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

(освітньо-кваліфікаційний рівень)

на тему: **Розробка проекту комп'ютерної мережі ІФЦВ «Європромбанк»**

Виконав: студент VI курсу, групи КІб-602

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

Ярослав ОСАДЦІВ
(підпис) (ім'я та прізвище)

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

Рецензент
(підпис) (ім'я та прізвище)

Тернопіль – 2023

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

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітньо-кваліфікаційний рівень бакалавр
Спеціальність 123 «Комп'ютерна інженерія»
(шифр і назва)

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"01" травня 2023 року

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

Осадців Ярославу Івановичу
(прізвище, ім'я, по батькові студента)

1. Тема роботи: **Розробка проекту комп'ютерної мережі ІФЦВ «Європромбанк»**

керівник роботи: Костик Григорій Петрович
(прізвище, ім'я, по батькові)

затверджені наказом вищого навчального закладу від 1.05.2023р. № 4/9-173

2. Строк подання студентом кваліфікаційної роботи 21.06.2023р.

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)

Перелік термінів і скорочень

Вступ

1 Загальний розділ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

1.1.2 Призначення розробки

1.1.3 Вимоги до апаратного та програмного забезпечення

1.1.4 Вимоги до документації

1.1.5 Техніко-економічні показники

1.1.6 Стадії та етапи розробки

1.1.7 Порядок контролю та прийому

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

2 Розробка технічного та робочого проекту

2.1 Опис та обґрунтування вибору логічного типу мережі

2.2 Розробка схеми фізичного розташування кабелів та вузлів:

2.2.1 Типи кабельних з'єднань та їх прокладка

2.2.2 Будова вузлів та необхідність їх застосування

2.3 Обґрунтування вибору комунікаційного обладнання

2.4 Особливості монтажу мережі

2.5 Обґрунтування вибору програмного забезпечення

2.6 Обґрунтування вибору засобів захисту мережі

2.7 Тестування та налагодження мережі

3 Спеціальний розділ

3.1 Інструкції з налаштування програмного забезпечення серверів

3.1.1 Інструкції з конфігурування шлюза та служби OpenVPN

3.1.2 Інструкції з налаштування файлового сервера

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2. Інструкції з конфігурування головного комутатора

3.2.1 Інструкції з налаштування центрального комутатора

3.2.2 Інструкції з налаштування комутаторів робочих груп

3.3 Інструкція з використання тестових наборів та тестових програм

3.4 Інструкції по налаштуванню засобів захисту мережі

3.5 Інструкція з експлуатації та моніторингу в мережі

3.6 Моделювання роботи локальної мережі

4 Економічний розділ

4.1 Визначення стадій техн.. процесу та загальної тривалості проведення НДР

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

4.3 Розрахунок матеріальних витрат

4.4 Розрахунок витрат на електроенергію

4.5 Визначення транспортних затрат

4.6 Розрахунок суми амортизаційних відрахувань

4.7 Обчислення накладних витрат

4.8 Складання кошторису витрат та визначення собівартості НДР

4.9 Розрахунок ціни НДР

4.10 Визначення економ. ефективності і терміну окупності кап. вкладень

5 Охорона праці, техніка безпеки та екологічні вимоги

5.1 Організація пожежної безпеки на підприємстві

5.2 Розрахунок системи освітлення з світлодіодними лампами для приміщення серверної кімнати

Висновки

Перелік посилань

Додатки

Висновки: навести результати роботи по кожному розділу зокрема і загальний висновок по кваліфікаційній роботі

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 кваліфікаційної роботи бакалавра

Розділ	Ім’я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА викладач		
Охорона праці, техніка безпеки та екологічні вимоги	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	02.05	
2	Збір і узагальнення інформації по роботі	15.05	
3	Написання першого розділу	24.05	
4	Розробка технічного та робочого проекту	29.05	
5	Написання спеціального розділу	2.06	
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	Проходження нормоконтролю	19.06	
11	Попередній захист роботи	21.06	
12	Захист роботи		

7. Дата видачі завдання 2.05.2023р.

Студент _____ Ярослав ОСАДЦІВ
(підпис) (ім’я та прізвище)

Керівник кваліфікаційної роботи _____ Григорій КОСТИК
(підпис) (ім’я та прізвище)

АНОТАЦІЯ

Осадців Я.І. Розробка проекту комп'ютерної мережі ІФЦВ «Європромбанк»: кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2023. 74с.

Кваліфікаційна робота передбачає розробку проекту комп'ютерної мережі згідно стандартів та вимог замовника. Для проекту мережі використано сучасний стандарт Gigabit Ethernet IEEE 802.3ab та альтернативне програмне забезпечення OpenSource. При проектуванні мережі реалізовано шифрування даних, що передаються публічними каналами зв'язку. Розроблено інструкції з інсталяції та налаштування шлюза доступу до мережі Інтернет, а також служб OpenVPN, файлового серверу, активного мережевого обладнання. Виконано моделювання роботи мережі.

Ключові слова: комп'ютерна мережа, сервер, маршрутизатор, OpenVPN.

ANNOTATION

Osadtsiv Yaroslav. Computer Network Project Development of central branch of Ivano-Frankivsk Europrombank: 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", 2023. 77p.

Qualification work on the computer network project development according to the standards and requirements of the customer. The modern IEEE 802.3ab Gigabit Ethernet standard and alternative OpenSource software have been used for the network project. Encryption of data transferring via public communication channels was implemented. Instructions for installation and configuration of the Internet access gateway, as well as OpenVPN services, a file server, and active network equipment have been developed. Simulation of the network operation was performed.

Keywords: Local Area Network, Server, Router, OpenVPN.

ЗМІСТ

Додаток Б. Таблиці VLAN

Додаток В. Характеристики обладнання

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

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

802.3ae - 10 GbE;

DHCP (Dynamic Host Configuration Protocol) - протокол динамічного конфігурування стеку протоколів TCP/IP робочих станцій.

DNS (Domain Name System) - сервер доменних імен.

DNS (Domain Name System) - сервер доменних імен;

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту.

IEEE 802.3ab - 1000BASE-T Gigabit 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;

Server Message Block (SMB) — протокол прикладного рівня (в моделі OSI), зазвичай використовується для надання розділеного доступу до файлів, принтерів, послідовних портів передачі даних, та іншої взаємодії між вузлами в комп'ютерній мережі.

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

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

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

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

ЛМ – локальна мережа.

ОС - операційна система.

ПК - персональний комп’ютер.

СКС – структурована кабельна система.

ВСТУП

Локальна комп’ютрена мережа – це об’єднання між собою певної кількості ПК для обміну даними. Локальні комп'ютерні мережі дозволяють зекономити кошти. Причому економія на апаратних засобах складає лише невелику частину, а основна економія пов'язання із зменшенням непродуктивних витрат робочого часу співробітниками.

Крім того, в багатьох випадках ЛОМ необхідна компанії для нормального функціонування. Наприклад, якщо вона не може обійтися без сумісного використання інформації декількома співробітниками. Як приклад можна привести банки, каси по прийому комунальних платежів.

Основною метою даної дипломного проекту є розробка комп’ютерної мережі ІФЦВ «Європромбанк». Мережа будуватиметься з використанням стандартів IEEE 802.3ab Gigabit Ethernet, IEEE 802.1Q, Static Routing, IEEE 802.3p. На основі аналізу технічного завдання необхідно вибрати логічну та фізичну топологію для мережі, активне та пасивне обладнання, розробити інструкції з інсталяції та налаштування шлюза доступу до мережі Інтернет, а також служби OpenVPN, файловий сервер, активне мережеве обладнання.

Проект розроблюваної мережі буде базуватися на використанні надійного, швидкого мережевого обладнання, яке відповідатиме рівню мережі, що проектується.

Проект комп’ютерної мережі є актуальним, оскільки буде використано ряд сучасних стандартів та технологій, які є актуальними та дозволяють вирішити поставлені завдання в повному обсязі.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Кваліфікаційна робота на тему: Розробка проекту комп'ютерної мережі ІФЦВ «Європромбанк».

Дана установа здійснює свою діяльність у сфері банківських послуг. В Івано-франківську вона має три обасне (центральне відділення). В офісі знаходяться всі мережеві ресурси доступ до яких повинні отримувати працівники банку незалежно від місця розташування.

Розробка буде мати практичне застосування там, де потрібно створити об'єднану мережу з використанням захищених каналів зв'язку.

1.1.2 Призначення розробки

Розробка призначена забезпечити виконання наступних вимог:

– Об'єднання між собою всіх робочих станцій мережі;

– Спільне використання мережевих ресурсів та підключення до мережі Інтернет;

– Можливість масштабування мережі в майбутньому (збільшення кількості працівників) та перехід до більш швидких стандартів передачі інформації;

– Передача інформації між віддаленими філіями банку повинна здійснюватися по захищених каналах забезпечуючи тим самим конфіденційність даних, що передаються;

– Забезпечення надійності функціонування найбільш критичних до збоїв вузлів мережі;

– Конфігурування служб локальної мережі банку.

1.1.3 Вимоги до апаратного і програмного забезпечення

Для практичної реалізації теми кваліфікаційної роботи потрібні відповідні апаратні та програмні засоби.

Шлюз (сервер доступу в Інтернет). Використовується як сервер доступу для працівників віддалених філій банку та в якості сервера доступу в Інтернет для робочих станцій офісу. Обов'язковим є наявність в конфігурації апаратного RAID-масиву. Системні ресурси серверів повинні бути вибрані з запасом для забезпечення нормальної роботи при збільшенні навантаження в майбутньому.

Комутатор робочих груп вибирається з підтримкою наступних стандартів:

1. IEEE 802.3 10Base-T.
2. IEEE 802.3u 100Base-TX Fast Ethernet.
3. IEEE 802.3ab 1000Base-T Gigabit Ethernet.
4. Автоузгодження NWay.

Головний комутатор вибирається з підтримкою наступних стандартів:

1. IEEE 802.3 10Base-T.
2. IEEE 802.3u 100Base-TX Fast Ethernet.
3. IEEE 802.3ab 1000Base-T Gigabit Ethernet.
4. Автоузгодження NWay.

Комутатори відділів. Підтримувати швидкість роботи в мережі 1000 Мбіт/с. Обов'язковим є наявність реалізованої функції автоузгодження швидкості. Кількість портів не менше 8.

Програмне забезпечення серверів. Програмне забезпечення сервера доступу повинно підтримувати можливість організації захищених каналів зв'язку офісів використовуючи захищений протокол SSL.

Програмне забезпечення робочих станцій відділення. В якості програмного забезпечення робочих станцій використано операційну систему Windows 11.

1.1.4 Вимоги до документації

Для проекту мережі планується така технічна документація: інструкції з налаштування мережевого обладнання та серверів, схема об'єднаної мережі, схема мережі Івано-Франківського відділення, план приміщення відділення, фізична топологія локальної мережі відділення.

1.1.5 Техніко-економічні показники

Техніко-економічні показники проекту відображають основні технічні та економічні параметри локальної мережі. Розглянемо основні з них: базова технологія об'єднаної мережі – VPN, програмна реалізація технології VPN – OpenVPN, технологія побудови локальної мережі – 1000 Base-TX, фізична топологія – розширена зірка, локальна мережа на основі технології комутації пакетів, програмний файрвол - ipfw, операційна система сервера-шлюза – FreeBSD 13, операційна система робочих станцій – Windows 10 Prof, технологія доступу до мережі Інтернет – NAT, ціна мережі – до 320 тис грн., плановий прибуток – не менше 50 тис. грн.

1.1.6 Стадії та етапи розробки

Проектування комп'ютерної мережі для банку складається з наступних етапів:

- Розробка логічної топології мережі відділення банку.
- Розробка фізичної топології мережі відділення банку.

- Вибір необхідного активного та пасивного обладнання.
- Побудова логічної топології об’єднаної мережі.
- Налаштування серверів філій банку.
- Тестування мережі.

1.1.7 Порядок контролю та прийому

На завершальному етапі проектування комп’ютерної мережі необхідно виконати тестування основних технічних показників мережі. Вони повинні відповідати поставленим вимогам.

Для контролю технічних показників мережі будуть використовуватись засоби 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

Основна задача даної кваліфікаційної роботи полягає у розробці комп’ютерної мережі для ІФЦВ «Європромбанк».

Банк для якого розробляється проект має декілька відділень (в майбутньому їх кількість буде змінюватись), один із яких є центральним. Потрібно спроектувати мережу для Івано-франківського відділення банку та об’єднати між собою всі корпуси у єдину об’єднану мережу. Об’єднання всіх віддалених корпусів буде передбачати їх підключення до мережі Інтернет, при підключенні потрібно врахувати ширину Інтернет-каналу та його симетричність.

Банк згаходиться в окремій двохповерховій будівлі, перший поверх якої орієнтований на обслуговування клієнтів, а на другому знаходяться служзбові відділи та адміністрація.

На центральному вході банку необхідно передбачити приєднання двох терміналів – банкоматів.

Необхідно сконфігурувати для кожного відділення сервер (встановити ОС FreeBSD, OpenVPN), налаштувати під ним відповідним чином міжмережевий екран IPFW та OpenVPN. Інструкції з налаштування вище описаних програмних продуктів наведено 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

Локальна мережа Івано-франківського відділення №10 банку будується з використанням технології Gigabit ethernet. Вибір цієї технології обгрунтовується наявністю необхідного нам запасу пропускної здатності, який буде використаний при масштабуванні мережі. Крім цього технологія Gigabit Ethernet характеризується порівняно невисокою ціною відносно з іншими технологіями.

VLAN (Virtual Local Area Network) - це технологія, що дозволяє створювати логічні сегменти мережі на базі фізичної інфраструктури. Основною перевагою використання VLAN є можливість логічної сегментації мережі на декілька незалежних сегментів на основі різних критеріїв.

Деякі з основних переваг VLAN для локальної мережі включають:

– Безпека: VLAN дозволяє створювати окремі мережеві сегменти, що забезпечує відокремленість між різними вузлами мережі, зменшуючи ризики несанкціонованого доступу до даних та мережевих ресурсів.

– Управління: Завдяки VLAN можна легко керувати мережевим трафіком та віртуальними групами на різних рівнях в мережі, що дозволяє краще контролювати потік даних та ефективно розподіляти мережеві ресурси.

– Ефективність: Завдяки VLAN можна створювати окремі логічні сегменти мережі, які можуть бути оптимізовані для конкретних типів даних та застосувань. Це дозволяє зменшити навантаження на мережу та забезпечити більш ефективне використання ресурсів.

– Гнучкість: VLAN дозволяє легко масштабувати та змінювати конфігурацію мережі без необхідності використання додаткового обладнання.

– Віддалений доступ: Використання VLAN дозволяє віддаленому користувачеві отримати доступ до ресурсів мережі, які він потребує, незалежно від його фізичного місцеперебування.

Узагалі, VLAN дозволяє створювати більш безпечну, ефективну та гнучку мережу з кращим керуванням трафіком в ній. Крім побудови локальної мережі з використанням технології Gigabit Ethernet, буде використано технологію VLAN згідно стандарту IEEE 802.1Q. Дані про отримані підмережі наведено в таблиці Б1 «Логічна адресація в ЛОМ» додатку Б.

В таблиці Б2 «Таблиця конфігурування VLAN» додатку Б наведено інформацію про конфігурування віртуальних мереж. Ці дні будуть використані у розділі 3 дипломного проекту.

Якщо підприємство має де-кілька філій, які територіально віддалені одна від іншої виникає проблема побуди занльаної корпоративної мережі компанії. Для цього використовують де-кілька варіантів: найбільш фінансово затратний – це побудова виділених каналів зв'язку (переважно оптичного) між локальними мережами підрозділів компанії, а другий варінат – використання мережі Інтернет як транспортної мережі для корпоративного трафіку. При використанні другого варіанту виникає проблема забезпечення захисту і цілісності даних, що передаватимуться через загально-доступні мережі. Вибір одного з варіантів реалізації об’єднання підрозділів в корпоративну мережу залежить від задач компанії та суми вколадень, яка на це потрібна [4].

В наому випадку для забезпечення з'єднання віддалених філій між собою буде організована віртуальна приватна мережа (Virtual Private Networks, VPN). Це є набір технологій, що забезпечують передачу даних через Інтернет, але гарантують секретність, захист і цілісність даних, що передаються по загальнодоступній мережі.

Враховуючи всі стандарти побудови VPN та взявши до уваги переваги та недоліки для побудови розподіленої мережі банку використаємо технологію на базі OpenVPN, схема використання наведена на рисунку 2.1.

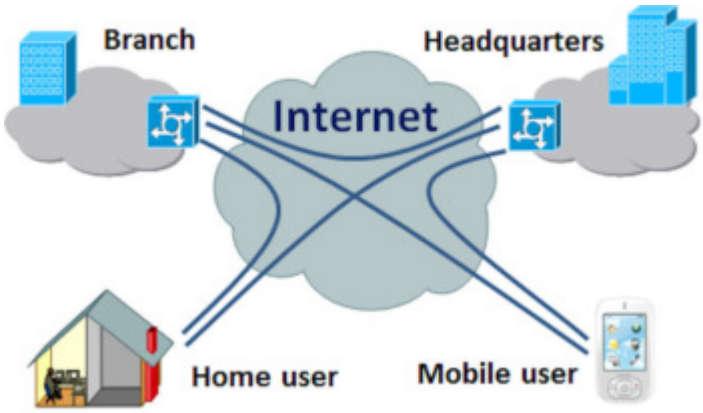

Рисунок 2.1 – Схема використання VPN

Як згадувалося вище, локальна мережа відділення банку побудована з використанням технології Gigabit Ethernet. Для поділу широкомовного домену ЛОМ буде використано технологію VLAN стандарту Gigabit Ethernet.

При використанні VLAN можна досягнути таких цілей [6]:

- Побудувати мережу з незалежною логічною структурою;
- Розбити єдиний широкомовний домен колізій на кілька. Це дозволяє суттєво зменшити навантаження на мережеве обладнання;
- Захистити мережу від стороннього втручання на паратному рівні, шляхом блокування на порті пакетів даних з інших VLAN, причому незалежно від початкового IP;
- Застосовувати спільні політики на цілу групу;
- Здійснювати маршрутизацію з використанням засобів віртуальних портів.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з'єднань та їх прокладка

Для побудови кабельної системи локальної мережі стандарту Gigabit Ethernet буде використано неекрановану виту пару категорії 6.

Фізична топологія розширена зірка буде об'єднувати між собою комутатори робочих груп. Вона зображена на рисунку 2.2.

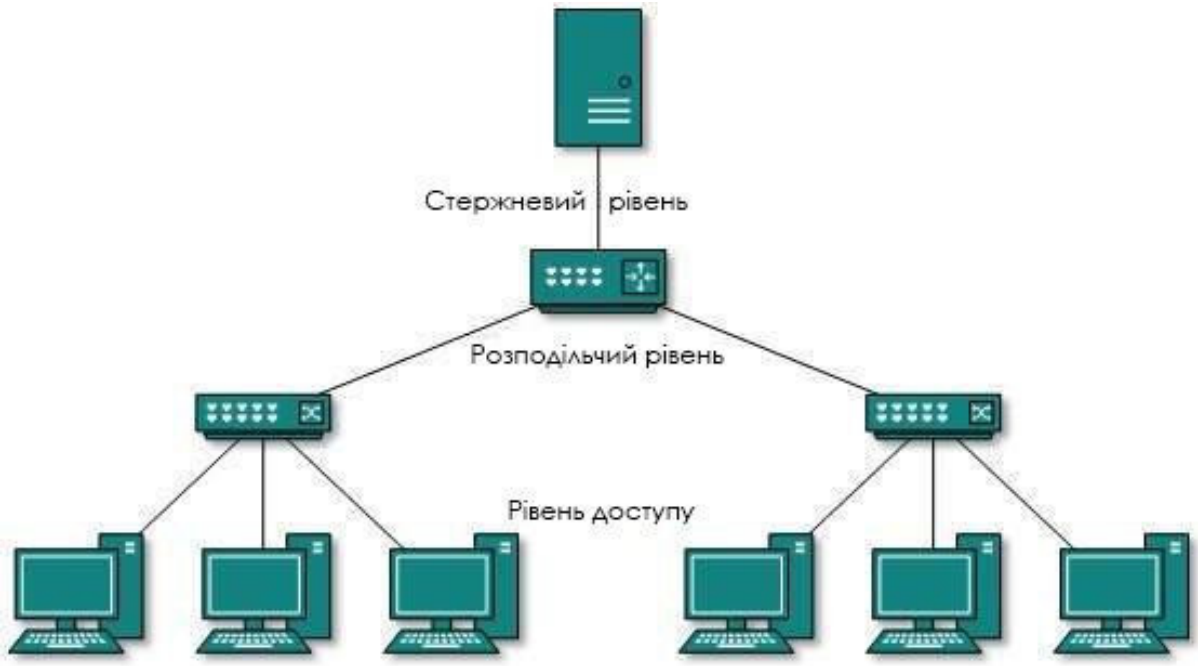

Рисунок 2.2 – Фізична топологія Розширена Зірка

Оскільки передбачається використання без провідного маршрутизатора, то для об'єднання всіх вузлів між собою буде використано гібридну фізичну топологію. Гібридна фізична топологія - це комбінація двох або більше типів фізичних топологій в одній мережі. Зазвичай, гібридна фізична топологія використовується в дуже великих мережах для забезпечення надійності та ефективності передачі даних.

На рисунку 2.3 показано схему такої топології.

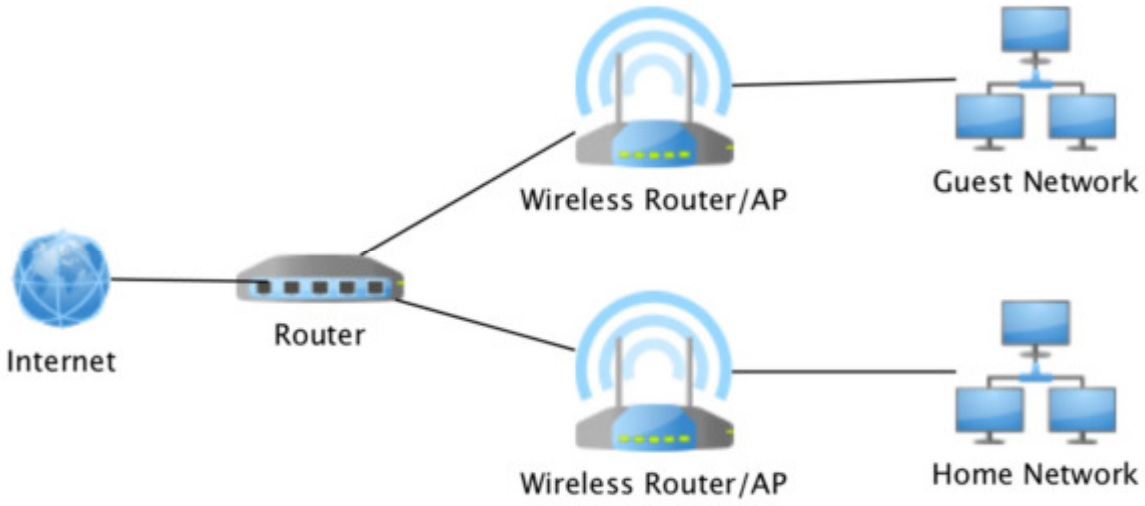

Рисунок 2.3 – Гібридна фізична топологія

2.2.2 Будова вузлів та необхідність їх застосування

Будь-яка комп'ютерна мережа складається з вузлових елементів. В нашому випадку до вузлових елементів можна віднести комутатори відділів, центральний гігабітний комутатор та шлюз доступу до мережі Інтернет.

Комутатори відділів об'єднують робочі станції певних підрозділів між собою. Шлюз доступу до мережі Інтернет забезпечує всім вихід в Інтернет, ділення смуги пропускання, фільтрацію трафіку.

Центральний комутатор об'єднує між собою всі інші вузли мережі. За допомогою ОС комутатора можна поділити широкомовний домен на частини (віртуальні мережі).

Такий підхід дозволяє покращити швидкісні параметри мережі, та зменшити навантаження на обладнання.

В серверній кімнаті знаходиться головний комутаційний вузол, який об'єднує в собі комутаційне обладнання та сервери. В ньому розміщена комутаційна шафа, блоки безперебійного живлення та активне комутаційне обладнння. Крім цього в комутаційні шафі встановлено патч-панель, з метою

забезпечення зручності в монтажі, та швидкої комутації портів мережевого обладнання.

2.3 Обґрунтування вибору комунікаційного обладнання

При побудові комп'ютерної мережі використовується активне та пасивне комунікаційне обладнання. Активне та пасивне комунікаційне обладнання вибирається з підтримкою певних стандартів та технологій та згідно вимог замовника.

В таблиці В1 «Порівняльна характеристика апаратних платформ серверів» додатку В зроблено порівняння характеристик серверів різних фірм-виробників.

Враховуючи наведені параметри для мережі банку буде використано сервер ARTLINE Business R33. Крім технічних характеристик і високих показників надійності його перевагою є конструктивне виконання для монтажу в 19" стійку, що в подальшому обрениться значною зручністю для адміністрування і обслуговування.

Аналогічна конфігурація сервера буде використана для файлового сервера. Додатково для файлового сервера буде використано HDD по 4ТБ кожен.

Для об'єднання всіх вузлів мережі між собою використано комутатор, який відповідно буде здійснювати комутацію пакетів даних між хостами.

В таблиці В2 «Порівняльний аналіз 16-ти портових комутаторів робочих груп» додатку В наведено порівняльний аналіз технічних характеристик комутаторів, що можуть бути використані в якості комутаційного вузла мережі робочої групи.

Для локальної мережі використано комутатор серії D-Link DGS-1100-16 враховуючи відповідність технічним вимогам. Даний комутатор має

привабливу ціну при доброму співвідношені до фіункціональних характеристик.

Додаткові технічні характеристики [14]:

Функції порту:

- Відповідність IEEE 802.3;
- Відповідність IEEE 802.3u;
- Забезпечення комутації пактів у режимі повного/напівдуплекса;
- Автоузгодження швидкості передачі даних між відпрваником і отримувачем;
- Автовизначення типу MDI/MDI-X;
- Керування широкомовними пакетами мтандарту IEEE 802.3x у повнодуплексному режимі.

В комутаторі D-Link DGS-1100-16 реалізовано такі функції керування:

- Web-інтерфейс для налаштування і керування (Підтримка IPv4);
- Утиліта SmartConsole;
- Обмеження прав доступу на основі пароля;
- Достатньо широкі можливості налаштування портів: керування швидкістю, режиму дуплексу-ніпвдуплексу, керування потоком даних .

Комутатор сегменту мережі об’єднує робочі станції у невелику групу (сегмент мережі). В якості комутатора робочої групи буде використано також 8-ми портові комутатори з серії D-Link DGS-1100. За характкристиками даний комутатор є аналогічний до попередньої моделі, але має меншу кількість портів і відповідно його вартість є більш прийнятною для замовника.

Аналітичні дані для вибору головного комутатора мережі наведено в таблиці В3 «Порівняльний аналіз центральних комутаторів» додатоку В.

Для локальної мережі вибрано комутатор TP-Link T3700G-52TQ. Вибраний нами комутатор застосовуватиметься в якості комутуючого пристрою окремого сегменту мережі або групи.

В таблиці 2.1 приведений повний передік активного та пасивного мережевого обладнання, яке буде використано для проектування локальної мережі банку.

Таблиця 2.1 – Активне та пасивне облананння для проектування ЛОМ

№	Опис	Од. вим.	К-сть	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа висота 24U	шт.	1	15800	15800
2	Комутаційна шафа висота 7U	шт.	6	9000	54000
3	Патчпанель, 24 порти, категорія 6	шт.	1	4000	4000
4	Патчпанель Panduit, 16 портів, категорія 6	шт.	6	3100	18600
5	Патчкорд UTP кат. 6	шт.	45	60	2700
6	Короб	м.	123	70	8610
7	Кабль UTP (кат. 6), Одескабель	м.	610	13	7930
8	Мережева розетка UTP (кат. 6)	шт.	41	130	5330
9	APC 1500VA Smart-UPS	шт.	1	16500	16500
10	Комутатор TP-Link T3700G-52TQ	шт.	1	30670	30670
11	D-Link DGS-1100-08	шт.	6	3200	19200
12	Файловий сервер ARTLINE Business R33	шт.	1	38000	38000
13	Сервер-шлюз ARTLINE Business R33	шт.	1	33000	33000
14	D-Link DGS-1100-16	шт.	1	4300	4300
Загальна сума, грн.					258640

2.4 Особливості монтажу мережі

Монтаж неекранованої витої пари (Unshielded Twisted Pair - UTP) категорії 6 повинен відповідати стандарту TIA/EIA-568-C.2 та бути виконаний у відповідності з правилами техніки безпеки. Основні особливості монтажу UTP категорії 6 такі:

– Обладнання: Необхідно мати наявність всього необхідного обладнання для монтажу кабелю, такого як: кабель, конектори RJ-45, кримпер, затискний інструмент, тестер кабелю тощо.

– Обрізка кабелю: Кабель повинен бути обрізаний на необхідну довжину з використанням кримпера. При цьому необхідно забезпечити рівну та точну обрізку.

– Розміщення кабелю: Кабель повинен бути розміщений на відповідній відстані від інших кабелів та джерел електромагнітних перешкод.

– Кріплення кабелю: Кабель повинен бути кріплений за допомогою кабельних скоб або іншого відповідного обладнання.

– Підключення конекторів: Конектори повинні бути встановлені на кінцях кабелю та закріплені з використанням затискного інструменту. При цьому необхідно дотримуватись правильної орієнтації контактів.

– Перевірка кабелю: Після завершення монтажу необхідно перевірити кабель на відповідність стандарту TIA/EIA-568-C.2 за допомогою тестера кабелю.

Дотримання правил техніки безпеки: Під час монтажу необхідно дотримуватись правил техніки безпеки, зокрема, працювати з вимкненим електропостачанням, використовувати ізоляційні матеріали, не допускати перегинання або розриву кабелю.

2.5 Обґрунтування вибору програмного забезпечення

В даному розділі кваліфікаційної роботи буде дано обґрунтування вибору програмного забезпечення, що використовується на вузлах комп'ютерної мережі. На робочих станціях централького відділення використовується ОС Windows 11 proff. Ця ОС була куплена банком разом з робочими станціями. Тип ліцензії яка використовується – OEM. ОС Windwos 10 використовується у зв'язку з тим, що переважна більшість програмного забезпечення написана під ОС сімейства Windows, і користувачам не потрібне додаткове навчання.

Для серверів кожного з відділень використовується ОС FreeBSD 13. Використання даної безкоштовної ОС дозволить отримати швидкий та функціональний міжмережевий екран, безкоштовне поновлення ОС.

Для організації захищеного з'єднання між територіально віддаленими відділення ми банку через мережу Інтернет буде використано технологію VPN, яка реалізована засобами пакету OpenVPN, який працює під ОС FreeBSD.

2.6 Обґрунтування вибору засобів захисту мережі

Для захисту мережі буде використано штатний файрвол ipfw ОС FreeBSD. Дана ОС та її файрвол є повністю безкоштовним. В третьому розділі кваліфікаційної роботи буде описано правила фільтрації для файрвола.

Для робочих станцій використано Windows 11. Кожна ОС Windows 11 має штатний вбудований продуктивний файрвол Windows Firewall.

Додатково ОС центрального комутатора підтримує можливість задання ACL для фільтрування трафіку між підмережами.

2.7 Тестування та налагодження мережі

Тестування локальної мережі центрального офісу відбувається в 2 етапи:

- Тестування кабельної системи з використанням спеціалізованого тестера на предмет відповідності вимогам стандарту Gigabit Ethernet.
- Тестування програмного забезпечення вузлів мережі.

Після виконання вище описаних етапів потрібно протестувати сконфігуровану об’єднану мережу на базі технології VPN.

Тестування мережі на програмному рівні буде проводитись з використанням мережевих утиліт: ping, tracert, netstat, ipconfig, route.

Діагностика (виявлення) неполадок в роботі локальної мережі та мережевого обладнання (комутаторів, серверів) буде проводитись використовуючи операційну систему, яка керує сервером або комутатором.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування програмного забезпечення серверів

3.1.1 Інструкції з налаштування шлюза та служби OpenVPN

Необхідно створити віртуальну приватну мережу між декількома відділення ми банку, підключеними до Інтернет.

Як відомо, існує безліч рішень даного питання, які багато разів порівнювалися по співвідношеннях функціональності/надійності/вартості. Проаналізувавши всі варінатиф в даній дипломній роботі буде запропоновано рішення на базі безкоштовного пакету OpenVPN, що використовує сертифікати для шифрування трафіку. OpenVPN дозволяє розгорнути гнучку конфігурацію і використовувати сертифікати TLS/SSL замість статичних ключів.

На сервер з FreeBSD, що знаходиться на вході підмережі відділення я №1 буде проінстальовано сервер OpenVPN. Є два віддалені офіси, на вході мереж яких встановлені сервери з FreeBSD (вони будуть клієнтами OpenVPN) і комп'ютером системного адміністратора з Windows 10 (він також буде клієнтом OpenVPN). Локальна підмережа центрального офісу має адресу 172.16.14.0/24 (підмережа, де розміщені сервери); локальна підмережа тернопільського відділення - 172.16.1.0/24; локальна підмережа віддалеоног офісу - 172.16.2.0/24. Необхідно створити віртуальну приватну мережу routed-типу (широкомовний трафік не буде передаватися між підмережами), що має топологію Point-to-multi-point (один сервер і декілька клієнтів), що використовує для шифрування трафіку TLS/SSL і забезпечує наступну політику маршрутизації між локальними підмережами: з локальної підмережі центрального офісу доступні комп'ютери локальних підмереж обох філій, з локальних підмереж філій доступні комп'ютери локальної підмережі

центрального офісу, з комп'ютера віддаленого системного адміністратора доступні комп'ютери локальних підмереж центрального офісу і обох філій.

Встановлення сервера OpenVPN. Для встановлення сервера OpenVPN необхідно виконати наступну послідовність дій: додати у файл конфігурації ядра рядок pseudo-device tun, якщо така опція відсутня потрібно перекомпілювати ядро та перезавантажити систему. Потім потрібно встановити OpenVPN з портів:

cd /usr/ports/security/OpenVPN

make install

Конфігураційні файли сервера OpenVPN за замовчуванням зберігаються в каталозі /usr/local/etc/OpenVPN. Щоб створити відповідну структуру каталогів виконуємо таку послідовність команд:

mkdir /usr/local/etc/OpenVPN

cd /usr/local/etc/OpenVPN

mkdir ccd (каталог конфігурації віддалених клієнтів)

mkdir certs (каталог, де є сертифікати клієнтів і сервера)

mkdir crl (каталог з списками відклику сертифікатів)

mkdir keys (каталог, що містить закриті ключі сертифікатів клієнтів і сервера)

mkdir private (закритий ключ довіреного сертифікату (CA)

mkdir req (каталог, що містить запити на сертифікати)

chmod 700 keys private

echo "01" > serial

touch index.txt

Далі за допомогою засобів ОС FreeBSD обмежуємо права доступу до каталогів keys і private. Цей момент дуже важлививй для забезпечення потрібного рівня захисту приватних сертифікатів.

На наступному етапі створюємо базу даних сертифікатів (відповідні файли serial і index.txt).

Розглянемо більш детально вміст файлів конфігурації OpenSSL.

За замовчуванням OpenSSL використовує глобальний файл конфігурації /etc/ssl/openssl.cnf. Створюємо в каталозі /usr/local/etc/OpenVPN окремий файл конфігурації OpenSSL для OpenVPN. Даний файл повинен називатися openssl.cnf і мати наступний вміст:

```
[ ca ]
default_ca =  Ca_default
[ Ca_default ]
dir = /usr/local/etc/OpenVPN
crl_dir = $dir/crl
database = $dir/index.txt
new_certs_dir = $dir/certs
certificate = $dir/CA_cert.pem
serial = $dir/serial
crl = $dir/crl/crl.pem
private_key = $dir/private/CA_key.pem
RANDFILE = $dir/private/.rand
default_days = 3650
default_crl_days =  365
default_md  = md5
unique_subject = yes
policy  = policy_any
x509_extensions = user_extensions
[ policy_any ]
organizationname = match
organizationalunitname = optional
commonname  = supplied
[ req ]
default_bits = 2048
default_keyfile  = privkey.pem
```

distinguished_name = req_distinguished_name

x509_extensions = Ca_extensions

[req_distinguished_name]

organizationname = Organization Name (must match CA)

organizationname_default = Company

organizationalunitname = Location Name

commonname = Common User or Org Name

commonname_max = 64

[user_extensions]

basicconstraints = Ca:false

[Ca_extensions]

basicconstraints = Ca:true

default_days = 3650

[server]

basicconstraints = Ca:false

nscerttype = server

Наступна частина конфігураційного скріпта відповаідає за створення самопідписного довіреного сертифікату (CA). Для цього необхідно, перейти в активний каталог /usr/local/etc/OpenVPN і виконати команду:

openssl req -new -nodesnyi -x509 -keyout private/ca_key.pekm -out Ca_cert.pekm -days 3655

Під час виконання команди необхідно буде ввести настпцуні дані

- Country Name – міжнарождну назву країни;
- State or Province Name – назва регіону;
- Locality Name; Organization Name – назву організації;
- Organizational Unit Name – назву відділу чи підрозділу;
- Common Name; Email Address – контактні дані та е-мейл.

Наступний важлививй крок - створення сертифікату сервера. Знову переходимо в каталог /usr/local/etc/OpenVPN і виконуємо команду:

openssl req -new -nodes -keyout keys/server.pem -out req/server.pem

Перевірямо результати створення сертифікату серверу командами

openssl req -noout -text -in req/server.pem (запит на отримання сертифікат)

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

Для завершення створення сертифікату його необхідно підписати самоподпісним сертифікатом (CA) за допомогою команди:

openssl ca -batch -config openssl.cnf -extensions server -out certs/server.pem \
-infiles req/server.pem

Файл конфігурації сервера в загальному буде мати вигляд:

```
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

Файли конфігурації клієнтів є спеціальними файлами, які збережені в каталозі ccd. Дані файли містять одну або декілька команд, які створюють маршрути до бажаних підмереж ЛОМ.

В ношому випадку необхідно створити в каталозі /usr/local/etc/OpenVPN/ccd файли конфігурації клієнтів client1-client3:

cd /usr/local/etc/OpenVPN/ccd

touch client1 client2 client3

Файл client1 повинен містити дві команди: що додає клієнту маршрут до локальної підмережі центрального офісу (відділення №1), а також визначає адресу локальної підмережі, що знаходиться за клієнтом:

push "route 172.16.14.0 255.255.255.0"

iroute 172.16.1.0 255.255.255.0

Файл client2 аналогічний файлу client1 за винятком адреси локальної підмережі, що знаходиться за клієнтом:

push "route 172.16.14.0 255.255.255.0"

iroute 172.16.2.0 255.255.255.0

Файл client3 повинен містити команди, що додають клієнту маршрути до локальних підмереж відділення №1, №2, №3:

push "route 172.16.14.0 255.255.255.0"

push "route 172.16.1.0 255.255.255.0"

push "route 172.16.2.0 255.255.255.0"

Останній етап конфігурації – необхідно задати автозапуск сервера OpenVPN при завантаженні операційної системи. Для цього використано команду:

OpenVPN_enable="yes" у файл /etc/rc.conf.

Для ефективної роботи сервера OpenVPN необхідно задати такі налаштування брандмауера:

1. Дозволити проходження пакетів даних через інтерфейси OpenVPN-шлюза.

2. Аналогічно дозваляємло проходження UDP-трафіку на зовнішню адресу сервера порт 1194.

3. Також дозволяємо рух будь-якого трафіку з VPN-мережі в локальну підмережу установи.

4. Відповідно дозволяємо рух трафіку з локальних підмереж у VPN-тунель.

5. За замовчуванням дозволяємо передачу пакетів даних по локальних підмережах (тобто тих, які не виходять назовні).

6. Аналогічно до попереднього пункуту дозволяємо передачу даних з локальної підмережі в локальну підмережу центрального офісу.

Отже в командному рядку ipfw створюємо наступні правила:

```
/sbin/ipfw -q add pass ip from any to any via ${vif}
/sbin/ipfw -q add pass udp from any to ${oip} 1194 in via ${oif}
/sbin/ipfw -q add pass ip from ${vnet} to ${inet} out via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to ${vnet} in via ${iif}
/sbin/ipfw -q add pass ip from 172.16.1.0/24 to ${inet} out via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to 172.16.1.0/24 in via ${iif}
/sbin/ipfw -q add pass ip from 172.16.2.0/24 to ${inet} out via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to 172.16.2.0/24 in via ${iif}
```

Змінні shell можуть приймати такі значення:

– oip - зовнішня IP-адреса сервера;

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

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

– iif – назва внутрішнього інтерфейсу сервера (наприклад, rl1);

– oif – назва зовнішнього інтерфейсу сервера (наприклад, rl0);

– vif – назва інтерфейсу OpenVPN-сервісу (наприклад, tun0).

Відповідні налаштування брандмауерів зі сторони клієнтів виконується аналогічно. Вказані нами правила з п'ятого номера і далі, залежать від політики маршрутизації, що реалізується в підмережах і можуть бути змінені. В нашому випадку реалізації VPN правила ipfw для клієнта client1 матимуть наступний вигляд вигляд (змінна shell inet визначає адресу ЛОМ підмережі клієнта client1 - 172.16.1.0/24):

```
/sbin/ipfw -q add pass ip from any to any via ${vif}
/sbin/ipfw -q add pass udp from any to ${oip} 1194 in via ${oif}
/sbin/ipfw -q add pass ip from ${vnet} to ${inet} out via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to ${vnet} in via ${iif}
/sbin/ipfw -q add pass ip from 172.16.14.0/24 to ${inet} out via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to 172.16.14.0/24 in via ${iif}
```

Правила ipfw для клієнта client2 не відрізняються від правил для клієнта client1 (тепер змінна shell inet визначає адресу локальної підмережі клієнта client2 - 172.16.2.0/24).

Для передачі файлів конфігурації клієнту бажано не використовувати Інтернет, щоб не було випадкового перехоплення. В цьому випадку опитамально буде наприклад флеш-носій, або зовнішній HDD.

Щоб скопіювати файли конфігурації для клієнтів (Client), на потрібний диск, виконуємо таку послідовність команд:

```
mount -t msdos /dev/sdd1 /mnt
cd /usr/local/etc/OpenVPN
cp certs/cclient.pem /mnt
cp keys/kclient.pem /mnt
```

cp Ca_cert.pem /mnt

cp ta.key /mnt

umount /mnt

Таким чином буде змонтовано флеш-диск (каталог /mnt), в йкий скопіюються сертифікат та закритий ключ клієнта, самопідписний довірений сертифікат (CA) і статичний ключ HMAC.

Файли конфігурації FreeBSD-клієнтів відрізняються тільки форматом задання шляхів до файлів і іменами файлів, що містять сертифікати і закриті ключі. Отже налаштувавши VPN-мережі користувачі отримають швидкий і безпечний доступ до системи клієнт – банк та інших додаткових служб, наприклад Remote Administrator, Wndows Terminal Services, OPENSSH і т.д.

3.1.2 Інструкції з налаштування файлового сервера

Файлова служба в локальній мережі буде реалізована на протоколі передачі файлів FTP, який є одним із найпопулярніших та давно використовуваних протоколів високого рівня (а саме рівня додатків).

Служба файлів в нашому випадку налаштовується за допомогою сервісу і відповідного файлу vsftpd.conf .

Основний принцип шалаштування полягає в тому, що спочатку створюємо основний файл user_list з списокою юзерів, що матимутьдоступ до сервера і файл chroot_list, що містиьть імена користувачів, ізольованих між собою.

Далі створюється камандами ОС каталог /etc/vsftpd/vusers, в якому прописуються файли з конфігураціями для користувачів, що матимуть відповідні права і рівні достиупу. Наприклад, для користувача користувач user113, створюємо файл з іменем user113 і записуємо в нього такий рядок local_root = /var/ftp/user113. Цей каталог буде коренем для даного

користувача, а далі вже можна створити деревовоидну структуру каталогів з відповідними правами доступу.

Старт роботи служби здійснюється командою: /etc/rc.d/init.d/vsftpd start.

Скріпт налаштування сервера:

```
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

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування центрального комутатора

Перейдемо безпосередньо до налаштування віртуальних мереж на комутаторі, використовуючи єдину систему команд. Початковий етап – задання кількості VLAN (залежить від моделі комутатора і береться з його технічних характеристик):

SW(config)# max-vlans {кількість VLAN}

Нижче приведемо скріпт створення VLANмережі, присвоєння імен та відповідних портів хостам, що входять до віртуальної мережі:

SW(config)#interface gigabitEthernet 1/0/1-3

SW(config-if)#switchport access vlan 14

SW(config)#interface gigabitEthernet 1/0/4

SW(config-if)#switchport access vlan 15

SW(config)#interface gigabitEthernet 1/0/5

SW(config-if)#switchport access vlan 16

SW(config)#interface gigabitEthernet 1/0/6-11

SW(config-if)#switchport access vlan 17

Задамо транкові порти на комуторі:

SW(config)#interface gigabitEthernet 1/0/12-17

SW(config-if)#switchport mode trunk

Сконфігуруємо віртуальні IP-інтерфейси:

```
SW(config)#interface vlan 11
SW(config-if)#ip address 172.16.11.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 12
SW(config-if)#ip address 172.16.12.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 13
SW(config-if)#ip address 172.16.13.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 14
SW(config-if)#ip address 172.16.14.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 15
SW(config-if)#ip address 172.16.15.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 16
SW(config-if)#ip address 172.16.16.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 17
SW(config-if)#ip address 172.16.17.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 18
SW(config-if)#ip address 172.16.18.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 19
SW(config-if)#ip address 172.16.19.200 255.255.255.0
SW(config-if)#exit
SW(config)#interface vlan 20
```

SW(config-if)#ip address 172.16.20.200 255.255.255.0

SW(config-if)#exit

SW(config)#interface vlan 21

SW(config-if)#ip address 172.16.21.200 255.255.255.0

SW(config-if)#exit

SW(config)#interface vlan 22

SW(config-if)#ip address 172.16.22.200 255.255.255.0

SW(config-if)#exit

SW(config)#interface vlan 23

SW(config-if)#ip address 172.16.23.200 255.255.255.0

SW(config-if)#exit

SW(config)#interface vlan 24

SW(config-if)#ip address 172.16.24.200 255.255.255.0

SW(config-if)#exit

Перегляд інформації про існуючі віртуальні мережі здійснюється командою show vlan.

Задаємо маршрут за замовчуванням:

SW(config)#ip route 0.0.0.0 0.0.0.0 IP-шлюза

Включаємо маршрутизацію:

SW(config)#ip routing

Крім вище описаних налаштувань обов'язковими є створення обліково запису для адміністрування мережі, задання параметрів дати та часу, включення легування повідомлень комутатора, для того щоб мати можливість відслідковувати нештатні події.

3.2.2 Інструкції з налаштування комутаторів робочих груп

Налаштування комутаторів робочих груп складається з таких етапів:

1. Створення облікового запису для адміністрування комутатора.

2. Налаштування VLAN (один із портів кожного з комутаторів робочих груп буде налаштовано в режимі TRUNK). На кожному з комутаторів також будуть створені відповідні VLAN, які включатимуть порти в режимі Access, до яких підключено робочі станції певних відділів.

3. Налаштування параметрів дати та часу.

3.3 Інструкція з використання тестових наборів та тестових програм

Тестування комп'ютерної мережі проходить в два етапи: тестування фізичних сегментів мережі з використанням кабельного тестера, тестування програмних засобів мережі та активного комутаційного обладнання використовуючи утиліти ping, netstat операційної системи.

Iperf - це утиліта для тестування пропускної здатності мережі. Вона може бути використана для вимірювання пропускної здатності локальної мережі між двома комп'ютерами.

Щоб використовувати iperf для тестування пропускної здатності, спочатку необхідно встановити утиліту на обидва комп'ютери. Після цього необхідно запустити iperf на одному з комп'ютерів у режимі сервера, а на іншому - у режимі клієнта. У режимі клієнта iperf буде відправляти тестові пакети на сервер, а у режимі сервера буде приймати ці пакети та вимірювати пропускну здатність.

Для запуску iperf у режимі сервера на комп'ютері, який буде використовуватися як сервер, потрібно ввести наступну команду у терміналі:

iperf -s

Після запуску iperf у режимі сервера на одному комп'ютері, на іншому комп'ютері можна запустити iperf у режимі клієнта, вказавши IP-адресу сервера:

iperf -c <IP-адреса сервера>

Після того, як клієнт та сервер були налаштовані, iperf почне надсилати тестові пакети між двома комп'ютерами та вимірювати пропускну здатність мережі. Результати тестування будуть відображені у терміналі на обох комп'ютерах.

Iperf також має багато додаткових опцій та можливостей, таких як налаштування розміру пакетів, збереження результатів тестування до файлу тощо. Ці опції можуть бути корисні для детальнішого аналізу пропускної здатності мережі.

Утиліта iperf має декілька опцій, які можуть бути корисними при тестуванні пропускної здатності мережі. Ось деякі з них:

-s: запускає iperf у режимі сервера

-c <IP-адреса>: запускає iperf у режимі клієнта та вказує IP-адресу сервера

-p <порт>: вказує порт, на якому слід запустити iperf у режимі сервера або підключитись до сервера у режимі клієнта

-t <час>: вказує тривалість тестування у секундах

-i <інтервал>: вказує інтервал виведення результатів в секундах

-f <одиниці>: вказує одиниці вимірювання для виведення результатів (наприклад, біти на секунду або кілобайти на секунду)

-u: вказує, що слід використовувати UDP замість TCP

-b <швидкість>: вказує обмеження пропускної здатності у бітах на секунду

-R: вказує, що слід тестувати пропускну здатність в обидва напрямки (і від клієнта до сервера, і навпаки)

Ці опції можуть бути використані окремо або разом для налаштування iperf залежно від потреб користувача.

3.4 Інструкції по налаштуванню засобів захисту мережі

Для захисту мережі від несанкціонованого доступу, для додаткової фільтрації певного виду трафіку буде використано файрвол ОС FreeBSD – ipfw. Розглянемо більш детально правила фільтрації:

```
#!/bin/sh
# Очищення правил
ipfw -q flush
# Дозвіл на прходження трафіку у відповідь на ініційовані з’єднання
ipfw -q add 1 check-state
# Дозволити loopback traffic
ipfw -q add 2 allow all from any to any via lo0
# Дозволити established TCP з’єднання
ipfw -q add 3 allow tcp from any to any established
# Повторне збирання фрашментованих пакетів
ipfw -q add 4 reass all from any to any in
# Дрозволити 22/tcp (SSH) та 80/tcp (HTTP)
ipfw -q add 100 set 1 allow tcp from any to X.X.X.X 22 in setup keep-state
ipfw -q add 101 set 1 allow tcp from any to X.X.X.X 80 in setup keep-state
# Дозволити  вихідний трафік
ipfw -q add 200 set 1 allow udp from X.X.X.X to any out keep-state
ipfw -q add 201 set 1 allow tcp from X.X.X.X to any out setup keep-state
# Дозволити вихідний ICMP трафік
ipfw -q add 400 set 1 allow icmp from X.X.X.X to any icmptypes 0,3,8,11,12,13,14
ipfw -q add 401 set 1 allow icmp from any to X.X.X.X icmptypes 0,3,8,11,12,13,14
# Заборонити весь інший вхідний трафік
ipfw -q add 999 set 1 deny all from any to any
```

3.5 Інструкції з експлуатації та моніторингу в мережі

Для експлуатації локальної мережі необхідними є наступні види документів:

1. Логічна топологія.
2. Фізична топологія.
3. План приміщення.
4. Таблиця IP-адрес.

В процесі експлуатації мережі з часом буде потреба в приєднанні нових користувачів. Для кожної робочої групи при розробці мережі було впроваджено резервні точки підключення клієнтів.

Моніторинг процесів в мережі є одним із найважливіших аспектів її експлуатації. Моніторинг мережевих процесів буде передбачати:

1. Збір статистики роботи протоколів канального рівня шляхом використання ОС центрального комутатора.

2. Використання діагностичних утиліт ОС сервера та файлів журналів.

3. Статистичні дані роботи мережевого сховища даних.

Програмне забезпечення OpenVPN пише власний журнал подій (openvpn-status.log), який знаходиться в каталозі /var/log. В цьому каталозі знаходяться журнали ОС freeBSD такі як: messages, secure, dmesg.

3.6 Моделювання роботи локальної мережі

Моделювання роботи локальної мережі використовується для того, шоб перевірити правильність проектування та налаштування вузлів мережі. Для моделювання можна використати наступне програмне забезпечення:

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

Для моделювання буде використано програму Packet Tracet 5.3, оскільки вона є безкоштовною. Packet Tracer - емулятор мережі передачі даних, що випускається фірмою Cisco Systems. Вона призначена створювати повнофункціональні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори і комутатори, взаємодіяти між декількома користувачами (через хмару).

Програма емулює популярні серії маршрутизаторів Cisco 1800, 2600, 2800 і комутаторів 2950, 2960, 3650 а також інші моделі. Крім того є сервери DHCP, HTTP, TFTP, FTP, робочі станції, різні модулі до комп'ютерів і маршрутизаторів, пристрої WiFi, різні кабелі. Галущь застосування програми від простих навчальни мереж на кілька (десятків) хостів до складних макетів мереж. Особливість даного ПЗ – здатність перевіряти на працездатність топології. Мета моделювання: перевірити зв’язок між вузлами локальної мережі. Засобами програми можна моделювати роботу проколів: ICMP, TCP, SNMP, SMTP та ін.

За допомогою програми Packet Tracer буде моделюватися робота протоколу ICMP між двома її вузлами, а саме між вузлом PC1 та сервером S1. Спроектована локальна мережа засобами програми Packet Tracer 5.3 наведена на рисунку 3.1.

Сконфігуруємо вузол PC1, згідно даних таблиці IP-адрес:

- IP-адреса: 172.16.11.1, маска: 255.255.255.0;
- Шлюз: 172.16.11.200;
- DNS: 172.16.14.202, 8.8.8.8.

Налаштуємо сервер S1, згідно даних таблиці IP-адрес:

- IP-адреса: 172.16.14.201, маска: 255.255.255.0;
- Шлюз: 172.16.14.200;
- DNS: 172.16.14.202, 8.8.8.8.

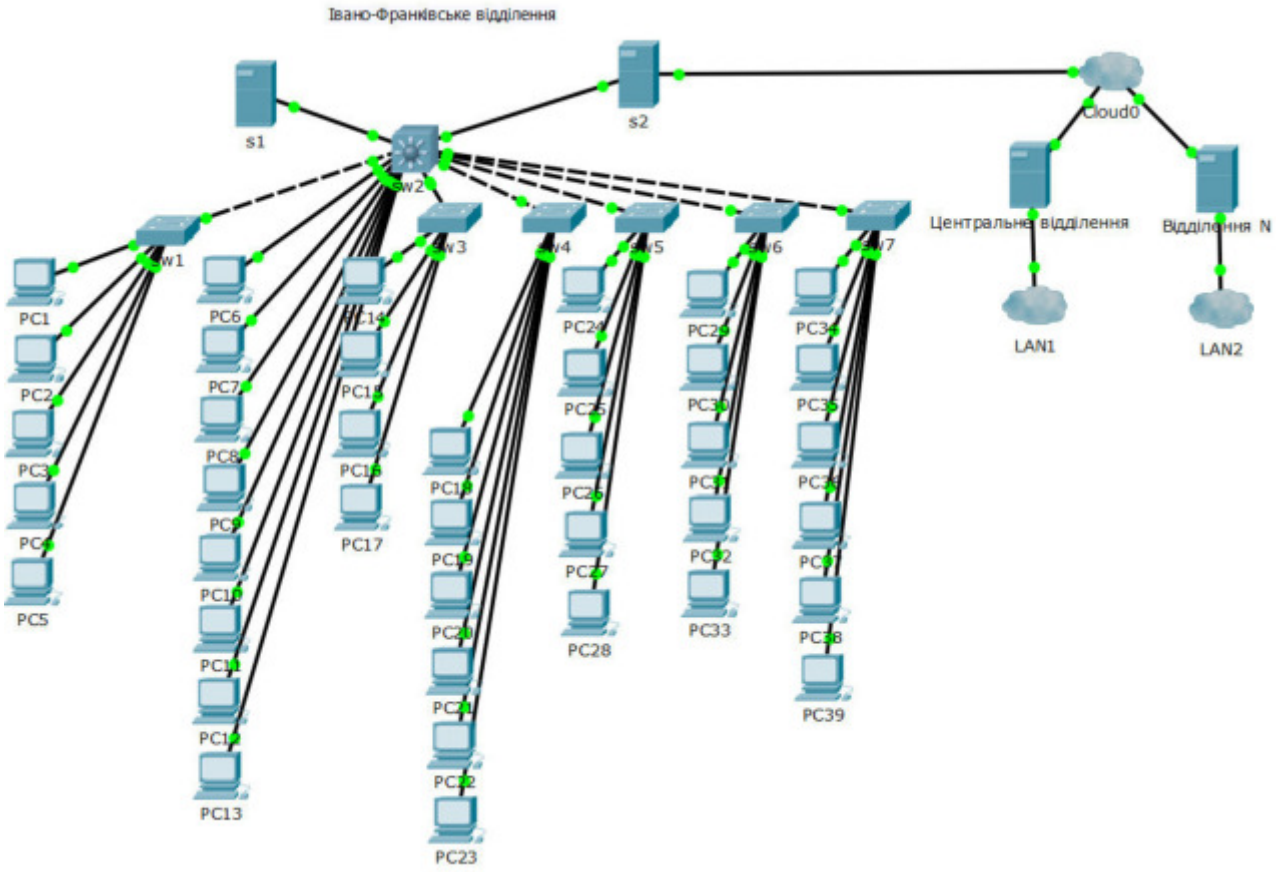

Рисунок 3.1 – Змодельована локальна мережа

Змоделюємо роботу протоколу ICMP шляхом відправки даних між вище описаними вузлами. Результат моделювання:

PC1>

ping 172.16.14.201

Pinging 172.16.14.201 with 32 bytes of data:

Reply from 172.16.14.201: bytes=32 time<1ms TTL=64

Reply from 172.16.14.201: bytes=32 time<1ms TTL=64

Reply from 172.16.14.201: bytes=32 time<1ms TTL=64

Reply from 172.16.14.201: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.14.201:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Вище наведений результат моделювання доводить коректність налаштування параметрів стеку TCP/IP вузлів локальної мережі і правильність прийнятих рішень.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної рооти роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для ІФЦВ «Європромбанк» 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 стадії	Виконавець	Середній час виконання операції, год.
1	Постановка задачі та збір інформації про об'єкт	Керівник проекту	10
2	Розробка проекту	Інженер	10
3	Затвердження проекту	Керівник проекту	2
4	Монтаж мережі	Технік	28
5	Налагодження мережі та створення технічної документації	Інженер	50
Разом			100

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для ІФЦВ «Європромбанк» складає 100 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:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проекту – 70 грн./год., інженер – 65 грн./год., технік – 55 грн./год.

Отже, основна заробітна плата для:

1. Керівник проекту - $З_{осн1} = 12 \cdot 70 = 840$ грн.
2. Інженер - $З_{осн2} = 60 \cdot 65 = 3900$ грн.
3. Технік - $З_{осн3} = 28 \cdot 55 = 1540$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 840 + 3900 + 1540 = 6280{,}00\ грн.$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту - $З_{дод1}$= 840 · 0,15 = 126,00 грн.
2. Інженер - $З_{дод2}$ = 3900 · 0,15 = 585,00 грн.
3. Технік - $З_{дод3}$ = 1540 · 0,15 = 231,00 грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 126,00+585,00+231,00 = 942,00 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

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

$$В_{о.п}=6280,00+942,00 = 7222,00 \text{ грн}$$

Необхідно визначити відрахування на соціальні заходи:

1. Фонд страхування на випадок безробіття – 1,6 %;
2. Фонд по тимчасовій втраті працездатності – 1,4 %;
3. Пенсійний фонд – 33,2 %;
4. 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.

$$В_{с.з.}= 7222,00 \cdot 0,376= 2715,47 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія прац.	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	70	12	840	126,00	-	-
2	Інженер	65	60	3900	585,00	-	-
3	Технік	55	28	1540	231,00	-	-
Разом				6280,00	942,00	7222,00	9937,47

Отже, загальні витрати на оплату праці становлять 9937,47 грн.

4.3 Розрахунок матеріальних витрат

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

$$M_{Bi} = q_i \cdot p_i \qquad (4.5)$$

де q_i – кількість витраченого матеріалу i-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum M_{Bi} \qquad (4.6)$$

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 24U	шт.	1	15800	15800
2	Комутаційна шафа висота 7U	шт.	6	9000	54000
3	Патчпанель, 24 порти, категорія 6	шт.	1	4000	4000
4	Патчпанель Panduit, 16 портів, категорія 6	шт.	6	3100	18600
5	Патчкорд UTP кат. 6	шт.	45	60	2700
6	Короб	м.	123	70	8610
7	Кабль UTP (кат. 6), Одескабель	м.	610	13	7930
8	Мережева розетка UTP (кат. 6)	шт.	41	130	5330
9	APC 1500VA Smart-UPS	шт.	1	16500	16500
10	Комутатор TP-Link T3700G-52TQ	шт.	1	30670	30670
11	D-Link DGS-1100-08	шт.	6	3200	19200
12	Файловий сервер ARTLINE Business R33	шт.	1	38000	38000
13	Сервер-шлюз ARTLINE Business R33	шт.	1	33000	33000
14	D-Link DGS-1100-16	шт.	1	4300	4300
Загальна сума, грн.					258640

Загальна сума матеріальних витрат на розробку мережі становить 258640,00 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 – 1,68 грн.

Тому витрати на електроенергію будуть становити:

$$З_е = 0,5 \cdot 18 \cdot 1,68 = 15,12 \text{ грн.}$$

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:

$$Т_в = 258640,00 \cdot 0,08 = 20691,20 \text{ грн.}$$

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 A – амортизаційні відрахування за звітний період, грн.

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

$Н_А$ – норма амортизації, %;

T – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 18 год., балансова вартість ПК – 25400 грн., тому:

$$A = \frac{25400 \cdot 0{,}05}{150} \cdot 18 = 152{,}40 \text{ грн.}$$

4.7 Обчислення накладних витрат

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

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

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

де, $Н_в$ – накладні витрати.

$$Н_в = 7222{,}00 \cdot 0{,}3 = 2166{,}60 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

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

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	7222,00	2,48
Відрахування на соціальні заходи	2715,47	0,93
Матеріальні витрати	258640,00	88,70
Витрати на електроенергію	15,12	0,01
Транспортні витрати	20691,20	7,10
Амортизаційні відрахування	152,40	0,05
Накладні витрати	2166,60	0,74
Собівартість	291602,79	100,00

Собівартість (C_B) НДР розрахуємо за формулою 4.11:

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

Отже, собівартість дорівнює: $C_в = 291602,79$ *грн.*

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

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

де $C_в$ – собівартість виконання НДР;

$Р_{рен.}$ – рівень рентабельності, 30 %

ПДВ – ставка податку на додану вартість, 20 %.

$$Ц = 291602,79 \cdot (1+0,3) \cdot (1+0,2) = 454900,36 \text{ грн.}$$

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:

$$П = Ц - С_в \qquad (4.13)$$

$$П = 454900,36 – 291602,79 = 163297,56 \text{ грн.}$$

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

$$Е_р = П / С_в, \qquad (4.14)$$

де $П$ – прибуток;

$С_в$ – собівартість.

$$Е_р = 163297,56 / 291602,79 = 0,56$$

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

$$Т_р = 1 / Е_р \qquad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку $T_р$=1/0,56=1,79.

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.	291602,79 грн.
2.	Плановий прибуток, грн.	163297,56 грн.
3.	Ціна, грн.	454900,36 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,79

Загальна вартість розробленої комп'ютерної мережі для ІФЦВ «Європромбанк» становить 454900,36 грн.

Зважаючи на високі показники економічної ефективності - 0,56, кошти, вкладені в проведення проектних робіт окупляться за 1,79 року.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

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 [2].

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 [2].

5.1 Організація пожежної безпеки на підприємстві

Протипожежна безпека на підприємстві в Україні – невіддільна частина організації робочого простору і процесів згідно з нормами чинного законодавства [2].

Зокрема, цю сферу регламентують Правила пожежної безпеки в Україні, затверджені наказом Міністерства внутрішніх справ України, зі змінами, які періодично вносяться відповідними наказами [2].

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.

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:

- 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 [3].

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, ДНАОП 0.00-1.31-99 та іншими нормативними документами [2].

Будівлі і ті 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.

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.

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).

Переносні вогнегасники містять у собі обмежену кількість вогнегасної речовини, безперервна подача якої відбувається протягом невеликого проміжку часу, внаслідок чого помилки, допущені під час їх використання, виправити неможливо. Тому слід досконало знати правила роботи з вогнегасниками.

Із закачаними порошковими вогнегасниками слід працювати так:

1) спрямувати насадок на осередок пожежі;

2) зірвати пломбу, висмикнути чеку;

3) натиснути на важіль;

4) розпочати гасіння пожежі.

В даному випадку вибрано вогнегасники ВВК-5, які містять 5 кілограм закачаного порошку (див. рис. 5.1).

Рисунок 5.1 – Вогнегасник ВВК-5

Даний тип вогнегасників призначений для гасіння загорянь різних речовин, горіння яких не може відбуватися без доступу повітря, загоряння електроустановок, що знаходяться під напругою не більше 10кВ. Так само даний вогнегасник отримав широке поширення в офісних приміщеннях за наявності оргтехніки, а також в житловому секторі.

5.2 Розрахунок системи освітлення з світлодіодними лампами для приміщення відділу

ПК встановлено у приміщеннях першого та другого поверху будівлі. Для розрахунку освітлення робочих місць вибрано приміщення відділу роботи з юридичними особами, оскільки воно займає найбільше площу.

Розрахунок виконаємо згідно методики [5].

Розміри приміщення відділу:

- довжина a =8,4 м,
- ширина b = 6 м,
- висота H = 2,7 м (до підвісної стелі).

Коефіцієнт відбиття ρстелі=70%, ρстін=50%. Висота робочих поверхонь столів h = 0,7 м.

Світильники монтуються в підвісну стелю, тому відстань від світильників до підлоги рівна 2,7м. Нормована освітленість для даного класу робіт виберемо $E_р$ = 300 лк (рекомендовані межі 200 – 500 лк).

Висота підвісу світильника над робочою поверхнею визначається за формулою:

$$h = h_o - h_p \qquad (5.1)$$

$$h = 2,7–0,7=2\ (м)$$

Схему визначення висоти підвісу світильника зображено на рисунку 5.2

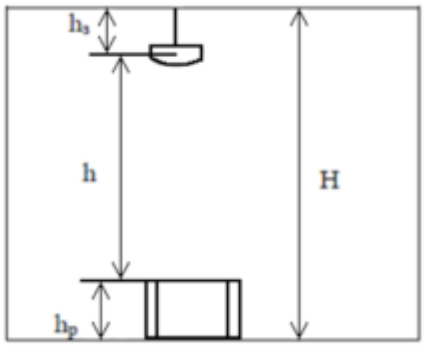

Рисунок 5.2 - Схема визначення висоти підвісу світильника

Рівномірність освітлення досягається при відповідному співвідношенні відстані між світильниками і висоти їх підвісу *h*. Визначимо рекомендовану відстань між світильниками:

$$L = 0,8h \qquad (5.2)$$

$$L = 0,8 \cdot 2=1,6\ (м),$$

Оскільки, світильники розміщуються в ніші підвісної стелі, то відстань між світильниками становитиме 1,8 (кратно до розмірів елементів підвісної стелі).

Розрахункова необхідна кількість світильників становить:

$$N = \frac{ab}{L^2} \qquad (5.3)$$

$$N = \frac{8,4 \cdot 6}{1,8^2} = 15,5шт.$$

Враховуючи розміри приміщення, розміри світильників та відстані між ними попередньо приймаємо 16 світильників, рівномірно розташовуємо їх у 4 ряди по 4 штук, як зображено на рисунку 5.3.

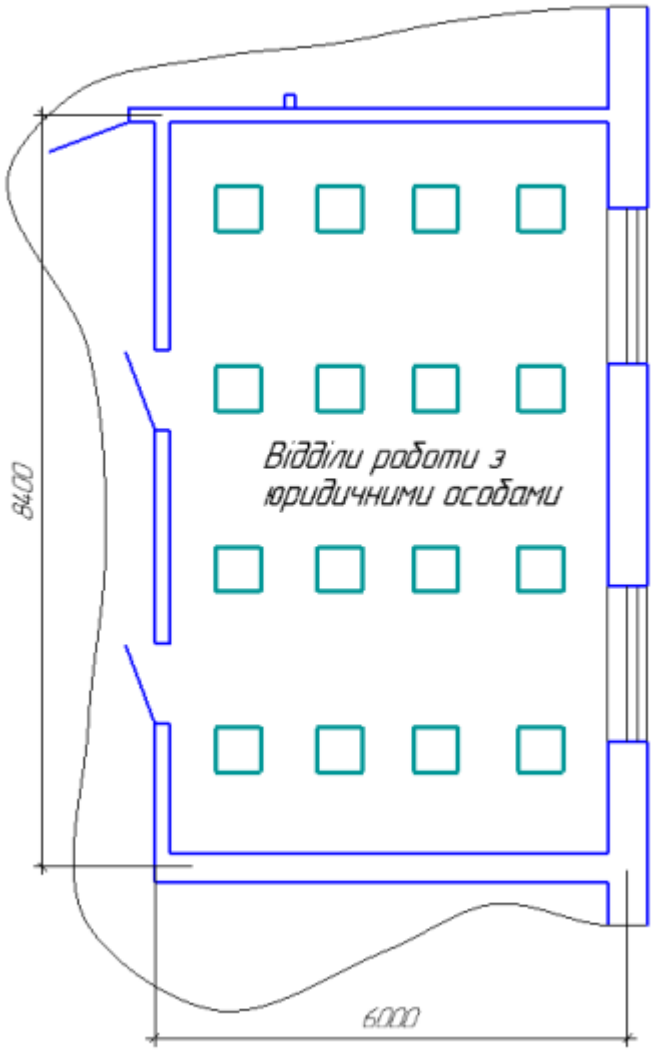

Рисунок 5.3 - Схема розташування світильників

Показник приміщення *i* становить:

$$i = \frac{ab}{h(a+b)} \tag{5.4}$$

$$i = \frac{8{,}4 \cdot 6}{2{,}7 \cdot (8{,}4+6)} = 1{,}29$$

Знаходимо коефіцієнт використання η = 0,47 для світильника при i = 1,25, $\rho_{СТЕЛІ}$ =70%, $\rho_{СТІН}$ =50%; $К_З$ – коефіцієнт запасу $К_З$=1,15; Z – коефіцієнт використання світлового потоку рівний 1,1.

Необхідний світловий потік одного світильника, а визначається за формулою:

$$\Phi_л = \frac{ESK_З Z}{N\eta} \qquad (5.5)$$

$$\Phi_л = \frac{300 \cdot 50{,}4 \cdot 1{,}15 \cdot 1{,}1}{16 \cdot 0{,}47} = 2543\ лм$$

З метою економії електроенергії а також забезпечення хорошого терміну служби світильників вибір буде проводитися серед світлодіодних світильників для монтажу в підвісну стелю.

Врахувавши всі критерії та відповідність ціни-якість вибрано Led панель 600x600 MAXUS assistance 36W 4000K (100 lm/w) (див. рисунок 5.4.)

Рисунок 5.4 - LED панель 600x600 MAXUS

Вона має такі характеристики:

- Світловий потік, Lm – 3600;
- Номінальна потужність, Вт – 36;
- Температурний режим експлуатації, С: 0 … +40;
- Термін гарантії, міс - 36;

- Індекс кольоропередачі (Ra) >83;
- Клас енергоспоживання: A+;
- Діапазон робочої напруги В: 175-265;
- Матеріал корпусу – Алюміній;
- Ступінь захисту від вологи - IP20;
- Форм-фактор – Panel;
- Колір корпусу - білий.

ВИСНОВКИ

Для проекту локальної мережі розроблено локальну мережу ІФЦВ «Європромбанк».

Проект мережі включає побудову мережі центрального відділення та розподілену локальну мережі, яка об’єднує в собі територіально віддалені філії.

Розроблено інструкції з налаштування вузлів локальної мережі:

- Сервер доступу до мережі Інтернет;
- Файловий сервер;
- Центральний комутатор;
- Комутатор робочих груп.

Описано процедуру налаштування серверів територіально віддалених мереж для роботи через VPN.

Для локальної мережі впроваджено файловий сервер для надійного зберігання даних працівників. Проект мережі передбачає використання альтернативного програмного забезпечення.

В економічному розділі зроблено розрахунок собівартості робіт по розробці, встановленні та налаштуванні мережі для ІФЦВ «Європромбанк».

В розділі охорона праці описано техніку безпеки при роботі з обчислювальною технікою, зроблено розрахунок системи штучного заземлення комп’ютерної мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Бірюков М.Л., Стеклов В.К., Костік Б.Я. Транспортні мережі телекомунікацій: системи мультиплексування: навч. посіб. Київ: Техніка, 2009. 312 с.

2. Жидецький В.Ц. Охорона праці користувачів комп'ютерів: навч. посіб. 2-ге вид., доп. Львів: Афіша, 2000. 176с.

3. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп'ютерних систем та мереж. Київ: НАУ. 2007. 361с.

4. Методичні вказівки до виконання кваліфікаційної роботи за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ» 2021. 54с.

5. Москальова В.М. Основи охорони праці: навч. підр. Київ: Професіонал. 2005. 672с.

6. Погорілий С.Д.. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: навч. підр. Київ: ВПЦ "Київський університет. 2018. 138с.

7. Ткаченко В. Комп'ютерні мережі та телекомунікації: навч. посіб. Харків: НТУ "ХПІ". 2011. 224 с.

8. Царьов Р. Ю. Структуровані кабельні системи : навч. посіб. Одеса: ОНАЗ ім. О.С. Поповаю 2013. 260 с.

9. Черкун О.М. Сучасні технології комп'ютерної безпеки. Монографія. Книга 7. Рівне: МЕГУ. 2012. 90с.

10. Швиденко М.З., Матус Ю.В.. Комп'ютерні мережні технології: Навч.-метод. посібн. Київ: ТОВ "Авета". 2016. 264с.

11. APC 1500 VA/ URL: https://www.apc.com/shop/ua/products/APC-Smart-UPS-1500-USB-230-/P-SUA1500I?isCurrentSite=false (дата звернення: 2.06.2023)

12. Cisco Packet Tracer. URL: https://wikipedia.org/wiki/Cisco_Packet_Tracer. (дата звернення: 04.06.2023).

13. D-Link DGS-1110. URL:: http://www.dlink.com/ua/products/1/816.html. (дата звернення: 1.06.2023).

14. FreeBSD: установка і настройка OpenVPN клієнта. URL: https://rtfm.co.ua/freebsd-ustanovka-i-nastrojka-openvpn-klienta/ (дата звернення: 3.06.2023).

15. T3700G-52TQ. URL:: https://www.tp-link.com/uф/products/details/cat-39_T3700G-52TQ.html. (дата звернення: 1.06.2023)

16. 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: 3.06.2023).

17. Настройка ipfw. URL: http://system-administrators.info/?p=1287 (дата звернення: 4.06.2023).

18. Настройка vsftpd. URL: http://ashep.org/2011/nastrojka-vsftpd/#.YLklt6j7TGg. (дата звернення: 3.06.2023).

19. 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: 20.05.2023).

20. Патч панель Panduit URL: https://svit-server.com.ua/patch-paneli/ (дата звернення: 1.06.2023)

21. Сервер ArtLine Business R33 URL: https://artline.ua/uk/product/server-artline-business-r33v08 (дата звернення: 2.06.2023)

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	Відділ роботи з юридичними особами	11	172.16.11.1/24	172.16.11.200
2	WS_2	Відділ роботи з юридичними особами	12	172.16.12.1/24	172.16.12.200
3	WS_3			172.16.12.2/24	
4	SW_1		1	192.168.1.1/24	-
5	WS_4	Відділ роботи з валютою	13	172.16.13.1/24	172.16.13.200
6	WS_5			172.16.13.2/24	
7	WS_6	Серверна	14	172.16.14.1/24	172.16.14.200
8	S_1			172.16.14.201/24	
9	S_2			172.16.14.202/24	
			-	93.44.65.2	93.44.65.253
10	SW_2		1	192.168.1.2/24	-
11	WS_7	Секретар	15	172.16.15.1/24	172.16.15.200
12	WS_8	Директор	16	172.16.16.1/24	172.16.16.200
13	WS_9	Відділ роботи з цінними паперами	17	172.16.17.1/24	172.16.17.200
14	WS_10			172.16.17.2/24	
15	WS_11			172.16.17.3/24	
16	WS_12			172.16.17.4/24	
17	WS_13			172.16.17.5/24	
18	WS_14	Відділ страхування	18	172.16.18.1/24	172.16.18.200
19	WS_15			172.16.18.2/24	
20	WS_16			172.16.18.3/24	

Продовження таблиці А1

1	2	3	4	5	6
21	WS_17			172.16.18.4/24	
22	SW_3		1	192.168.1.3/24	-
23	WS_18	Кредитний відділ	19	172.16.19.1/24	172.16.19.200
24	WS_19			172.16.19.2/24	
25	WS_20			172.16.19.3/24	
26	WS_21			172.16.19.4/24	
27	SW_4		1	192.168.1.4/24	
28	WS_22	Депозитний відділ	20	172.16.20.1/24	172.16.20.200
29	WS_23			172.16.20.2/24	
30	WS_24	Розрахункова група	21	172.16.21.1/24	172.16.21.200
31	WS_25			172.16.21.2/24	
32	WS_26			172.16.21.3/24	
33	WS_27			172.16.21.4/24	
34	WS_28			172.16.21.5/24	
35	SW_5		1	192.168.1.5/24	-
36	WS_29	Каси	22	172.16.22./24	172.16.22.200
37	WS_30			172.16.22./24	
38	WS_31			172.16.22./24	
39	WS_32			172.16.22./24	
40	WS_33			172.16.22./24	
41	SW_6		1	192.168.1.6/24	-
42	WS_34	Центр обслуговування клієнтів	23	172.16.23.1/24	172.16.23.200
43	WS_35			172.16.23.2/24	
44	WS_36			172.16.23.3/24	
45	WS_37			172.16.23.4/24	
46	WS_38			172.16.23.5/24	
47	SW_7		1	192.168.1.7/24	-
48	WS_39	-	24	172.16.24.1/24	172.16.24.200
49	RJ_1			172.16.24.2/24	
50	RJ_2			172.16.24.3/24	

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	-	1	-	Відділ роботи з юридичними особами	-	11	172.16.11.0/24
WS_2-WS_3, SW_1	-	3	-	Відділ роботи з юридичними особами	-	12	172.16.12.0/24
WS_4-WS_5	-	2	-	Відділ роботи з валютою	-	13	172.16.13.0/24
WS_6, S_1, S_2, SW_2	-	4	-	Серверна	-	14	172.16.14.0/24
WS_7	-	1	-	Секретар	-	15	172.16.15.0/24
WS_8	-	1	-	Директор	-	16	172.16.16.0/24
WS_9-WS_13	-	5	-	Відділ роботи з цінними паперами	-	17	172.16.17.0/24
WS_14-WS_17	-	4	-	Відділ страхування	-	18	172.16.18.0/24
WS_18-WS_21, SW_4	-	5	-	Кредитний відділ	-	19	172.16.19.0/24
WS_22-WS_23	-	2	-	Депозитний відділ	-	20	172.16.20.0/24
WS_24-WS_28, SW_5	-	5	-	Розрахункова група	-	21	172.16.21.0/24
WS_29-WS_33, SW_6	-	6	-	Каси	-	22	172.16.22.0/24
WS_34-WS_38, SW_7	-	6	-	Відділ обсл. клієнтів	-	23	172.16.23.0/24
WS_39, RJ_1, RJ_2	-	3	-	-	-	24	172.16.24.0/24

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	Eth0	-	SW_1	1	Access	11
2	WS_2-WS_3	Eth0	-	SW_1	2-3	Access	12
3	WS_4-WS_5	Eth0	-	SW_1	4-5	Access	13
4	WS_6, S_1, S_2	Eth0	-	SW_2	1-3	Access	14
5	WS_7	Eth0	-	SW_2	4	Access	15
6	WS_8	Eth0	-	SW_2	5	Access	16
7	WS_9-WS_13	Eth0	-	SW_2	6-11	Access	17
8	WS_14-WS_17	Eth0	-	SW_3	1-4	Access	18
9	WS_18-WS_21	Eth0	-	SW_4	1-4	Access	19
10	WS_22-WS_23	Eth0	-	SW_4	5-6	Access	20
11	WS_24-WS_28	Eth0	-	SW_5	1-5	Access	21
12	WS_29-WS_33	Eth0	-	SW_6	1-5	Access	22
13	WS_34-WS_38, SW_7	Eth0	-	SW_7	1-5	Access	23
14	WS_39, RJ_1, RJ_2	Eth0	-	SW_7	6-8	Access	24
15	SW_1	6	Trunk	SW_2	12	Trunk	-
16	SW_3	5	Trunk	SW_2	13	Trunk	-
17	SW_4	7	Trunk	SW_2	14	Trunk	-
18	SW_5	6	Trunk	SW_2	15	Trunk	-
19	SW_6	6	Trunk	SW_2	16	Trunk	-
20	SW_7	9	Trunk	SW_2	17	Trunk	-

Додаток В. Характеристики обладнання

Таблиця В1 - Порівняльна характеристика апаратних платформ серверів

	ARTLINE Business R33	ProServer DL360p
Процесор	Intel Xeon E-2224G	Intel Xeon E-2136
Об’єм ОЗП	16ГБ	16ГБ
Тип ОЗП	DDR4-2666 МГц (4 слоти, макс. обсяг пам'яті 64 ГБ)	2666/2400/2133 МГц ECC DDR4 SDRAM
Дискова підсистема	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ
Мережева плата	інтегрована	інтегрована
Блок живлення	650 Вт	650Вт

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
К-сть портів 10/100/1000	16 + 2SFP	16 + 2 SFP
Підтримка базових протоколів канального рівня (VLAN, Port Mirroring, Spanning Tree, IGMP, QoS)	Так	Так

Таблиця В3 - Порівняльний аналіз центральних комутаторів

Модель /Параметри	TP-Link T3700G-52TQ	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	48	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	+	+	+