з окремою логічною структурою;
- Розділити один широкомовний домен колізій на декілька. Це дозволяє істотно знизити навантаження на мережеві пристрої;
- Забезпечити захист мережі від несанкціонованого доступу на апаратному рівні, через обмеження доступу на порту для пакетів з інших VLAN, при цьому незалежно від початкової IP-адреси;
- Використовувати спільні політики для всієї групи;
- Виконувати маршрутизацію за допомогою засобів віртуальних портів.

У таблиці «Логічна адресація в ЛОМ» додатку Б наведено інформацію про розподіл ЛОМ головного офісу на відокремлені підмережі.

У таблиці «Таблиця конфігурування VLAN» додатку Б надано інформацію про типи портів комутаторів для налаштування VLAN.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з’єднань та їх прокладка

Для організації кабельної системи локальної мережі стандарту Gigabit Ethernet застосовуватиметься неекранована вита пара категорії 6.

Фізична топологія «розширена зірка» об'єднуватиме комутатори робочих груп. Її представлено на рисунку 2.2. [2]

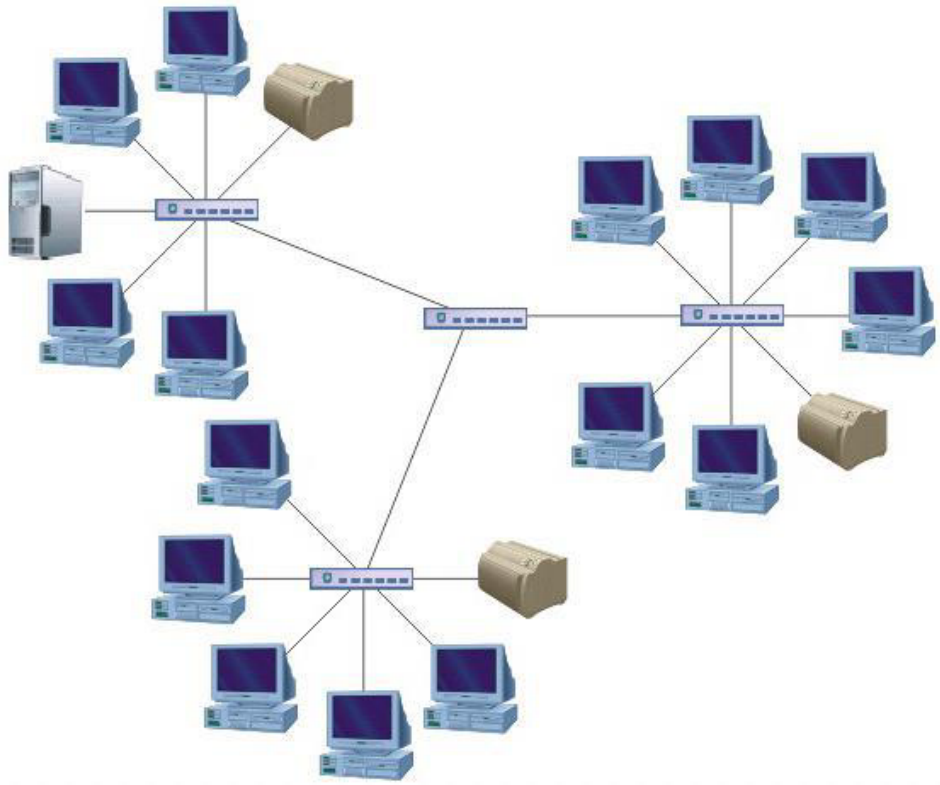

Рисунок 2.2 – Фізична топологія Розширена Зірка

У зв'язку з тим що планується застосування бездротового маршрутизатора, тому для з'єднання всіх вузлів між собою буде застосовано гібридну фізичну топологію. На рисунку 2.3 представлено схему такої топології.

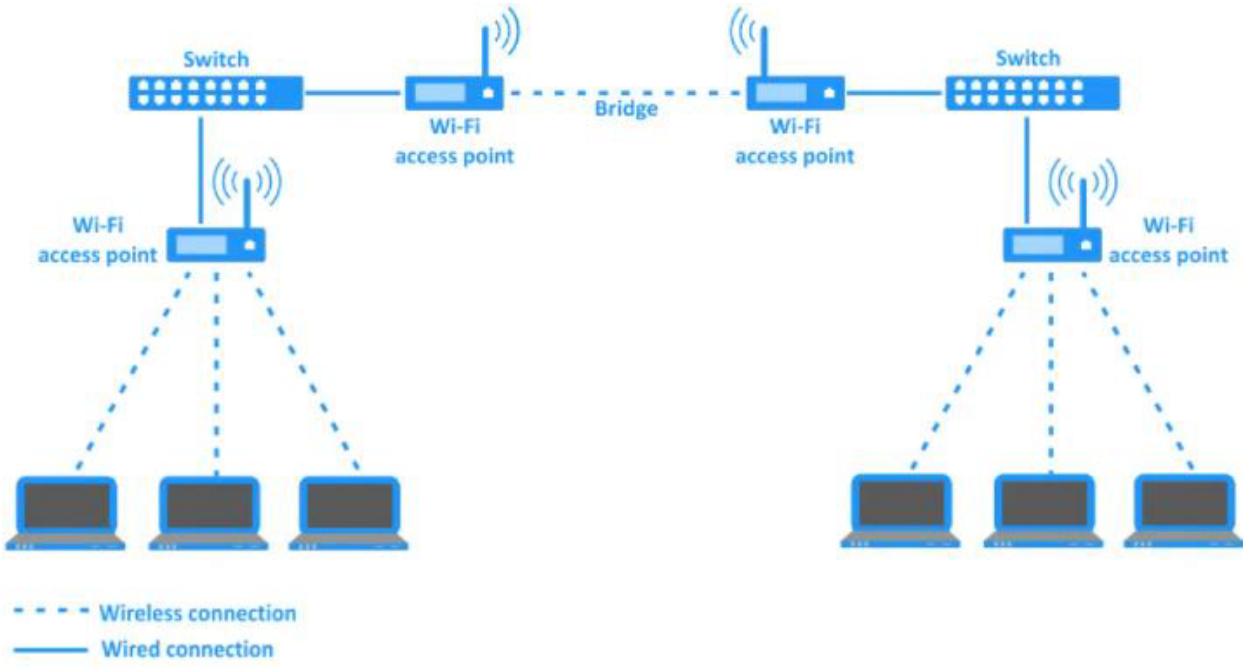

Рисунок 2.3 – Гібридна фізична топологія

2.2.2 Будова вузлів та необхідність їх застосування

Кожна комп'ютерна мережа формується з вузлових компонентів. У даному випадку до вузлових елементів можна зарахувати комутатори відділів, шлюз Інтернет-доступу і центральний гігабітний комутатор [1].

Комутатори відділів з'єднують робочі станції окремих філій між собою. Шлюз Інтернет-доступу надає усім можливість виходу в Інтернет, розподіл смуги пропускання, фільтрація трафіку.

Головний комутатор з'єднує всі інші вузли мережі між собою. З використанням ОС комутатора можна розподілити широкомовний домен на сегменти (віртуальні мережі).

Цей метод сприяє поліпшенню швидкісних параметрів мережі, та дозволяє знизити навантаження на технічні засоби.

У серверній кімнаті розташований основний комутаційний вузол, який включає в себе комутаційне обладнання та сервери. У якому розташована блоки безперебійного живлення, активне комутаційне обладнння та комутаційна шафа

. Також у комутаційній шафі знаходиться патч-панель, задля зручності монтажу та оперативної комутації портів мережевого обладнання.

2.3 Обґрунтування вибору мережевого обладнання

Під час створення комп'ютерної мережі застосовують як пасивне, так і активне комунікаційне обладнання. Пасивне та активне комунікаційне обладнання обирається з урахуванням підтримки певних стандартів і технологій, а також вимог замовника.

В таблиці «Порівняльна характеристика апаратних платформ серверів» додатку В зроблено порівняння характеристик серверів різних фірм-виробників. Для порівннян було вибрано три популярні на українському ринку на даний час моделі для офісних мереж середнього масштабу: ARTLINE Business R19, HPE ProLiant DL20 Gen10 Plus та Lenovo ThinkSystem ST250 V2.

З огляду на визначені в стандартах параметри для корпоративної мережі, було обрано серверну модель ARTLINE Business R19, зображену на рисунку 2.4. Однією з ключових переваг цього рішення, окрім високої надійності та потужних технічних характеристик, є його форм-фактор, що дозволяє встановлення в стандартну 19-дюймову серверну стійку. Це значно спрощує подальше адміністрування та обслуговування мережевої інфраструктури.

Додатковим аргументом на користь вибору саме цієї моделі стало оптимальне співвідношення вартості та функціональних можливостей. Важливо також зазначити, що сервер ARTLINE Business R19 вже оснащено продуктивною дисковою підсистемою, що дозволяє уникнути додаткових витрат на придбання окремих накопичувачів [28].

Рисунок 2.4 – Сервер ARTLINE Business R19

Ідентична серверна конфігурація буде застосована для створення файлового сервера. Додатково до нього буде встановлено жорсткі диски обсягом по 4 ТБ кожен, що забезпечить необхідний рівень зберігання даних.

Для забезпечення взаємозв’язку між усіма мережевими вузлами використано комутатор, який виконує функцію комутації пакетів даних між окремими хостами мережі. У додатку В у таблиці «Порівняльний аналіз 16-ти портових комутаторів робочих груп» представлено технічне порівняння моделей, які можуть бути використані як комутаційні елементи в локальній мережі робочої групи.

У межах побудови локальної мережі було обрано комутатор серії D-Link DGS-1100-16, який повністю відповідає поставленим технічним вимогам. Його зображення наведено на рисунку 2.5. Зазначена модель вирізняється вигідною ціною при достатньому рівні функціональності, що стало визначальним критерієм при виборі [18].

Рисунок 2.5 - Комутатор D-Link DGS-1100-16

Додаткові технічні особливості комутатора наведено згідно з джерелом [18]:

Базові портові функції включають:

- підтримку стандартів IEEE 802.3 та IEEE 802.3u;
- можливість комутації пакетів у режимах повного та напівдуплексу;
- автоматичне узгодження швидкості передачі даних між передавачем і приймачем;
- автоматичне визначення типу з’єднання MDI/MDI-X;
- підтримку управління широкомовними потоками згідно зі стандартом IEEE 802.3x у повнодуплексному режимі.

У комутаторі D-Link DGS-1100-16 реалізовано розширені функції керування, зокрема:

- веб-інтерфейс для конфігурації та адміністрування (з підтримкою IPv4);
- програмне забезпечення SmartConsole для зручного управління;
- функцію обмеження доступу на основі пароля;
- гнучке налаштування параметрів портів, зокрема швидкості передачі, дуплексного режиму та управління потоком даних.

Комутатор цього типу використовується для об’єднання робочих станцій у межах окремого сегмента мережі. Як пристрій для сегментування локальної мережі додатково застосовуватимуться 8-портові комутатори тієї ж серії D-Link DGS-1100, зображені на рисунку 2.6. За технічними характеристиками вони є подібними до моделі з 16 портами, проте мають меншу кількість портів, що

позитивно впливає на їхню вартість та робить їх більш доцільними для використання в окремих частинах мережі з обмеженою кількістю підключень.

Рисунок 2.6 - Комутатор D-Link DGS-1100-8

Аналітичну інформацію, що була використана для обґрунтування вибору центрального комутатора мережі, подано в таблиці «Порівняльний аналіз центральних комутаторів», яка розміщена у додатку В.

Для побудови локальної мережі було обрано модель комутатора TP-Link T3700G-28TQ, зображену на рисунку 2.7 [19]. Даний комутатор буде використовуватись як центральний елемент комутації сегменту мережі або об’єднаної групи вузлів. Такий вибір зумовлений відповідністю технічних характеристик пристрою до вимог проєктованої мережі, а також його функціональними можливостями та високим MTBF.

Рисунок 2.7 - Комутатор TP-Link T3700G- 28TQ

У таблиці 2.1 наведено практично повний перелік активного та пасивного мережевого обладнання, що планується до використання під час проєктування локальної мережі підприємства.

Таблиця 2.1 – Активне та пасивне обланання для проектування ЛОМ

№	Опис	Од. вим.	К-сть	Ціна, грн.	Сума, грн.
1	Комутаційна шафа висота 18U	шт.	1	8760	8760
2	Комутаційна шафа висота 7U	шт.	6	5600	33600
3	Патчпанель, 24 порти, категорія 6	шт.	1	2000	2000
4	Патчпанель Panduit, 16 портів, категорія 6	шт.	6	1300	7800
5	Патчкорд UTP кат. 6	шт.	40	15	600
6	Короб	м.	105	60	6300
7	Кабль UTP (кат. 6), Одескабель	м.	610	23,30	14213
8	Мережева розетка UTP (кат. 6)	шт.	40	100	4000
9	Блок безперебійного живлення APC 1500VA Smart-UPS	шт.	1	18200	18200
10	Комутатор TP-Link T3700G- 28TQ	шт.	1	26900	26900
11	Комутатор робочих груп D-Link DGS-1100-08	шт.	3	1900	5700
12	Комутатор робочих груп D-Link DGS-1100-16	шт.	2	3300	6600
13	Файловий сервер ARTLINE Business R19	шт.	1	63000	63000
14	Сервер-шлюз ARTLINE Business R19	шт.	1	63000	60000
Загальна сума, грн.					260673

2.4 Особливості монтажу мережі

Створення локальної мережі умовно можна поділити на кілька етапів [3]:

- Затвердження з клієнтом шляхів і точних місць для монтажу комутаційної шафи, груп комутаторів, кабельних трас, та прокладання коробів.
- Підготовка об'єктів для установки мереж;
- Установка та перевірка кабельної мережі;
- Установка активного мережевого обладнання;
- Конфігурація робочих станцій ,програмного забезпечення комутаторів та серверів .

Усі ці етапи потребують ретельної уваги, оскільки вони взаємозалежні.

Структуровану кабельну систему локальної мережі фірми будується на основі екранованої витої пари категорії 6, отже, решта компонентів СКС повинні відповідати стандартам шостої категорії.

2.5 Обґрунтування вибору програмного забезпечення

В цьому розділі кваліфікаційної роботи буде наведено аргументацію вибору програмного забезпечення, що застосовується на вузлах комп'ютерної мережі. Для робочих станцій головного підрозділу використовується операційна система Windows 10 Pro. Операційну систему було придбано одночасно з робочими станціями. Ліцензія, яка використовується, має тип OEM. Вибір ОС Windows 10 зумовлений тим, що більшість програм працює під ОС сімейства Windows і користувачам не потрібно проходити додаткове навчання [20].

Операційна система FreeBSD 13 використовується для серверів кожної філії. Застосування цієї безкоштовної ОС дасть змогу забезпечити швидкий та функціональний фаєрвол, а також безкоштовне оновлення системи [27].

З метою забезпечення захищеного зв'язку між територіально віддаленими філіалами фірми через Інтернет буде реалізовано використання технології VPN, це реалізовано за допомогою пакету OpenVPN, який функціонує на операційній системі FreeBSD.

2.6 Обґрунтування вибору засобів захисту мережі

Для забезпечення безпеки мережі буде використано стандартний міжмережевий екран ipfw, що входить до складу ОС FreeBSD. Ця операційна система і її міжмережевий екран доступні безкоштовно. У третьому розділі кваліфікаційної роботи буде наведено правила фільтрації для міжмережевого екрану.

На робочих станціях використовується операційна система Windows 10. Операційні системи Windows 10 оснащені вбудованим фаєрволом Windows Firewall, що відрізняється високою ефективністю.

ОС центрального комутатора додатково підтримує встановлення ACL для фільтрації трафіку між різними підмережами.

2.7 Тестування та налагодження мережі

Процес тестування локальної мережі головного офісу складається з двох етапів:

- Перевірка кабельної системи за допомогою спеціалізованого тестера для перевірки відповідності вимогам стандарту Gigabit Ethernet.
- Тестування ПЗ на вузлах мережі.

Після виконання вищезазначених етапів необхідно провести тестування налаштованої об'єднаної мережі на основі технології VPN.

Мережа буде протестована на програмному рівні з використанням мережевих утиліт: tracert, route , ipconfig, ping, netstat.

Для виявлення проблем в роботі локальної мережі та мережевого обладнання (комутаторів, серверів) буде застосовуватись операційна система, що контролює сервер або комутатор.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування програмного забезпечення серверів

3.1.1 Інструкції з налаштування серверу-шлюзу і сервісу OpenVPN

Необхідно організувати віртуальну приватну мережу для кількох підрозділів компанії, підключеними до Інтернету.

Існує багато різних рішень цього питання, які неодноразово порівнювалися за показниками вартості, функціональності та надійності. Після аналізу всіх варіантів у цій дипломній роботі буде представлено рішення, засноване на безкоштовному пакеті OpenVPN, яке здійснює шифрування трафіку за допомогою сертифікатів. OpenVPN дає змогу реалізувати гнучку конфігурацію і застосовувати сертифікати TLS/SSL замість статичних ключів [24].

Для сервера на базі FreeBSD, розташованому на вході в підмережу філії №1, буде встановлено сервер OpenVPN. На вході в мережі двох віддалених офісів встановлені сервери з FreeBSD, що будуть клієнтами OpenVPN і системний адміністратор працюватиме на комп'ютері з Windows 10, який також буде клієнтом OpenVPN. Локальна підмережа головного офісу має адресу 172.16.14.0/24 (підмережа, де розташовані сервери) ; підмережа віддалеоного відділення - 172.16.2.0/24; підмережа тернопільського офісу - 172.16.1.0/24. Потрібно налаштувати віртуальну приватну мережу з маршрутизацією ”routed-типу” (Між підмережами не буде здійснюватися передача широкомовного трафіку), що характеризується топологією Point-to-multi-point (декілька клієнтів і один сервер), що застосовує TLS/SSL для шифрування трафіку та реалізує політику маршрутизації між локальними підмережами: з головного офісу є доступ до комп'ютерів локальних підмереж обох філій, Комп'ютери локальної підмережі головного офісу доступні з локальних підмереж філій, до комп'ютерів

локальних підмереж як центрального офісу, так і обох філій можна отримати доступ з комп'ютера віддаленого системного адміністратора.

Інсталяція сервера OpenVPN. Для того, щоб інсталювати сервер OpenVPN, потрібно здійснити наступні кроки: Внести рядок pseudo-device tun у файл конфігурації ядра, у разі відсутності цієї опції необхідно перекомпілювати ядро та перезапустити систему. На наступному етапі виконується встановлення OpenVPN з системи портів FreeBSD. Для цього потрібно перейти до відповідного каталогу та виконати компіляцію і встановлення пакунку:

cd /usr/ports/security/openvpn && make install clean

За замовчуванням конфігураційні файли сервера OpenVPN розміщуються в каталозі /usr/local/etc/OpenVPN. Для створення необхідної структури каталогів використовується така послідовність команд:

mkdir /usr/local/etc/OpenVPN

cd /usr/local/etc/OpenVPN

mkdir ccd (директорія де є конфігурації віддалених клієнтів)

mkdir certs (директорія з сертифікатами клієнтів і сервера)

mkdir crl (директорія, що містить списки відкликаних сертифікатів)

mkdir keys (директорія з закритими ключами сертифікатів клієнтів і сервера)

mkdir private (закритий ключ для довіреного сертифікату (CA))

mkdir req (директорія, що включає заявки на сертифікати)

chmod 700 keys private

echo "01" > serial

touch index.txt

Наступним кроком завдяки засобам ОС FreeBSD обмежуємо доступ до каталогів keys і private. Цей аспект є ключовим для гарантування необхідного рівня захисту приватних сертифікатів.

Наступним кроком є створення бази даних сертифікатів (відповідні файли index.txt і serial).

Давайте більш детально розглянемо вміст конфігураційних файлів OpenSSL.

Стандартним глобальним файлом конфігурації який використовує OpenSSL є /etc/ssl/openssl.cnf. У каталозі створюємо /usr/local/etc/OpenVPN відокремлений файл конфігурації OpenSSL для OpenVPN. Цей файл повинен мати назву openssl.cnf і містити наступний вміст:

```
# Основний блок налаштувань  центру сертифікації
[ main_ca ]
default_ca = main_ca_config
# Конфігурація CA (сертифікаційного центру)
[ main_ca_config ]
basedir = /etc/openvpn/ca       # Коренева директорія для файлів сертифікатів та ключів
revoked_dir = $basedir/revoked       # Каталог для зберігання відкликаних сертифікатів
index = $basedir/db/index.txt          # Файл індексу виданих сертифікатів
certs_store = $basedir/issued            # Каталог виданих сертифікатів
cert_file = $basedir/ca_cert.pem           # Файл сертифіката CA
serial_file = $basedir/db/serial        # Файл серійного номера сертифікатів
crl_file = $basedir/revoked/crl.pem          # Файл списку відкликаних сертифікатів
key_file = $basedir/private/ca_key.pem       # Приватний ключ CA
rand_source = $basedir/private/.rand        # Джерело випадкових чисел
valid_days = 3650                    # Термін дії сертифікатів у днях
crl_valid_days = 365                  # Термін дії CRL
hash_algorithm = sha256                # Алгоритм хешування
unique_subject = yes                  # Унікальність імен у сертифікатах
cert_policy = accept_all          # Політика перевірки полів
x509_ext = user_exts           # Розширення для сертифікатів користувачів
```

```
# Політика для валідації полів у сертифікаті
[ accept_all ]
organizationName = match              # Назва організації повинна збігатись
organizationalUnitName = optional     # Назва підрозділу - необов'язкова
commonName = supplied           # Обов’язкове поле загальної назви (CN)
# Блок налаштувань для створення запиту на сертифікат
[ request ]
key_size = 2048                       # Розмір ключа в бітах
output_key = private_key.pem        # Ім’я вихідного файлу з приватним ключем
dn_section = dn_fields                # Секція з Distinguished Name полями
x509_extensions = ca_exts             # Розширення, що застосовуються при створенні сертифікату
# Опис DN (Distinguished Name) полів
[ dn_fields ]
organizationName = Company Name (must match CA)
organizationName_default = MyCompany  # Значення за замовчуванням
organizationalUnitName = Department
commonName = Full Name or Service
commonName_max = 64                   # Максимальна довжина поля CN
# Розширення для сертифікатів користувачів
[ user_exts ]
basicConstraints = CA:FALSE           # Вказує, що це не сертифікат CA
# Розширення для сертифікатів CA
[ ca_exts ]
basicConstraints = CA:TRUE            # Вказує, що це сертифікат CA
valid_days = 3650
# Розширення для серверного сертифіката
[ server_cert ]
```

basicConstraints = CA:FALSE # Сертифікат не є сертифікатом CA

nsCertType = server # Вказує, що це сертифікат сервера

Тепер розглянемо наступну частину конфігураційного скріпта яка призначена для створення самопідписного довіреного сертифікату (CA). Для виконання цієї операції слід перейти до активного каталогу /usr/local/etc/OpenVPN і запустити команду:

openssl req -x509 -newkey rsa:2048 -nodes -days 3655 \

-keyout ./private/ca_key.pem -out ./Ca_cert.pem

При виконанні команди слід ввести такі дані:

- Country Name – офіційне міжнародне ім’я країни;
- State or Province Name – офіційна назва регіону;
- Locality Name; Organization Name – назву підприємства;
- Organizational Unit Name -ім'я відділу чи підрозділу;
- Common Name; Email Address – назва та електронна пошта.

Далі потрібно створити сертифікат сервера, що є важливим етапом. Потрібно знову перейти в каталог /usr/local/etc/OpenVPN і виконати наступну команду:

openssl genrsa -out private/server_key.pem 2048

openssl req -new -key private/server_key.pem -out csr/server_request.pem

Для перевірки створення сертифікату сервера виконуємо такі команди:

openssl req -noout -text -in req/server.pem (запит на видачу сертифіката)

openssl rsa -noout -text -in keys/server.pem (запит на видачу закритого ключа)

Завершальним етапом створення сертифіката є його підписання самопідписним сертифікатом (CA) через відповідну команду:

openssl ca -config ./openssl.cnf -extensions server -in reqs/server.csr \

-out signed_certs/server_cert.pem -batch

Загальний вигляд файлу конфігурації сервера подано в додатку Г.

Каталог ccd містить спеціальні файли конфігурації клієнтів. У вказаних файлах задаються одна або декілька команд для формування маршрутів до відповідних підмереж ЛОМ.

Для нашого випадку слід створити в каталозі /usr/local/etc/OpenVPN/ccd конфігураційні файли клієнтів client1-client3:

```
# Переходимо до каталогу конфігурацій OpenVPN для клієнтів
cd /etc/openvpn/ccd_configs
# Створюємо конфігураційні файли для трьох окремих клієнтів
for CLIENT in nodeA nodeB nodeC; do
  touch "$CLIENT"
done
```

У файлі client1 повинні бути зазначені дві команди: команда що додає клієнту маршрут, який забезпечує доступ до локальної підмережі головного офісу (відділення №1); крім того, вказує адресу локальної підмережі, що перебуває за клієнтом:

```
# У серверному конфігураційному файлі OpenVPN (server.conf або server.ovpn):
# Передаємо клієнтам маршрут до мережі 172.16.14.0/24 при підключенні
push "route 172.16.14.0 255.255.255.0"
# У конфігураційному файлі клієнта в директорії CCD (наприклад, ccd/client1):
# Вказуємо, що через цього клієнта доступна мережа 172.16.1.0/24
iroute 172.16.1.0 255.255.255.0
```

Файл client2 подібний до файлу client1, але з іншою адресою локальної підмережі, що розташована за клієнтом:

```
# Це дозволяє клієнту направляти трафік до цієї підмережі через VPN
push "route 172.16.14.0 255.255.255.0"
# Сервер OpenVPN направлятиме трафік до цієї мережі через відповідного клієнта
```

iroute 172.16.2.0 255.255.255.0

У файлі client3 повинні бути зазначені команди має містити команди, які додають маршрути до локальних підмереж відділення №1, №2, №3 для клієнта:

Додаємо маршрут до підмережі центрального офісу або базової інфраструктури

push "route 172.16.14.0 255.255.255.0"

Додаємо маршрут до локальної мережі відділення №1

push "route 172.16.1.0 255.255.255.0"

Додаємо маршрут до локальної мережі відділення №2

push "route 172.16.2.0 255.255.255.0"

Фінальним етапом є налаштування автозапуску сервера OpenVPN під час завантаження ОС. Це досягається за допомогою команди:

Щоб служба OpenVPN запускалася автоматично під час старту операційної системи, необхідно внести відповідний параметр у конфігураційний файл /etc/rc.conf.

Для цього додайте такий рядок:

OpenVPN_enable="YES"

Для належної роботи сервера OpenVPN слід конфігурувати брандмауер з такими налаштуваннями:

1. Дозволити передачу пакетів через інтерфейси OpenVPN-шлюза.

2. Ідентично дозволити передачу UDP-трафіку на зовнішню адресу сервера порт 1194.

3. А ще забезпечуємо дозвіл для проходження будь-якого трафіку з VPN-мережі до локальної підмережі організації.

4. Дозволяємо проходження трафіку у VPN-тунель з локальних підмереж.

5. Дозволяємо передачу пакетів даних між локальними підмережами за умовчанням (які не мають виходу назовні).

6. Як і в попередньому пункті, дозволяємо передачу даних з локальної підмережі до локальної підмережі головного офісу.

У командному рядку ipfw налаштовуємо такі правила для контролю мережевого трафіку:

/sbin/ipfw -q add pass ip from any to any via ${vif}

Дозволяємо увесь IP-трафік через віртуальний інтерфейс

/sbin/ipfw -q add pass udp from any to ${oip} 1194 in via ${oif}

Дозволяємо вхідний UDP трафік на порт 1194 через зовнішній інтерфейс

/sbin/ipfw -q add pass ip from ${vnet} to ${inet} out via ${iif}

Дозволяємо вихідний IP-трафік з віртуальної мережі у внутрішню мережу через інтерфейс iif

/sbin/ipfw -q add pass ip from ${inet} to ${vnet} in via ${iif}

Дозволяємо вхідний IP-трафік з внутрішньої мережі до віртуальної через інтерфейс iif

/sbin/ipfw -q add pass ip from 172.16.1.0/24 to ${inet} out via ${iif}

Дозволяємо вихідний трафік з підмережі 172.16.1.0/24 у внутрішню мережу

/sbin/ipfw -q add pass ip from ${inet} to 172.16.1.0/24 in via ${iif}

Дозволяємо вхідний трафік з внутрішньої мережі до підмережі 172.16.1.0/24

/sbin/ipfw -q add pass ip from 172.16.2.0/24 to ${inet} out via ${iif}

Дозволяємо вихідний трафік з підмережі 172.16.2.0/24 у внутрішню мережу

/sbin/ipfw -q add pass ip from ${inet} to 172.16.2.0/24 in via ${iif}

Дозволяємо вхідний трафік з внутрішньої мережі до підмережі 172.16.2.0/24

Shell-змінні можуть містити наступні значення:

– vif – Ідентифікатор мережевого інтерфейсу служби OpenVPN (наприклад, tun0).

– oif – Ідентифікатор зовнішнього мережевого інтерфейсу сервера (наприклад, rl0);

– iif – ідентифікатор внутрішнього мережевого інтерфейсу сервер (наприклад, rl1);

– vnet - адреса VPN мережі (у нашому випадку 10.0.0.0/24);

– inet - адреса ЛОМ (у нашому випадку - 172.16.14.0/24);

– oip - зовнішня IP-адреса сервера;

Подібні параметри міжмережевих екранів з боку клієнтів здійснюються аналогічним чином. Описані нами правила, починаючи з п’ятого номера, залежать від політики маршрутизації, що впроваджена в підмережах, і можуть підлягати зміні. При реалізації VPN у нашому випадку, правила ipfw для клієнта client1 виглядатимуть наступним чином (Змінна shell inet задає адресу локальної мережі підмережі клієнта client1 - 172.16.1.0/24):

/sbin/ipfw -q add pass ip from any to any via ${vif}

Дозволяємо весь IP-трафік через віртуальний інтерфейс

/sbin/ipfw -q add pass udp from any to ${oip} 1194 in via ${oif}

Дозволяємо вхідний UDP трафік на порт 1194 через зовнішній інтерфейс

/sbin/ipfw -q add pass ip from ${vnet} to ${inet} out via ${iif}

Дозволяємо вихідний IP-трафік із віртуальної мережі до локальної підмережі client1

/sbin/ipfw -q add pass ip from ${inet} to ${vnet} in via ${iif}

Дозволяємо вхідний IP-трафік із локальної підмережі client1 до віртуальної мережі

/sbin/ipfw -q add pass ip from 172.16.14.0/24 to ${inet} out via ${iif}

Дозволяємо вихідний трафік з підмережі 172.16.14.0/24 до локальної мережі client1

/sbin/ipfw -q add pass ip from ${inet} to 172.16.14.0/24 in via ${iif}

Дозволяємо вхідний трафік із локальної мережі client1 до підмережі 172.16.14.0/24

Правила ipfw для client2 збігаються з правилами для client1(тепер змінна shell inet визначає IP-адресу локальної підмережі client2 - 172.16.2.0/24).

Краще передавати файли конфігурації клієнту без підключення до Інтернету, з метою уникнення ненавмисного перехоплення. У такому разі доцільним рішенням буде використання, наприклад, флеш-накопичувача або зовнішнього жорсткого диска.

Для копіювання конфігураційних файлів клієнтів (Client) на необхідний диск виконуємо наступний порядок команд:

```
# Підмонтуємо флеш-накопичувач або диск із файловою системою MSDOS у директорію /mnt
mount -t msdos /dev/sdd1 /mnt
# Перейдемо у директорію з конфігураційними файлами OpenVPN
cd /usr/local/etc/OpenVPN
# Копіюємо сертифікат клієнта на змонтований диск
cp certs/cclient.pem /mnt
# Копіюємо приватний ключ клієнта
cp keys/kclient.pem /mnt
# Копіюємо сертифікат центру сертифікації (CA)
cp Ca_cert.pem /mnt
# Копіюємо ключ TLS-аутентифікації (ta.key)
cp ta.key /mnt
# Відмонтовуємо диск після завершення копіювання
umount /mnt
```

Таким чином буде змонтовано флеш-накопичувач (каталог /mnt), куди будуть скопійовані сертифікат та приватний ключ клієнта, статичний ключ HMAC та самопідписаний довірений сертифікат (CA).

Конфігураційні файли для FreeBSD-клієнтів відрізняються лише тим, як задають шляхи до файлів і назвами файлів із сертифікатами та закритими ключами. Таким чином, налаштувавши VPN, користувачі отримають швидкий і захищений доступ до системи клієнт-банк і інших додаткових служб, таких як OPENSSH, Remote Administrator, Wndows Terminal Services і т.д.

3.1.2 Інструкції з налаштування файлового сервера

Файлова служба в межах локальної мережі реалізується за допомогою протоколу FTP (File Transfer Protocol), який є одним із найбільш поширених та довготривало використовуваних протоколів прикладного рівня моделі OSI. У даному випадку застосовується легкий, безпечний і ефективний FTP-сервер — vsftpd (Very Secure FTP Daemon) [23].

Налаштування служби здійснюється за допомогою конфігураційного файлу vsftpd.conf, який визначає політику доступу, поведінку сервера, дозволені команди, режими доступу тощо. Повний перелік параметрів конфігурації подано в додатку Г.

Ключовий етап конфігурації полягає у створенні двох основних списків користувачів:

- user_list — перелік дозволених користувачів, які мають право підключатися до FTP-сервера;

- chroot_list — список імен користувачів, для яких буде застосовано ізоляцію в межах власного домашнього каталогу.

Наступним кроком є створення спеціального каталогу vusers у директорії /etc/vsftpd/, де будуть зберігатися індивідуальні конфігураційні файли для кожного віртуального користувача. Наприклад, для користувача з ім’ям user113 створюється відповідний файл /etc/vsftpd/vusers/user113 зі вмістом:

local_root=/var/ftp/user113

Наведений шлях вказує на домашній каталог користувача, який слугуватиме його кореневою директорією в межах FTP-сервера. Це дозволяє ефективно структурувати файлову систему, створюючи деревоподібну архітектуру каталогів із розмежованими правами доступу.

Додатково в конфігурації можуть бути передбачені такі параметри:

write_enable=YES — дозволяє запис файлів;

local_umask=022 — визначає маску дозволів для новостворених файлів;

chroot_local_user=YES — ізолює користувача в його домашньому каталозі;

user_sub_token=$USER — використовується для динамічної підстановки імені користувача у шляхи.

Після завершення всіх налаштувань служба FTP-сервера запускається командою:

/etc/rc.d/init.d/vsftpd start

або в сучасних дистрибутивах з підтримкою systemd:

systemctl start vsftpd

Реалізація файлової служби в локальній мережі за допомогою FTP-протоколу на базі сервера vsftpd є ефективним і безпечним рішенням для централізованого зберігання та доступу до даних. Завдяки можливості гнучкого налаштування списків користувачів, їхніх домашніх каталогів, прав доступу та ізоляції (chroot), забезпечується належний рівень контролю й безпеки даних. Індивідуальні конфігурації для кожного користувача дозволяють реалізувати чітке розмежування доступу до ресурсів, що є важливим для підтримки політики безпеки в корпоративному середовищі. Такий підхід забезпечує надійну та зручну інфраструктуру обміну файлами всередині організації.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування центрального комутатора

Розглянемо безпосередній процес налаштування віртуальних мереж (VLAN) на мережевому комутаторі, через одну загальну систему команд. На першому етапі вказується кількість VLAN, що будуть використовуватись (визначається моделлю комутатора та вказується у його технічній документації): SW(config)# max-vlans {кількість VLAN}

Далі наведемо скрипт, що створює VLAN-мережу, задавання імен хостам і вказання портів для підключення, які належать до віртуальної мережі:

```
SW(config)# interface range gigabitEthernet 1/0/1 - 1/0/3
SW(config-if-range)# switchport mode access
SW(config-if-range)# switchport access vlan 14
// Порти з 1 по 3 переводяться в access-режим та прив'язуються до VLAN 14
SW(config)# interface gigabitEthernet 1/0/4
SW(config-if)# switchport mode access
SW(config-if)# switchport access vlan 15
// Порт 1/0/4 під'єднується до VLAN 15 у режимі доступу
SW(config)# interface gigabitEthernet 1/0/5
SW(config-if)# switchport mode access
SW(config-if)# switchport access vlan 16
// Порт 1/0/5 налаштовується для VLAN 16
SW(config)# interface range gigabitEthernet 1/0/6 - 1/0/11
SW(config-if-range)# switchport mode access
SW(config-if-range)# switchport access vlan 17
// Порти з 6 по 11 включно налаштовуються на VLAN 17
```

Для налаштування транкових (trunk) портів на комутаторі необхідно виконати наступні дії в конфігураційному режимі:

```
SW(config)# interface range gigabitEthernet 1/0/12 - 17
SW(config-if-range)# switchport mode trunk
```

Для реалізації міжвланової маршрутизації необхідно створити віртуальні інтерфейси VLAN (SVI) та призначити їм відповідні IP-адреси. Це дозволить маршрутизувати трафік між VLAN без використання зовнішнього маршрутизатора.

```
SW(config)# interface vlan 11
! Налаштування інтерфейсу VLAN 11 — логічна підмережа №1
SW(config-if)# ip address 172.16.11.200 255.255.255.0
! Призначення статичної IP-адреси шлюзу для VLAN 11
SW(config-if)# exit
```

SW(config)# interface vlan 12

! Створення VLAN 12 — обслуговування іншого сегмента мережі

SW(config-if)# ip address 172.16.12.200 255.255.255.0

! Призначення IP-адреси шлюзу для VLAN 12

SW(config-if)# exit

SW(config)# interface vlan 13

! Ініціалізація VLAN 13 для окремої підмережі

SW(config-if)# ip address 172.16.13.200 255.255.255.0

! Вказуємо IP шлюзу для даного віртуального інтерфейсу

SW(config-if)# exit

SW(config)# interface vlan 14

! Конфігуруємо VLAN 14 — наступна логічна мережа

SW(config-if)# ip address 172.16.14.200 255.255.255.0

! Призначення унікальної IP-адреси для шлюзу VLAN 14

SW(config-if)# exit

SW(config)# interface vlan 15

! Налаштовуємо інтерфейс VLAN 15 для п’ятої підмережі

SW(config-if)# ip address 172.16.15.200 255.255.255.0

! Встановлюємо адресу шлюзу для VLAN 15

SW(config-if)# exit

SW(config)# interface vlan 16

! Додаємо VLAN 16 — частина мережевої структури підприємства

SW(config-if)# ip address 172.16.16.200 255.255.255.0

! IP-адреса шлюзу для шостої VLAN

SW(config-if)# exit

SW(config)# interface vlan 17

! Активуємо VLAN 17 для додаткового мережевого сегмента

SW(config-if)# ip address 172.16.17.200 255.255.255.0

! Призначаємо IP для віртуального інтерфейсу VLAN 17

SW(config-if)# exit

SW(config)# interface vlan 18

! Остання VLAN у переліку — VLAN 18

SW(config-if)# ip address 172.16.18.200 255.255.255.0

! Налаштування адреси шлюзу для восьмої VLAN

SW(config-if)# exit

Отримання інформації про наявні віртуальні мережі виконується за допомогою команди show vlan.

! Перевірка поточного списку створених VLAN на комутаторі

SW# show vlan brief

! Додавання маршруту за замовчуванням до основного шлюзу мережі

SW(config)# ip route 0.0.0.0 0.0.0.0 <IP-адреса_шлюзу>

! Наприклад:

! SW(config)# ip route 0.0.0.0 0.0.0.0 172.16.11.1

! Увімкнення внутрішньої маршрутизації між VLAN

SW(config)# ip routing

! Створення адміністративного користувача з правами доступу

SW(config)# username admin privilege 15 secret StrongPassword123

! Параметри: ім’я користувача, рівень привілеїв (15 — максимальний), захищений пароль

! Налаштування поточного часу (важливо для логування та синхронізації подій)

SW(config)# clock set 14:30:00 10 June 2025

! Формат: год:хв:сек день місяць рік

! Увімкнення системного логування для відслідковування помилок та подій

SW(config)# logging buffered 8192

! Це дозволяє зберігати системні повідомлення у буфері пам’яті комутатора

У процесі налаштування комутатора було здійснено повну конфігурацію логічних інтерфейсів VLAN із призначенням статичних IP-адрес, що дозволяє організувати окремі підмережі всередині корпоративної мережі та забезпечити сегментацію трафіку. Це є критично важливим для підвищення безпеки, продуктивності та зручності адміністрування.

Крім того, було реалізовано основні кроки з активації маршрутизації між VLAN, встановлення маршруту за замовчуванням для виходу в зовнішні мережі, створення облікового запису адміністратора та налаштування системного логування. Це дозволяє ефективно керувати мережею, контролювати події та підтримувати стабільну роботу інфраструктури.

Завдяки реалізованим налаштуванням комутатор виконує роль базового рівня маршрутизатора в локальній мережі підприємства, забезпечуючи як функціональність, так і безпеку відповідно до вимог сучасних мережевих систем.

3.2.2 Інструкції з налаштування комутаторів робочих груп

Налаштування мережевого обладнання в межах локальної мережі підприємства розпочинається з конфігурації комутаторів другого рівня, які забезпечують зв’язок між комп’ютерами в межах окремих відділів. Основні етапи налаштування комутаторів серії DGS-1100-16 включають [8]:

1. Створення облікового запису адміністратора

На першому етапі виконується налаштування облікових даних для доступу до веб-інтерфейсу або CLI-комутатора. З міркувань безпеки задається унікальний логін та складний пароль, а також, за потреби, визначається рівень привілеїв для адміністративного керування пристроєм.

2. Створення та налаштування VLAN

Для логічного поділу мережі на окремі підмережі (відповідно до структури

організації) на кожному комутаторі створюються VLAN (віртуальні локальні мережі).

- Порти, до яких підключені користувацькі пристрої, налаштовуються в режимі Access і прив'язуються до відповідного VLAN.

- Один із портів комутатора переводиться в режим Trunk, що забезпечує передачу трафіку кількох VLAN до головного комутатора або маршрутизатора, який здійснює маршрутизацію між підмережами.

3. Налаштування дати та часу

Для забезпечення коректного логування подій, синхронізації системних процесів та відстеження мережевої активності виконується налаштування поточних параметрів дати й часу. Це можливо як вручну, так і через протокол NTP (Network Time Protocol), якщо є доступ до зовнішнього або локального NTP-сервера.

3.3 Інструкція з використання тестових наборів та тестових програм

Для перевірки кабелів локальної мережі візьмемо кабельний аналізатор, який відповідає стандартам технології 1000Base-T. Для фізичного тестування кабельних з’єднань провідних сегментів застосовується кабельний тестер який оснащений функціями виявлення обривів та коротких замикань проводів у парах і атестації кабельної проводки відповідно до встановлених вимог. У проекті мережі планується застосування кабельного тестера Benetech GM60, що представлений на рисунку 3.1.

Рисунок 3.1 – Кабельний тестер

Для виконання базової діагностики та тестування мережі можна скористатися вбудованими інструментами операційної системи. Серед них [12]:

1. ROUTE – дає змогу переглянути поточну таблицю маршрутизації або внести до неї зміни.
2. RSH (Remote Shell) – дозволяє запускати команди на віддаленому сервері з операційною системою UNIX.
3. ARP – відображає асоціацію IP-адрес з фізичними MAC-адресами в локальному ARP-кеші.
4. REXEC (Remote Execution) – використовується для ініціації виконання процесу на віддаленій системі.
5. NETSTAT – надає інформацію про активні з'єднання, відкриті порти та статистику мережевих інтерфейсів.

6. Telnet – застосовується для підключення до віддалених пристроїв з імітацією терміналу.

7. IPCONFIG – виводить поточні налаштування мережевих інтерфейсів у Windows-системах.

8. HOSTNAME – вказує назву вузла (комп'ютера), з якого виконується команда.

9. PING – тестує доступність вузлів у мережі, надсилаючи пакети й аналізуючи відповіді.

Крім того, при діагностиці можливих несправностей мережевих адаптерів або інших апаратних компонентів в середовищі Linux застосовуються спеціалізовані інструменти. До них належать:

- lshw – надає детальну інформацію про обладнання системи.

- lsusb – виводить дані про USB-пристрої, підключені до комп’ютера.

- lspci – використовується найчастіше, оскільки демонструє всі пристрої, що працюють через шину PCI/PCIe, зокрема мережеві карти.

Остання команда особливо корисна адміністраторам, оскільки дає змогу швидко ідентифікувати встановлені контролери та перевірити їхню коректну роботу.

3.4 Інструкція з захисту мережі

Для захисту локальної мережі від несанкціонованого доступу та фільтрації небажаного трафіку на маршрутизаторі з ОС FreeBSD буде налаштовано вбудований міжмережевий екран IPFW. Він дозволяє гнучко керувати доступом до системи на основі адрес, портів, типів протоколів та стану з’єднань [22].

Нижче наведено приклад базового скрипту з правилами фільтрації, адаптованими під потреби локального сервера:

```
#!/bin/sh
# Очищення всіх існуючих правил фільтрації
```

```
ipfw -q flush
# Дозвіл для трафіку, що є частиною вже встановлених сесій
ipfw -q add 10 check-state
# Дозвіл для локального інтерфейсу (loopback)
ipfw -q add 20 allow ip from any to any via lo0
# Пропуск активних TCP-з'єднань
ipfw -q add 30 allow tcp from any to any established
# Обробка фрагментованих IP-пакетів
ipfw -q add 40 reass ip from any to any in
# Дозвіл вхідного трафіку на порт 22 (SSH) та 443 (HTTPS) із збереженням стану
ipfw -q add 100 set 10 allow tcp from any to 192.168.1.1 22 in setup keep-state
ipfw -q add 101 set 10 allow tcp from any to 192.168.1.1 443 in setup keep-state
# Дозвіл вихідного UDP- та TCP-трафіку з локального хоста
ipfw -q add 200 set 10 allow udp from 192.168.1.1 to any out keep-state
ipfw -q add 201 set 10 allow tcp from 192.168.1.1 to any out setup keep-state
# Дозвіл ICMP-пакетів для діагностики (ping, traceroute тощо)
ipfw -q add 300 set 10 allow icmp from 192.168.1.1 to any icmptypes 0,3,8,11
ipfw -q add 301 set 10 allow icmp from any to 192.168.1.1 icmptypes 0,3,8,11
# Блокування всього іншого вхідного трафіку, не дозволеного вище
ipfw -q add 999 set 10 deny ip from any to any
```

3.5 Інструкції з експлуатації та моніторингу в мережі

Для забезпечення роботи локальної мережі потрібні такі типи документів:

1. Фізична топологія.
2. Логічна топологія.
3. Таблиця IP-адрес.

4. План приміщення.

У ході експлуатації мережі з часом постане необхідність долучення нових користувачів. У процесі проєктування мережі для всіх робочих груп були реалізовані додаткові точки доступу для клієнтів.

Контроль за процесами в мережі становить критично важливу складову її експлуатації. Контроль над процесами в мережі включатиме:

1. Отримання даних про роботу протоколів канального рівня через операційну систему центрального комутатора.

2. Застосування діагностичних програм операційної системи сервера і файлів журналів.

3. Аналітичні дані щодо роботи мережевого сховища.

ПЗ OpenVPN фіксує події у власному журналі (openvpn-status.log), який розміщений у директорії /var/log. У цій директорії розташовані журнали ОС FreeBSD, зокрема: dmesg, secure,messages.

3.6 Моделювання роботи мережі компанії

Симуляція роботи локальної мережі використовується з метою контролю правильності розробки та налаштування мережевих компонентів. Для моделювання підходить наступне програмне забезпечення:

1. Packet Tracer.
2. Opnet Modeler.
3. Netcracker.

Для створення моделі буде задіяна програма Packet Tracet 5.3, з огляду на те, що вона не потребує оплати. Packet Tracer - програма для імітації мережі передачі даних від компанії Cisco Systems. Вона має на меті створювати повноцінні моделі мережі, конфігурувати (за допомогою команд Cisco IOS) маршрутизатори й комутатори, а також забезпечувати взаємодію між кількома користувачами (через хмарне середовище) [17] .

Програма симулює широко використовувані серії комутаторів 2950, 2960, 3650 і маршрутизаторів Cisco 1800, 2600, 2800 а ще інші моделі. До того ж існують сервери TFTP, DHCP , FTP, HTTP, пристрої WiFi, різні блоки для ПК і маршрутизаторів, робочі станції а також різні кабелі. Сфера використання програми охоплює як прості навчальні мережі з кількома (десятками) хостів так і складніші мережеві макети. Головна риса даної програми – здатність перевіряти функціональність топології. Мета створення моделі: перевірка комунікації між вузлами локальної мережі. Засоби програми дають змогу відтворювати роботу протоколів: TCP, SMTP, ICMP, SNMP, та ін.

Програма Racket Tracer дозволить імітувати роботу протоколу ICMP між вузлом PC1 та сервером S1. Локальна мережа, створена за допомогою програми Packet Tracer 5.3, представлена на рисунку 3.2.

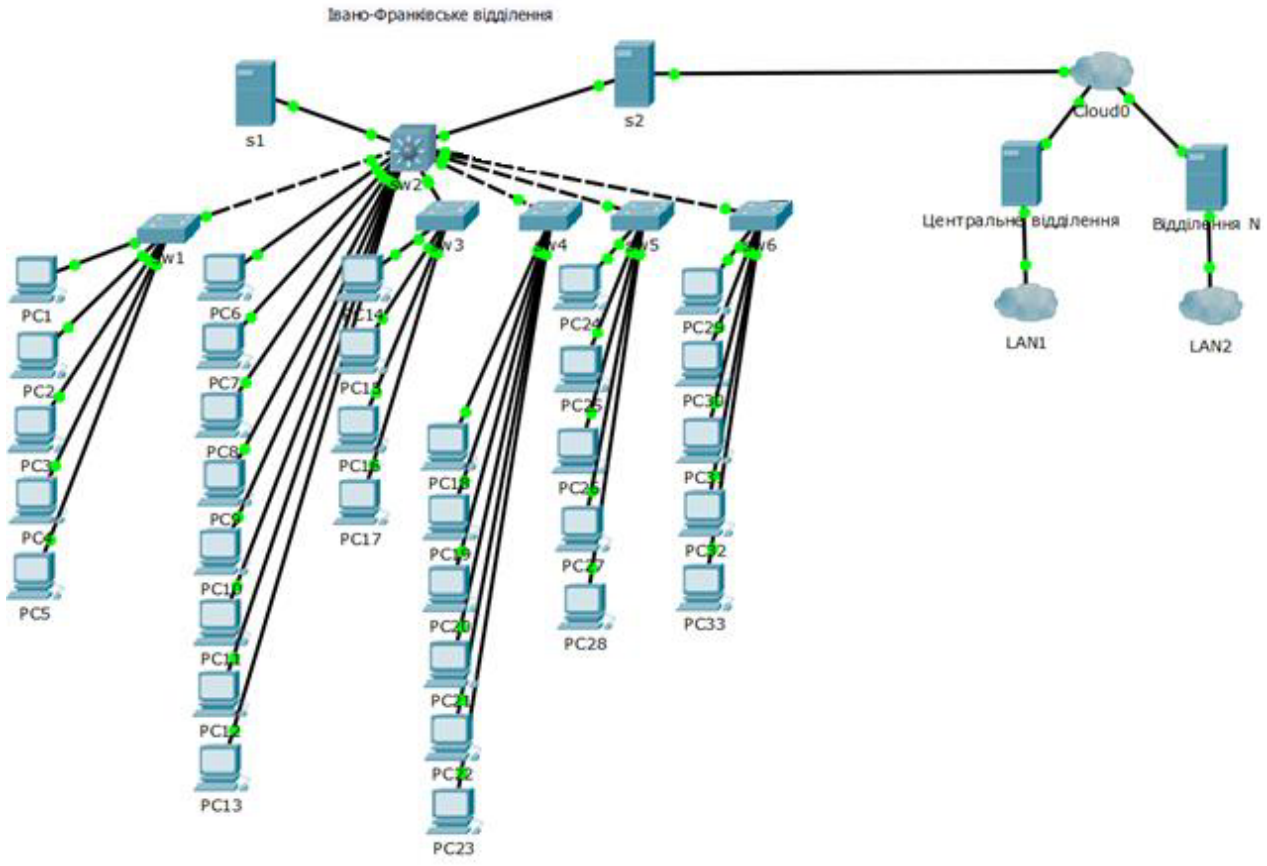

Рисунок 3.2 – Змодельована локальна мережа

Налаштування вузла PC1.

Для коректної роботи комп’ютера PC1 у корпоративній мережі необхідно задати параметри IP-конфігурації згідно з виділеними адресами. Конфігурацію виконуємо наступним чином:

IP-адреса пристрою: 172.16.11.1;

Маска підмережі: 255.255.255.0, що відповідає класу C та дозволяє до 254 хостів у підмережі;

Основний шлюз (default gateway): 172.16.11.200 — це IP-адреса маршрутизатора, через який здійснюється вихід за межі підмережі;

DNS-сервери:

- первинний DNS: 172.16.14.202 — корпоративний сервер імен;
- альтернативний DNS: 8.8.8.8 — публічний сервер Google для резервного розпізнавання доменів.

Ці параметри можна внести вручну у властивостях мережевого адаптера операційної системи або ж задати через DHCP, якщо сервер надає динамічну IP-конфігурацію.

Налаштування сервера S1.

Так само необхідно прописати мережеві налаштування для сервера S1, який забезпечуватиме обслуговування клієнтів. Для стабільного функціонування сервер має мати статичну адресу:

- IP-адреса сервера: 172.16.14.201;
- Маска підмережі: 255.255.255.0;
- Шлюз за замовчуванням: 172.16.14.200, що забезпечує вихід з підмережі до інших сегментів або в інтернет;

DNS-сервери:

- основний: 172.16.14.202 — внутрішній сервер DNS;
- резервний: 8.8.8.8 — загальнодоступний DNS для аварійного використання.

Зазначені параметри забезпечують коректну взаємодію вузлів у рамках локальної мережі та з зовнішніми ресурсами через маршрутизатор. Рекомендується перевірити зв’язок між вузлами за допомогою команд ping та nslookup після завершення налаштувань.

Імітуємо роботу протоколу ICMP через передачу даних між зазначеними вузлами. Запускаємо команду ping як на риснку 3.3

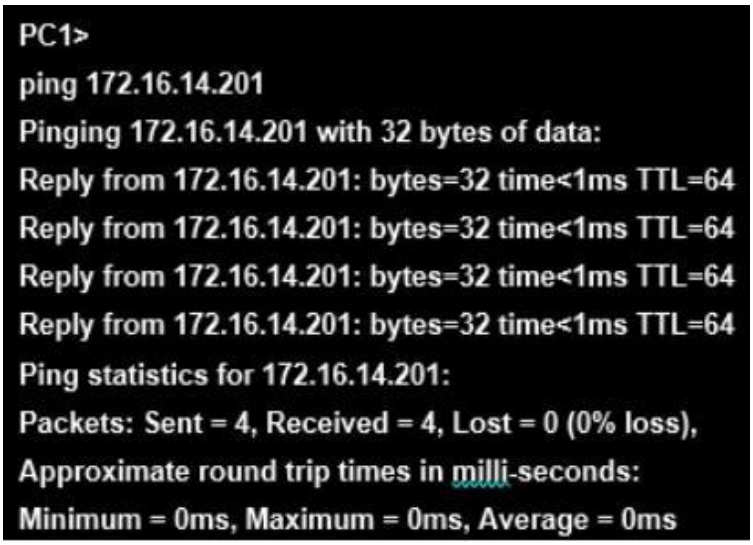

Рисунок 3.3 – Результати роботи команди ping

Цей результат свідчить про успішне з’єднання між пристроями в локальній мережі, з нульовими затримками і втратою пакетів. Це типовий позитивний результат у симуляційному середовищі, такому як Cisco Packet Tracer, який вказує на правильність прийнятих рішень і здійснених налаштувань. Таким чином, результати моделювання підтвердили працездатність запропонованої топології мережі, її масштабованість та відповідність поставленим вимогам до продуктивності, безпеки й надійності. Отримана модель може бути використана як основа для подальшого фізичного впровадження комп’ютерної мережі на підприємстві.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для Івано-Франківського відділення ТзОВ «ВНС Group» і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Час викон. операції, год.
1	2	3	4
1	Постановка задачі та формування технічного завдання	Керівник проекту	6
2	Розробка проекту. Проектування логічної та фізичної топології локальної мережі. Підбір пасивного та активного мережевого обладнання	Інженер	12
3	Прокладання мережі (коробів, кабелів, розеток і т.д.). Монтаж обладнання.	Технік	24
4	Налаштування мережі. Конфігурування мережевих служб та сервісів.	Інженер	24

Продовження таблиці 4.1

1	2	3	4
5	Оформлення документації	Інженер	12
	Разом	-	78

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для Івано-Франківського відділення ТзОВ «ВНС Group» складає 78 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

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

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

Основна заробітна плата розраховується за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проекту – 260 грн./год., інженер – 190 грн./год., технік – 150 грн./год.

Отже, основна заробітна плата для:

1. Керівник проекту - $З_{осн1} = 6 \cdot 260 = 1560$ грн.
2. Інженер - $З_{осн2} = 48 \cdot 190 = 9120$ грн.
3. Технік - $З_{осн3} = 24 \cdot 150 = 3600$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 1560 + 9120 + 3600 = 14280{,}00 \text{ грн.}$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту - $З_{дод1} = 1560 \cdot 0{,}13 = 202{,}80$ грн.
2. Інженер - $З_{дод2} = 9120 \cdot 0{,}13 = 1185{,}60$ грн.
3. Технік - $З_{дод3} = 3600 \cdot 0{,}13 = 468{,}00$ грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 202{,}80 + 1185{,}60 + 468{,}00 = 1856{,}4 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

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

$$В_{о.п} = 14280 + 1856{,}4 = 16136{,}4 \text{ грн.}$$

Необхідно визначити відрахування на соціальні заходи:

- фонд страхування на випадок безробіття – 1,6 %;
- фонд по тимчасовій втраті працездатності – 1,4 %;
- пенсійний фонд – 33,2 %;
- внески на страхування від нещасного випадку на виробництві та професійного захворювання - 1,4%.

Загальна сума зазначених відрахувань становить 37,6 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = ФОП \cdot 0{,}376, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 16136,4 \cdot 0,376 = 6067,29 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахування на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпрацьов. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	260	6	1560	202,8	-	-
2	Інженер	190	48	9120	1185,6	-	-
3	Технік	150	24	3600	468,0	-	-
			Разом	14280	1856,4	6067,29	22203,69

Отже, загальні витрати на оплату праці становлять 22203,69 грн.

4.3 Розрахунок матеріальних витрат

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

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

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum М_{Вi} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№	Опис	Од. вим.	К-сть	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа висота 18U	шт.	1	8760	8760
2	Комутаційна шафа висота 7U	шт.	6	5600	33600
3	Патчпанель, 24 порти, категорія 6	шт.	1	2000	2000
4	Патчпанель Panduit, 16 портів, категорія 6	шт.	6	1300	7800
5	Патчкорд UTP кат. 6	шт.	40	15	600
6	Короб	м.	105	60	6300
7	Кабль UTP (кат. 6), Одескабель	м.	610	23,30	14213
8	Мережева розетка UTP (кат. 6)	шт.	40	100	4000
9	Блок безперебійного живлення APC 1500VA Smart-UPS	шт.	1	18200	18200
10	Комутатор TP-Link T3700G- 28TQ	шт.	1	26900	26900
11	Комутатор робочих груп D-Link DGS-1100-08	шт.	3	1900	5700
12	Комутатор робочих груп D-Link DGS-1100-16	шт.	2	3300	6600
13	Файловий сервер ARTLINE Business R19	шт.	1	63000	63000
14	Сервер-шлюз ARTLINE Business R19	шт.	1	63000	63000
Загальна сума, грн.					260673

Загальна сума матеріальних витрат на розробку та встановлення мережі становить: 260673 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання розраховуються за формулою 4.7:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 18 годин, споживана потужність - 0,5 кВт/год, вартість 1 кВт електроенергії – 7 грн.

Тому витрати на електроенергію будуть становити:

$$З_е = 0,5 \cdot 18 \cdot 7 = 63 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8 – 10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8.

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

де $Т_в$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_в = 260673 \cdot 0,08 = 20853,84 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фонді. Мінімально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань використовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{150\%} \cdot T, \quad (4.9)$$

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 18 год., балансова вартість ПК – 25600 грн., тому:

$$A = \frac{25600 \cdot 0{,}05}{150} \cdot 18 = 153{,}6\ грн.$$

4.7 Обчислення накладних витрат

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

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

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

де, $Н_в$ – накладні витрати.

$$Н_в = 16136,4 \cdot 0,4 = 6454,56 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

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

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	16136,4	5,20
Відрахування на соціальні заходи	6067,29	1,95
Матеріальні витрати	260673	83,98
Витрати на електроенергію	63,00	0,02
Транспортні витрати	20853,84	6,72
Амортизаційні відрахування	153,60	0,05
Накладні витрати	6454,56	2,08
Собівартість	310401,69	100,00

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

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

Отже, собівартість дорівнює: $С_в = 310401,69$ грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

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

де $С_в$ – собівартість виконання НДР;

$Р_{рен.}$ – рівень рентабельності, на даний час для ІТ галузі - 20 %

ПДВ – ставка податку на додану вартість, 20 %.

$$Ц = 310401,69 \cdot (1+0,2) \cdot (1+0,2) = 446978,44 \text{ грн.}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва - категорія, яка характеризує результативність виробництва. Вона свідчить не лише про приріст обсягів виробництва, а й про те, якими витратами ресурсів досягається цей приріст, тобто свідчить про якість економічного зростання.

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

$$П = 446978,44 - 310401,69 = 136576,75 \text{ грн.}$$

Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14.

$$Е_р = П / С_в, \quad (4.14)$$

де П – прибуток;

$С_в$ – собівартість.

$$Е_р = 136576,75 / 310401,69 = 0,44$$

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

$$Т_р = 1 / Е_р \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку

$$T_р=1/0,44=2,27.$$

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

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	310401,69 грн.
2.	Плановий прибуток, грн.	136576,75 грн.
3.	Ціна, грн.	446978,44 грн.
4.	Економічна ефективність	0,44
5.	Термін окупності, рік	2,27

Загальна вартість реалізації проєкту зі створення комп'ютерної мережі для Івано-Франківського відділення ТзОВ «ВНС Group» становить 446 978,44 грн. Проведені розрахунки підтверджують доцільність і економічну обґрунтованість інвестицій: коефіцієнт економічної ефективності дорівнює 0,44, що свідчить про високий рівень прибутковості проєкту в межах галузевих стандартів.

Очікуваний період окупності вкладених коштів становить 2,27 року, що є прийнятним терміном для інфраструктурних ІТ-проєктів такого масштабу. Це означає, що витрати на впровадження мережі будуть повністю компенсовані за рахунок економії ресурсів, підвищення продуктивності та ефективності роботи підрозділу менш ніж за 3 роки.

Таким чином, реалізація даного проєкту дозволить ТзОВ «ВНС Group» не лише оптимізувати внутрішні бізнес-процеси, а й створити надійну технічну основу для подальшого масштабування інформаційної інфраструктури.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

На даний час широке розповсюдження отримали персональні комп'ютери. Однак їх використання загострило проблеми збереження власного та суспільного здоров'я, вимагає удосконалення існуючих та розробки нових підходів до організації робочих місць, проведення профілактичних заходів для запобігання розвитку негативних наслідків впливу ПК на здоров'я користувачів [7].

Заходи з охорони праці користувачів ПК необхідно розглядати в трьох основних аспектах: соціальному, психологічному та медичному. У соціальному плані розв'язання цих проблем пов'язане з оптимізацією умов життя, праці, відпочинку, харчування, побуту, розвитком культури, транспорту.

Значне місце у профілактиці розладів здоров'я належить психології праці. Тому заходи, пов'язані з формуванням раціональних виробничих колективів, у яких відсутня психологічна несумісність, сприяють зменшенню нервово-психічного перенапруження, підвищенню працездатності та ефективності праці [7].

5.1 Забезпечення та контроль стану пожежної безпеки в ТзОВ «ВНС Group»

Протипожежна безпека на підприємстві в Україні – невіддільна частина організації робочого простору і процесів згідно з нормами чинного законодавства [13].

Зокрема, цю сферу регламентують Правила пожежної безпеки в Україні, затверджені наказом Міністерства внутрішніх справ України, зі змінами, які періодично вносяться відповідними наказами [13].

Зафіксовані на законодавчому рівні вимоги пожежної безпеки зобов'язані виконувати – незалежно від приналежності та розміру статутного капіталу, обороту, кількості співробітників, форми власності, кодів ЗЕД, сфери роботи та інших аспектів – будь-які суб'єкти, що ведуть свою господарську діяльність на українській території [13].

Тому необхідно бути в курсі цих змін і коригувати організаційну роботу в даному секторі на виробництвах і в компаніях.

А для цього слід регулярно проводити моніторинг нормативної бази та проходити відповідне навчання, щоб оновити не лише теоретичну базу, а й практичні навички співробітників.

Пожежна безпека входить в комплекс заходів з охорони праці, і організаційна робота в цій сфері на об'єктах господарювання включає широкий спектр заходів, а саме [7]:

- створення умов для безпечної праці,
- мінімізації ризику виникнення пожеж,
- своєчасне і повноцінне забезпечення технічними засобами для запобігання займання та усунення самих пожеж та їх наслідків,
- контроль дотримання протипожежних вимог і норм законодавства,
- розробка і впровадження регламентів по гасінню пожеж, евакуації та порятунку з місць пожежі й задимлення людей і майна (матеріальних цінностей),
- внутрішнє і зовнішнє навчання співробітників [11].

У разі, якщо підприємство орендує площі в іншої особи, сторони повинні в письмовій формі домовитися про те, хто з них і на яких умовах здійснює ці роботи.

Вимоги до пожежної безпеки на підприємстві неухильно повинен дотримуватися кожен співробітник, а організаційна складова при цьому покладається на посадових осіб за відповідним рішенням керівництва і прописується в посадових інструкціях і положеннях по структурним підрозділам.

Зокрема, вказуються конкретні території, ділянки, зони, об’єкти, цілі будівлі і їх частини, поверхи, на яких відповідального співробітника повинне проводити такі організаційні роботи.

Відповідальні особи зобов’язуються розробити, впровадити та підтримувати в певному інструкцією і положенням на ввірених їм об’єктах протипожежний режим і інструкції відповідно до вимог, викладених в нормативних актах.

Залежно від особливостей виробничого процесу, крім загальних вимог пожежної безпеки, здійснюються спеціальні протипожежні заходи для окремих видів виробництв, технологічних процесів та промислових об'єктів. Для споруд та приміщень, в яких експлуатуються відеотермінали та ЕОМ такі заходи визначені правилами пожежної безпеки в Україні, та іншими нормативними документами [13].

Будівлі та їх частини, в яких розташовуються ЕОМ, повинні бути не нижче II ступеня вогнестійкості. Над та під приміщеннями, де розташовуються ЕОМ, а також у суміжних з ними приміщеннях не дозволяється розташування приміщень категорій А і Б за вибухопожежною небезпекою. Приміщення категорії В слід відділяти від приміщень з ЕОМ протипожежними стінами.

Важливою складовою протипожежного режиму на будь-якому об’єкті є розробка і впровадження порядку дій при виникненні пожежі. Неодмінно має бути план евакуації, описано, як повинні відключатися електроустановки, що і в якій послідовності необхідно робити співробітникам [4].

Відповідно, для кожного об’єкта, кожного приміщення (крім коридорів, санвузлів, басейнів і подібних приміщень), окремих видів робіт складаються інструкції, за якими повинен працювати персонал, залучений на певних ділянках і в виконанні окремих видів робіт. За інструкціями проводиться навчання (інструктаж) персоналу з подальшим контролем знань.

План евакуації розроблено згідно вимог [26] і наведено на рисунку 5.1.

На ньому вказано шляхи евакуації, а також розміщення вогнегасників та пожежного гідранта в будівлі, де інсталюється проектована мережа.

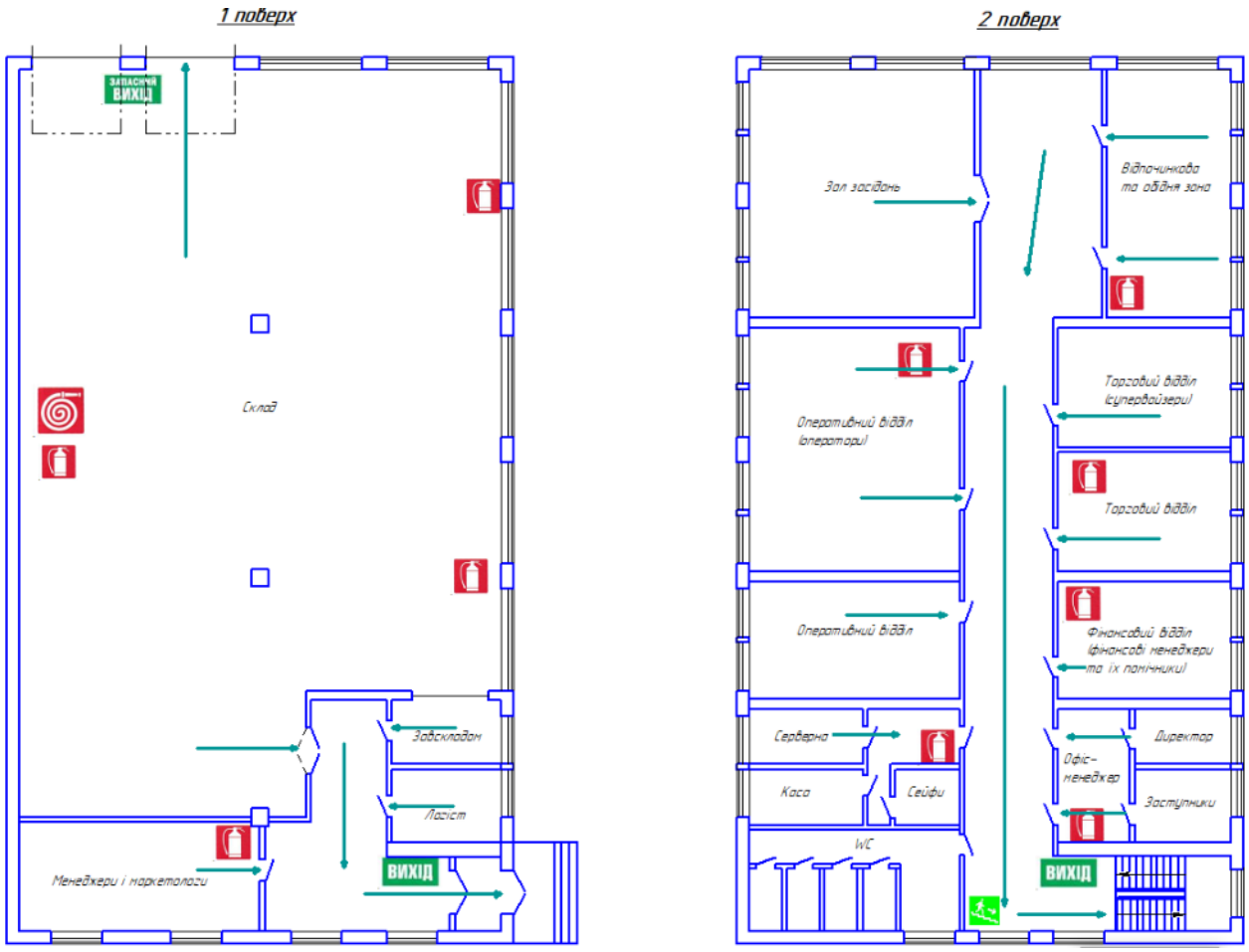

Рисунок 5.1 – План евакуації на випадок пожежі

Для ліквідації невеликих осередків пожежі, а також для гасіння пожеж на початковій стадії їх розвитку (до прибуття штатних підрозділів пожежної охорони) призначені первинні засоби пожежогасіння.

Поміж первинних засобів пожежогасіння найважливіша роль відводиться найефективнішим із них - вогнегасникам. Установлено, що з використанням вогнегасників успішно ліквідують загоряння протягом перших чотирьох хвилин від миті їх виникнення, тобто ще до прибуття пожежних підрозділів.

Вогнегасники слід установлювати в легкодоступних місцях (у коридорах, біля входів або виходів із приміщень тощо) та на видноті, а також у

пожежонебезпечних місцях, де найімовірнішою є поява осередків пожежі. При цьому слід забезпечити їх захист від потрапляння прямих сонячних променів та безпосередньої (без загороджувальних щитків) дії опалювальних і нагрівальних приладів. Переносні вогнегасники мають розміщуватися шляхом навішування їх на вертикальні конструкції на висоті не більше 1,5 м від рівня підлоги до нижнього торця вогнегасника та на відстані од дверей, достатній для їх повного відчинення, або встановлення в пожежних шафах поряд із пожежними кранами, в спеціальних тумбах або на пожежних щитах (стендах).

Для захисту об’єкта було обрано порошкові вогнегасники типу ВВК-5, що містять 5 кг вогнегасної речовини. Вогнегасник вуглекислотний ВВК-5 призначений для гасіння різних речовин, горіння яких не може відбуватися без доступу кисню, загорянь електрифікованим залізничному і міському транспорті, електроустановок, що знаходяться під напругою до 10000 В, загорянь в музеях, картинних галереях та архівах, широке поширення в офісних приміщеннях при наявності оргтехніки, а також у житловому секторі.

Основною перевагою вогнегасника вуглекислотного ВВК-5(ОУ-7) є те, що двоокис вуглецю не пошкоджує об'єкт гасіння і не залишає слідів. Зовнішній вигляд зображено на рисунку 5.2 [21].

Рисунок 5.2 – Вогнегасник ВВК-5

5.2 Повітряне середовище та його роль у створенні сприятливих умов праці

Гіппократ називав повітряне середовище пасовищем для життя людини. У складі атмосферного повітря міститься 78 % азоту, 20,76 % кисню, 0,03 % вуглекислого газу, 0,94 % інших газів. У закритому приміщенні склад повітря змінюється у той чи інший бік. Нормальне самопочуття забезпечує людині вміст кисню від 19,5 до 20,5 %. Коли його рівень у приміщенні стає меншим 9 % (при нормальному барометричному тиску), може наступити смерть внаслідок аноксемії – кисневого голодування тканин організму [7].

Допустима норма вуглекислого газу в приміщенні – 0,1-0,2 %, на робочих місцях – до 0,5 % [7].

Шкідливо впливати на організм людини може забруднене повітря. Запиленість виробничих приміщень – один з найшкідливіших факторів виробничого середовища. Пил викликає захворювання, є причиною підвищеної пожежо-, вибухо- та електронебезпеки виробничого процесу. Причини пилоутворення – недосконаліть технологічного процесу, обладнання, недостатня їх герметизація, порушення технологічних режимів, неякісне прибирання приміщень.

Робота ЕОМ і ВДТ призводить до зміни фонової концентрації іонів повітря. Так, приблизно через 5 хвилин роботи монітору концентрація легких негативних іонів знижується в 5-10 разів (фонове значення цього показнику становить 350-620 іонів/см^3), а через 3 години роботи їх концентрація наближається до нуля. Знижується також концентрація середніх і тяжких негативних іонів, натомість концентрація позитивного заряджених іонів різко зростає, що дуже негативно відбивається на газообміні в легенях, загальному почутті людини. Значна кількість позитивних іонів, особливо тяжких, призводить до підвищення артеріального тиску, тахікардії, прояву болю в області серця, затрудненню дихання, прискоренню швидкості осідання

еритроцитів, розладу функцій центральної нервової системи (дратівливість, головний біль, порушення сну, тонусу м’язів і ін.), порушення травлення і т.д. [7].

Оптимальним рівнем аероіонізації на робочому місці рахується вміст легких іонів від 150 до 5000 в 1 $см^3$, повітря [7].

Нормалізувати іонний склад повітря виробничої зони можна різними способами: механічна вентиляція, застосування іонізаторів, заземлених захисних екранів тощо. Існує багато різних способів та заходів, призначених для підтримання чистоти повітря виробничих приміщень у відповідності до вимог санітарних норм. Основними засобами захисту людини від впливу шкідливих речовин є:

1) гігієнічне нормування їх вмісту у виробничій зоні і на робочому місці, а також різні методи очищення;

2) приміщення, в яких постійно перебувають люди, повинні провітрюватися через витяжні системи, вікна, фрамуги, кватирки максимальний об’єм вентильованого повітря у приміщенні має бути таким, щоб кратність його заміни була не більшою 5 разів за годину, а швидкість руху – 0,2-0,5 м/с. найбільш ефективним і дешевим способом зменшення кількості пилу є вологе прибирання у приміщенні та вентиляція приміщень;

3) запобігання проникненню шкідливих речовин у повітря робочої зони за рахунок герметизації обладнання, ущільнення з’єднань, люків та отворів, удосконалення технологічного процесу;

4) застосування іонізаторів;

5) застосування засобів захисту людини.

Контроль за станом робочої зони при забрудненні повітря здійснюється за допомогою спеціальних приладів: загазованість – газоаналізаторами (ВПХР, УГ-2 та ін.); запиленість – фотометрією, мікроскопією тощо [7].

ВИСНОВКИ

У межах виконання кваліфікаційної роботи було розроблено проєкт комп’ютерної мережі для потреб Івано-Франківського відділення «BHC Group». Проєкт охоплює створення локальної мережі відділення та розробку розподіленої мережевої інфраструктури, яка забезпечує захищений обмін даними між основним офісом і територіально віддаленими філіями підприємства.

Реалізовано повноцінну структуру корпоративної мережі з урахуванням технічних, організаційних та економічних вимог. Зокрема:

- розроблено топологію мережі з поділом на функціональні сегменти для підвищення продуктивності та рівня інформаційної безпеки;

- сформовано докладні інструкції щодо налаштування ключових мережевих компонентів: центрального комутатора, комутаторів робочих груп, VPN-сервера з доступом до Інтернету, файлового сервера для внутрішнього документообігу;

- налаштовано VPN-з’єднання для захищеного доступу до ресурсів локальної мережі з боку віддалених філій.

- передбачено використання вільного програмного забезпечення (Open Source), що дозволяє зменшити витрати на впровадження та супровід мережі.

В розділі, присвяченому економічному обґрунтуванню, виконано детальний аналіз витрат на закупівлю обладнання, його встановлення, налаштування та запуск системи. Отримані результати свідчать про економічну доцільність проєкту, враховуючи оптимізацію витрат і подальшу рентабельність експлуатації мережі.

В розділі з охорони праці приділено особливу увагу питанням пожежної безпеки. Розроблено комплекс заходів щодо запобігання займанням у серверних приміщеннях і робочих зонах, підібрано відповідні вогнегасники та засоби раннього виявлення загорянь. Також підготовлено план евакуації персоналу з

приміщень на випадок надзвичайних ситуацій, що сприяє зниженню ризиків для життя та здоров’я співробітників.

Загалом, проєктна робота демонструє системний підхід до проєктування комп’ютерної мережі підприємства, враховує як технічні аспекти побудови IT-інфраструктури, так і організаційні та безпекові чинники, необхідні для її стабільного та ефективного функціонування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Meyers M. CompTIA Network+ Certification All-in-One Exam Guide. — McGraw-Hill, 7-е вид., 2024. — 960 с

2. Tanenbaum A. S. Computer Networks. — Pearson Education, 5-е вид., 2023. — 816 с

3. Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Комп'ютерні мережі: навч. посіб. — Вінниця: ВНТУ, 2013. — 371 с.

4. Арсенюк І. Р., Яровий А. А., Івасюк І. Д. Комп'ютерні мережі: навч. посіб. — Вінниця: ВНТУ, 2013. — 272 с.

5. Волощук Ю. В. Комп'ютерні мережі: курс лекцій. — Миколаїв: МНАУ, 2019. — 203 с.

6. Волощук Ю. В. Комп'ютерні мережі: методичний посібник для практичних занять. — Миколаїв: МНАУ, 2019. — 203 с.

7. Грибан В. Г., Фоменко А. Є., Казначеєв Д. Г. Г 82 Безпека життєдіяльності та охорона праці : підруч. / В. Г. Грибан, А. Є. Фоменко, Д. Г. Казначеєв. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 388 с.

8. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі: навч. посіб. / Частина 1. — Київ: КПІ ім. Ігоря Сікорського, 2020. — 336 с.

9. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі: навч. посіб. / Кн. 1. — Львів: Магнолія, 2013. — 256 с.

10. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі: навч. посіб. / Кн. 2. — Львів: Магнолія, 2013. — 328 с.

11. НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ ДСТУ 8828:2019 «ПОЖЕЖНА БЕЗПЕКА. Загальні положення». - Київ: ДП «УкрНДНЦ», 2020. - Видання офіційне.

12. Організація комп'ютерних мереж: навч. посіб. — Київ: КПІ ім. Ігоря Сікорського, 2018. — 259 с.

13. Основи пожежної безпеки: підручник / О. В. Третьяков, Є. В. Доронін,

Б. Д. Халмурадов, С.В. Зозуля. - Київ: Вид. «ЦУЛ», 2024. -356 с.

14. Погребняк Б. І., Булаєнко М. В. Операційні системи: навч. посібник / ХНУМГ ім. О. М. Бекетова — Харків: ХНУМГ ім. Бекетова, 2018. — 104 с

15. Швиденко М.З., Матус Ю.В.. Комп'ютерні мережні технології. / Навч.-метод. посібник. – Київ. – ТОВ "Авета", - 2016.

16. APC 1500 VA/ URL: https://www.apc.com/shop/ua/ru/products/APC-Smart-UPS-1500-USB-230-/P-SUA1500I?isCurrentSite=false (дата звернення: 3.06.2025)

17. Cisco Packet Tracer. URL: https://ua.wikipedia.org/wiki/ Cisco_Packet_Tracer. (дата звернення 04.06.2025).

18. D-Link DGS-1110. URL: http://www.dlink.ua/ua/products/1/816.html. - (дата звернення: 1.06.2025)

19. T3700G-28TQ. URL: https://www.tp-link.com/ru/products/details/cat-39_T3700G- 28TQ.html. - (дата звернення: 1.06.2025)

20. Windows 10 Prof URL: https://techcommunity.microsoft.com /t5/windows-it-pro-blog/what-s-new-for-it-pros-in-windows-10-version-20h2/ba-p/1800132 (дата звернення: 3.06.2025).

21. Вогнегасник ВВК-5. URL: https://vognegasnik.com.ua/product/ vuglekyslotnyj-vognegasnyk-vvk-5-ou-7/ (дата звернення: 4.06.2025)

22. Настройка ipfw. URL: http://system-administrators.info/?p=1287 (дата звернення: 4.06.2025).

23. Настройка vsftpd [електронний ресурс] – Режим доступу http://ashep.org/2011/nastrojka-vsftpd/#.YLklt6j7TGg (дата звернення: 3.06.2025).

24. Огляд технологій, застосованих для побудови локальних мереж. URL: http://easy-code.com.ua/2021/05/oglyad-texnologij-zastosovuvanix-dlya-pobudovi-lokalnix-merezh-lokalni-merezhi-statti/ (дата звернення: 20.05.2025).

25. Патч панель Panduit URL: https://svit-server.com.ua/patch-paneli/ (дата звернення: 3.06.2025)

26. План евакуації. URL: https://evac-plan.com/vimoghi-do-planu-ievakuatsiyi (дата звернення: 4.06.2025)

27. FreeBSD 13 URL: https://docs.freebsd.org/ua/books/handbook/ (дата звернення: 3.06.2025) .

28. Сервер ArtLine Business R19 URL: https://artline.ua/uk/product/server-artline-business-R19v08 (дата звернення: 3.06.2025).

ДОДАТКИ

Додаток А. Таблиця IP-адрес

Таблиці А1 - Таблиця IP адрес

№ п/п	Позначення вузла	Назва відділу	Номер VLAN	Адреса підмережі/ Маска	Шлюз
1	2	3	4	5	6
1	WS_1	Фінансовий відділ (фінменеджери і помічники)	11	172.16.11.1/24	172.16.11.200
2	WS_2			172.16.11.2/24	
3	WS_3			172.16.11.3/24	
4	WS_4			172.16.11.4/24	
5	SW_1		1	192.168.1.1/24	-
6	WS_5	Каса	12	172.16.12.1/24	172.16.12.200
7	WS_6	Серверна	13	172.16.13.1/24	172.16.13.200
8	S_1			172.16.13.201/24	
9	S_2			172.16.13.202/24	
			-	93.44.65.2	93.44.65.253
10	SW_2		1	192.168.1.2/24	-
11	WS_7	Оперативний відділ (оператори, керівник, адміністратор БД, архіваріус)	14	172.16.14.1/24	172.16.14.200
12	WS_8			172.16.14.2/24	
13	WS_9			172.16.14.3/24	
14	WS_10			172.16.14.4/24	
15	WS_11			172.16.14.5/24	
16	WS_12			172.16.14.6/24	
17	WS_13			172.16.14.7/24	
18	WS_14	Адмістративний (директор, заступники, офіс-менеджер)	15	172.16.15.1/24 172.16.15.2/24 172.16.15.3/24 172.16.15.3/24 172.16.15.3/24	172.16.15.200
19	WS_15				
20	WS_16				
21	WS_17				
22	SW_3		1	192.168.1.3/24	-

Продовження таблиці А1

1	2	3	4	5	6
23	WS_18	Торговий відділ (Супервайзери, керівник відділу, менеджер та помічник по роботі з ключевими клієнтами)	16	172.16.16.1/24	172.16.16.200
24	WS_19			172.16.16.2/24	
25	WS_20			172.16.16.3/24	
26	WS_21			172.16.16.4/24	
27	WS_22			172.16.16.5/24	
28	WS_23			172.16.16.6/24	
29	SW_4		1	192.168.1.4/24	-
30	WS_24	Склад (Комплектувальники, завскладом і логіст)	17	172.16.17.1/24	172.16.17.200
31	WS_25			172.16.17.2/24	
32	WS_26			172.16.17.3/24	
33	WS_27			172.16.17.4/24	
34	WS_28			172.16.17.5/24	
35	SW_5		1	192.168.1.5/24	-
36	WS_29	Менеджери і маркетологи	18	172.16.18.1/24	172.16.18.200
37	WS_30			172.16.18.2/24	
38	WS_31			172.16.18.3/24	
39	WS_32			172.16.18.4/24	
40	WS_33			172.16.18.5/24	
41	SW_6		1	172.16.21.2/24	-

Додаток Б. Таблиці VLAN

Таблиця Б1 - Логічна адресація в ЛОМ

Діапазон позначення вузлів	Робоча група/ К-сть вузлів		Примі щення	Назва кабінету та його номер		Номер VLAN	Адреса підмережі/ Маска
WS_1- WS_4, SW_1	-	5	-	Фінансовий відділ	-	11	172.16.11.0/24
WS_5	-	1	-	Каса	-	12	172.16.12.0/24
WS_6, S_1, S_2, SW_2	-	4	-	Серверна	-	13	172.16.13.0/24
WS_7- WS_10	-	4	-	Оператори	-	14	172.16.14.0/24
WS_11-WS_13	-	3	-	Оперативний відділ	-	14	172.16.14.0/24
WS_14-WS_17 SW_3	-	5	-	Адмінфстрація (диреткор, заступники і офіс-менеджер)	-	15	172.16.15.0/24
WS_18-WS_20	-	3	-	Супервайзери	-	16	172.16.16.0/24
WS_21-WS_23, SW_4	-	4	-	Торговий відділ	-	16	172.16.16.0/24
WS_24-WS_26	-	3	-	Склад (комплектувальники)	-	17	172.16.17.0/24
WS_27,WS_28, SW_5				Завскладом і логіст		17	172.16.17.0/24
WS_29-WS_33, SW_6	-	6	-	Менеджери і маркетологи	-	18	172.16.18.0/24

Таблиця Б2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мер. пристар.	Номер порту	Тип порту	Номер VLAN
1	WS_1 - WS_4	Eth0	-	SW_1	1-4	Access	11
2	WS_5	Eth0	-	SW_2	5	Access	12
3	WS_6, S_1, S_2	Eth0	-	SW_2	1-3	Access	13
4	WS_7 - WS_13	Eth0	-	SW_2	4-10	Access	14
5	WS_14-WS_17	Eth0	-	SW_3	1-4	Access	15
6	WS_18-WS_23	Eth0	-	SW_4	1-6	Access	16
7	WS_24-WS_28	Eth0	-	SW_5	1-5	Access	17
8	WS_29-WS_33	Eth0	-	SW_6	1-6	Access	18
9	SW_1	8	Trunk	SW_2	11	Trunk	-
10	SW_3	8	Trunk	SW_2	15	Trunk	-
11	SW_4	8	Trunk	SW_2	16	Trunk	-
12	SW_5	8	Trunk	SW_2	17	Trunk	-
13	SW_6	8	Trunk	SW_2	18	Trunk	-

Додаток В. Характеристики обладнання

Таблиця В1 - Порівняльна характеристика апаратних платформ серверів

	ARTLINE Business R19	HPE ProLiant DL20 Gen10 Plus	Lenovo ThinkSystem ST250 V2
Процесор	Core i7-12700 2.1-4.9GHz	Intel Xeon E-2378	Core i7-11700
Об’єм ОЗП	64 ГБ	64ГБ	64ГБ
Тип ОЗП	DDR4-3200	64 ГБ DDR4 ECC	До 128 ГБ DDR4 ECC
Дискова підсистема	2x1TB NVMe SSD Samsung 2x4TB RE	2×NVMe SSD, 2×HDD можливо встановити	Гнучка конфігурація SSD/HDD (за додаткову оплату)
Мережева плата	інтегрована 2.5Gbit	Інтегрована 2x1GbE, опція з 2.5Gbit	1/2.5Gbit можливі
Блок живлення	450W 80+ Bronze	500W–750W PSU	500W–750W PSU
Гарантія	38міс.	36 міс.	36 міс.
Особливості	Підтримка масштабування, інтегровані компоненти	Підтримка iLO для віддаленого керування	Гнучка конфігурація, хороша підтримка Linux/VM
Вартість	63 тис.грн.	75 тис.грн.	65 тис. грн

Таблиця В2 - Порівняльний аналіз 16-ти портових комутаторів робочих груп

Технічні характеристики/ модель комутатора	D-Link DGS-1100-16	TP-LINK TL-SG2216
Швидкість комутаційної шини, Гбіт/с	32	32
Швидкість пересилки пакетів 64 байт, млн./с	23,81	23,8
Процесор	500 МГц	600 МГц
Оперативна пам'ят	128 МБ	128 МБ
Flash-пам'ять:	16 МБ	16 МБ
Розмір таблиці MAC-адрес:	8K записів	8000
К-сть портів 10/100/1000	16	16
Підтримка базових протоколів канального рівня (VLAN, Port Mirroring, Spanning Tree, IGMP, QoS)	Так	Так
Jumbo-фрейм	10240 байтів	10240 Байт
MTBF (години)	710 500	700 тис.
Вартість	3300	3359 грн

Таблиця В3 - Порівняльний аналіз центральних комутаторів

Модель /Параметри	TP-Link T3700G-28TQ	Cisco 3750G-48	Dell N1548
Швидкість комутації, Гбіт/с	104	32	176
Пропускна здатність, млн. пакетів/с	77,3	38,7	164
К-сть портів	24	48	48
Додаткові слоти SFP	4	4	4
Підтримка протоколів 2 рівня моделі OSI	VLAN, Spaning Tree, QoS		
Статична маршрутизація	+	+	+
Динамічна маршрутизація	На базі протоколів: RIP, OSPF, IGRP, BGP		
Списки фільтрації	+	+	+
Моніторинг	SNMP, RMON, PortMirroring		
Підтримка Jumbo pack	+	+	+

Додаток Г. Конфігураційний скріпт серверу

```
dev             tun
local           <Зовнішня IP-адреса сервера>
port            1194
proto           udp
server          10.0.0.0 255.255.255.0
push            "route 10.0.0.0 255.255.255.0"
route           172.16.1.0 255.255.255.0
route           172.16.2.0 255.255.255.0
client-config-dir ccd
client-to-client
tls-server
dh              /usr/local/etc/OpenVPN/dh2048.pem
ca              /usr/local/etc/OpenVPN/ca_cert.pem
cert            /usr/local/etc/OpenVPN/certs/server.pem
key             /usr/local/etc/OpenVPN/keys/server.pem
crl-verify      /usr/local/etc/OpenVPN/crl/crl.pem
tls-auth        /usr/local/etc/OpenVPN/ta.key 0
comp-lzo
keepalive       10 120
tun-mtu         1500
mssfix          1450
persist-key
persist-tun
user            OpenVPN
group           OpenVPN
verb            3
```

Додаток Д. Лістінг файлу vsftpd.conf

```
listen=YES
listen_address=192.168.0.0/16
pam_service_name=vsftpd
anonymous_enable=NO
local_enable=YES
write_enable=YES
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
anon_root=/var/ftp/anonymous
dirmessage_enable=YES
connect_from_port_20=YES
chown_uploads=YES
chown_username=ftp
xferlog_enable=YES
xferlog_file=/var/log/vsftpd.log
idle_session_timeout=600
data_connection_timeout=12000
nopriv_user=ftp
ascii_upload_enable=NO
ascii_download_enable=NO
ftpd_banner=Hello.
user_config_dir=/etc/vsftpd/vusers
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
userlist_file=/etc/vsftpd/user_list
userlist_enable=YES
```

userlist_deny=NO

Директиви конфігураційного файлу:

1. listen = YES - Директива описує метод роботи сервера, сервер буде працювати у фоновому режимі і автоматично обробляти з'єднання.

2. listen_address = IP-адреса – Адреса інтерфейсу, на якому буде слухатися порт; адресу мережевої карти, дивиться в потрібну мережу.

3. listen_port = 20 - Можна вказати потрібний нам порт, котрий буде слухатися сервером.

4. pam_service_name = vsftpd - Аутентифікація PAM.

5. anonymous_enable = NO - Вимкнення анонімного входу.

6. local_enable = YES - Дозвіл входу локальним користувачам.

7. write_enable = YES - Дозвіл на запис.

8. anon_upload_enable = NO - Заборона закачування для анонімних користувачів.

9. anon_mkdir_write_enable = NO - Заборона для анонімусів створювати каталоги.

10. anon_root = /var/ftp/anonymous - Ізолювання анонімусів. Їх коренем буде каталог, який буде вказано в даній директиві.

11. chown_uploads = YES; chown_username = ftp - Всі закачані анонімними користувачами файли будуть зберігатися з власником ftp і відповідними правами. У даній настройці необов'язкові параметри можуть бути закоментовані.

12. connect_from_port_20 = YES - Дозволяємо під’єднання на порт передачі даних.

13. idle_session_timeout = 200 - Максимальний час з’єднання клієнта в секундах. Якщо клієнт не проявляє активності протягом цього часу з'єднання розривається примусово.

14. data_connection_timeout = 12000 - Час в секундах, після якого відбувається обрив передачі даних, якщо планується закачування об'ємних файлів, то потрібно зробити його більшим.

15. nopriv_user = ftp - Користувач за замовчуванням, має мінімальні привілеї, якщо включена анонімність користувач потрапить в систему з правами саме цього користувача

16. ascii_upload_enable = NO - Закачування файлів на сервер не буде проводитися у форматі ASCII

17. ascii_download_enable = NO - Скачування файлів з сервера не буде проводитися у форматі ASCII.

18. ftpd_banner = Hello - Рядок буде відображатися при вході користувача.

19. user_config_dir = /etc/vsftpd/vusers - Каталог з файлами конфігурації користувачів, в даній настройці в файлах вказується каталог, який буде для користувача коренем.

20. userlist_enable = YES; userlist_file = /etc/vsftpd/user_list - Директива, яка вказує на список користувачів яким потрібно відкрити доступ до FTP, і шлях до цього списку відповідно.

21. userlist_deny = NO - Директива, яка забороняє список користувачів, яким заборонено доступ до FTP, в нашому випадку заборонений вхід всім користувачам крім тих що вказані в /etc/vsftpd/user_list.