Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра
(бакалавра, спеціаліста, магістра)

студента Сидоренко Олексія Романовича
(ПІБ)
академічної групи 123-17ск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему «Комп'ютерна система з блокчейн технологією підтримки реєстру студентів НТУ «Дніпровська політехніка» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	ас. Панферова Я.В.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розрахунок мережі	ас. Панферова Я.В.			
економічний розділ	ст. викл. Яремчук І.О.			
охорона праці	доц. Іконніков М.Ю.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри

__інформаційних систем_
_____та технологій__ ____
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

«_27__»_січня____2020 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Сидоренко О.Р. **академічної групи** 123-17ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)

на тему « Комп'ютерна система з блокчейн технологією підтримки реєстру студентів НТУ «Дніпровська політехніка» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від №

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи	10.05.2020
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи	17.05.2020
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи з опрацюванням побудови і захисту інформації та налаштуванням корпоративної мережі	24.05.2020
Економічна частина	Економічно обґрунтувати доцільність витрат на створення та дослідження системи керування	30.06.2020
Охорона праці	Розробити організаційно-технічні заходи, щодо реалізації правил безпеки при експлуатації системи	1.06.2020

Завдання видано _____ _Панферова Я.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі _27 січня_ 2020 р._

Дата подання до екзаменаційної комісії 10.06.2020 р.

Прийнято до виконання _____ Сидоренко О.Р.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 81 с., 9 рис., 5 табл., 5додатків, 6 джерел.

Об’єкт розробки: мережа с блокчейн технологією для Національного технічного університету «Дніпровська Політехніка»

Мета: вдосконалення системи та зменьшення затрат на працю.

Розробка комп’ютерної системи з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову систем роботи з програмою Cisco Packet Tracer, а також для з иження початкових витрат на розгортання системи та при її модернізації.

Система виконана відкритою і дозволяє здійснювати технічну і програмну модернізацію системи, а так само забезпечує виконання наступних функцій:

– Доступ до даних з будь якої точки світу де є доступ до інтернету;

– Збільшення надійності зберігання інформації;

– Зменшення витрат на єлектроенергію та оренду пріміщень.

Розробка комп’ютерної мережі виконана відповідно до завдання на дипломну роботу бакалавра.

Розроблена схема мережі реалізована за допомогою додаткової літератури. Робота протестована за допомогою програми Cisco Packet Tracer.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці

УМОВНІ ПОЗНАЧЕННЯ

ACL – (Access Control List) - список контролю доступу

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

DNS – (Domain Name System) система доменних імен

FTP – (File Transfer Protocol) - протокол передачі файлів

HD – (High Definition) - висока чіткість

HFC – (Hybrid fibre-coaxial) - гібридна коаксіально-оптична мережа

ICMP – (Internet Control Message Protocol) - міжмережевий протокол керуючих повідомлень

IEEE – (Institute of Electrical and Electronics Engineers) - інститут інженерів з електротехніки та електроніки

IP – (Internet Protocol) - міжмережевий протокол

LAN – (Local Area Network) - локальна обчислювальна мережа

VLSM (Variable Length Subnet Mask - маска підмережі змінної довжини

NAT (Network Address Translation) - трансляція мережевих адрес

КОМУТАТОР - пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі

МАРШРУТИЗАТОР- пристрій, що використовується для поєднання двох або більше мереж

ЗМІСТ

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика та аналіз діяльності

Проектування мережі – це комплексний процес, результатом якого є формування загальної модель майбутньої мережі з повним набором документації до неї. Цей процес можна розділити на два основні етапи:

Підготовчі роботи (збирання та аналіз вимог замовника до мережі, що проектується). Аналіз вимог до мережі допоможе оцінити значущість інформаційно-технологічних рішень, визначити головні цілі і вибрати пріоритети для окремих частин комп'ютерної мережі, яку необхідно спроектувати. Чітке визначення вимог до функцій мережі допоможе уникнути реалізації непотрібних властивостей мережі, що заощадить гроші.

Створення моделі майбутньої мережі. На цьому етапі обирається топологія мережі, визначаються типи кабелів та обладнання і т.п. – формується загальна модель мережі. Здійснюється опрацьовування створеної моделі мережі в різних програмах проектування. Висновки, які формуються на основі отриманих результатів, впливають на рішення застосування створеної моделі в тому або іншому випадку.

На кожному етапі проводиться детальне документування. В результаті цього формується пакет документації за проектом мережі, який описує всі аспекти спроектованої мережі. У цей пакет, наприклад, можуть входити наступні документи: список устаткування, що використовується у мережі, схема розміщення пристроїв мережі, таблиця кабельних трас, логічна та фізична карти мережі, схема адресації і т.п. Ця документація допоможе не тільки побудувати мережу, але й швидко і легко усунути несправності.

1.2 Проблема неякісного проектування

На сьогоднішній день досить велика кількість організацій пропонують цілковитий спектр послуг щодо комп'ютерних мереж: проектування, монтаж

та підтримка. В основному це організації з великим досвідом роботи і гарними рекомендаціями, з цими організаціями проблеми неякісного проектування не виникає.

Ця проблема дуже актуальна для невеликих організацій, які сьогодні надають послуги з підключення користувачів до комп'ютерної мережі (більшою мірою – до локальної мережі, яка у свою чергу має вихід в глобальну мережу Internet). В більшості випадків для підключення до мережі використовується кабельне з'єднання – кабель UTP 5-ї категорії та мережевий адаптер Fast Ethernet для роботи на швидкостях 10/100 Мб/с.

Розглянемо загальний процес впровадження мережі, яка була спроектована силами самої організації або за допомогою спеціалістів даного напрямку. За проектом мережі купується різне мережеве устаткування (маршрутизатори, комутатори, концентратори, сервери) та кабелі. Далі проводяться роботи по установці обладнання і прокладці| основних кабельних магістралей. В останню чергу організація через засоби ЗМІ оповіщають про послуги, що надаються.

На ранніх етапах масового підключення користувачі задоволені якістю послуг, що надаються. Підчас збільшення комп'ютерів в мережі реальне навантаження наближається до спроектованого. Коли кількість хостів в мережі наближається до критичної (максимальному допустимому в проекті мережі), жорстко відчуваються нестача смуги пропускання для передачі або прийому даних, часові затримки при роботі і т.п.

У певний момент (якщо підключення хостів ще продовжується) мережа стає непрацездатною або розпадається на частини. Оскільки в основному використовуються різні варіанти зіркоподібної топології, мережа розпадається на декілька комутованих мереж, які не можуть взаємодіяти одна з одною.

Виникає велика, а в деяких випадках нездійсненна, проблема перегляду проекту мережі, яка спричинить великі фінансові втрати (основна стаття витрат – обладнання мережі)

2 ФОРМУЛЮВАННЯ ТЕХНІЧНИХ ВИМОГ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до мережі

Сьогодні обслуговування клієнтів на базі Інтернет - технологій нерідко має проводитися в режимі 24 години на добу. Це означає, що тимчасова доступність комерційних мереж повинна бути практично стовідсотковою. При цьому вони повинні передбачати автоматичний захист від непередбачених погроз безпеки мережі. Крім того, комерційні мережі повинні адаптуватися до змін навантаження трафіку, щоб час відгуку додатків залишався постійним.

Основна мета дипломної роботи - для університету « Дніпровська Політехніка» розробити проект електронної обчислювальної мережі на основі Cisco та blockchain, та впровадити заходи, для подальшого повноцінного функціонування, підтримки цієї мережі, та її розширення.

Для рішення поставленої мети в дипломній роботі вирішуються наступні завдання:

– вибір мережевої архітектури;

– вибір топології, типу кабельної системи;

– вибір способу керування мережею;

– конфігурація мережевого встаткування ;

– керування мережевими ресурсами й користувачами мережі;

– розгляд питань безпеки мережі;

– підключення блокчейну;

– подальше обслуговування мережі.

2.2 Вимоги до мережевого обладнання

2.2.1 Вимоги до активного встаткування ЛОМ

До складу активного встаткування ЛОМ повинні входити комутатори з підтримкою технологій віртуальних мереж і мережевого керування, а також маршрутизатор з технологією міжмережевого екрана (firewall).

2.2.2 Вимоги до системи керування ЛОМ

Система керування ЛОМ повинна забезпечити керування всіма інформаційними ресурсами ЛОМ, у тому числі й ЛОМ першої черги.

Система керування ЛОМ повинна здійснювати:

– інвентаризацію - одержання інформації про стан апаратних і програмних засобів, що входять у мережу;

– збір статистики й моніторинг основних параметрів продуктивності мережі: швидкості передачі пакетів, навантаження, рівня помилок і ін.;

– можливість настроювання параметрів мережі;

– виготовлювачем системи керування ЛОМ повинна бути компанія Microsoft.

2.2.3 Вимоги до серверів

Для керування корпоративною базою даних, центрального файлового сервера, файлового сервера робочих груп, сервера бухгалтерії, сервера електронної пошти, web-сервера й сервера резервного копіювання повинні бути використані комп'ютери з характеристиками не нижче, ніж наступні:

– не менш 2-х процесорів з параметрами не нижче Intel Xeon 2.4 ГГц, с обсягом L2-cache не менш 12 MB);

– оперативна пам'ять не менш 32 GB;

– обсяг дискового простору не менш 1000 GB;

– Windows Server 2015 і вище;

– мережна карта 1000Base-TX;

– сервери повинен бути встановлений у серверній.

2.2.4 Вимоги до надійності

Устаткування в складі локальної обчислювальної мережі повинно забезпечувати сталість фізичних характеристик каналу між портом активного обладнання і абонементські обладнанням незалежно від траси комутації на панелях перемикання розподільних вузлів. Постійність фізичних параметрів каналу має забезпечуватися при наступних перекроссіровках незалежно від їх числа (але не більше визначеного виробником обладнання локальної обчислювальної мережі).Розрив будь-якого каналу локальної обчислювальної мережі можливий тільки при комутації на панелях перемикання розподільних вузлів.

У разі виходу з ладу будь-якого з каналів повинна забезпечуватися можливість переходу на використання альтернативного каналу з числа резервних за допомогою зміни з'єднань на панелях перемикання розподільних вузлів. Обладнання повинно функціонувати 24 години на добу, 7 днів на тиждень, без урахування часу, необхідного для проведення регламентних робіт відповідно до рекомендацій виробника.

2.2.5 Вимоги до робочих станцій

До складу ЛОМ повинні входити робочі станції наступного функціонального призначення:

– робочі станції для керівництва;

– робочі станції для працівників бухгалтерії;

– комп’ютер адміністратора;

– інші робочі станції

Перечень критеріїв до мережевого устаткування представлений у таб. 1.

Таблиця 1 - *Комплектація робочих станцій мережі*

Тип комп'ютера	Комп'ютер адміністратора	Комп'ютер керівництва	Інші робочі станції
Операційна система	Windows 10	Windows 10	Windows 10
Процесор	Core™ i5 9400F	Core™ i5 9400F	Core™ i3-9100F
Системна плата	H310 mATX	H310 mATX	Intel H310
Плата відеопам'яті	nVidia GeForce GTX 1050	nVidia GeForce GTX 1050	nVidia GeForce GTX 1050
Жорсткий диск	1000 GB WD	1000 GB WD	240 GB WD
ОЗП	16 GB	16 GB	16 GB
CD	Asus DVD±R/RW	Asus DVD±R/RW	
Монітор	Dell P2418D	Dell SE2416H	Dell E2218HN
NIC - плата	GIGABIT LAN інтегрована	GIGABIT LAN інтегрована	GIGABIT LAN інтегрована

3 СПЕЦІАЛЬНА ЧАСТИНА

3.1 Трирівнева модель мережі

Трирівнева модель мережі являє собою ієрархічну структуру передачі даних не в термінах протоколів або моделей (типу моделі OSI або TCP / IP), а в термінах функціонування абстрактних елементів мережі. Зовнішній вид моделі представлено на Рис.1.

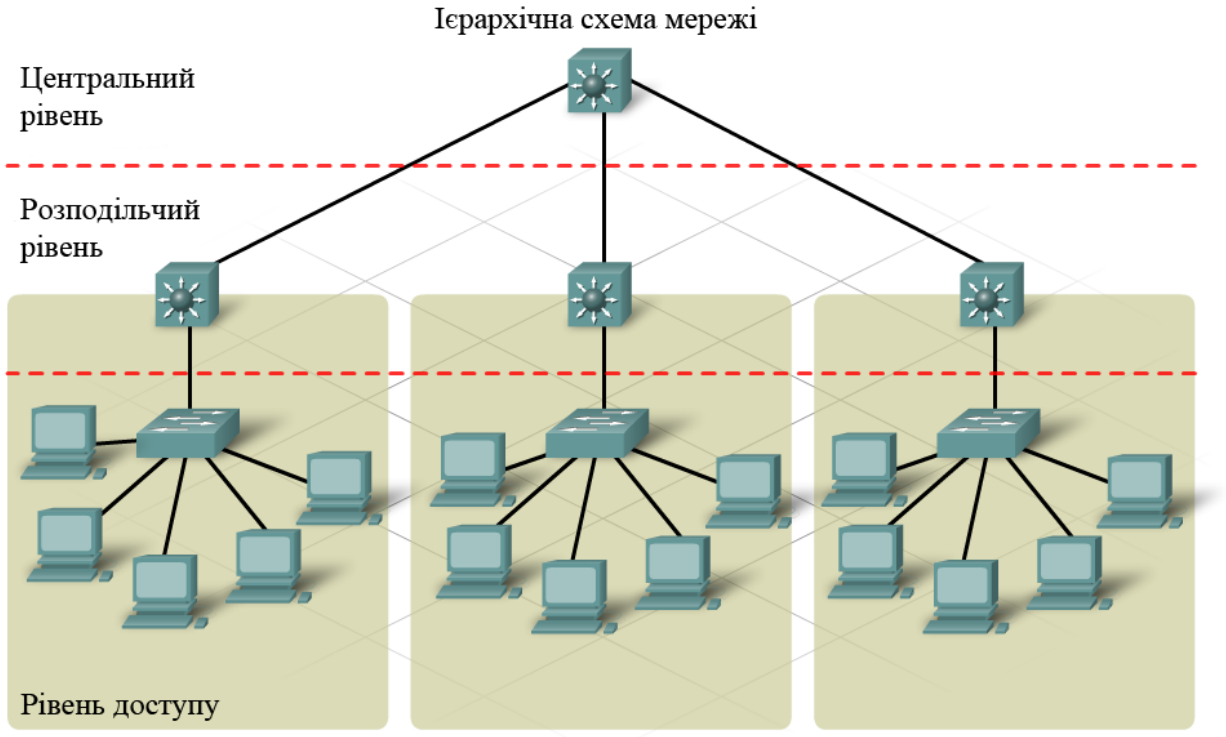


Рисунок 1 - Ієрархічна трирівнева схема мережі

Всі елементи мережі можемо розділити на три так званих рівня. Цей поділ дозволяє створити працездатні, надійні, масштабовані мережі передачі даних. Роль для рівнів швидше логічна, тому не обов'язково існує фізична прив'язка до конкретного устаткування.

3.2 Центральний рівень (Core Layer)

3.2.1 Цілі центрального рівня

Проектування центрального рівня передбачає ефективну високошвидкісну передачу даних між ділянками мережі. Основними цілями проектування на центральному рівні є:

- забезпечення 100% часу роботи;
- доведення до максимуму пропускної здатності;
- спрощення розширення мережі.

3.2.2 Рівень розподілу (Distribution Layer)

Являє собою «з'єднання» між рівнем доступу і рівнем ядра (центральним рівнем). Саме на цьому рівні здійснюється контроль над мережевою передачею даних. Також можна створювати широкомовні домени, створювати VLAN'и, якщо необхідно, а так само впроваджувати різні політики (безпеки та управління). На рівні розподілу може здійснюватися правило звернення до рівня ядра. Наведу деякі особливості і рекомендації при проектуванні рівня розподілу, які виділяють провідні виробники мережевого устаткування.

– QoS. Маршрутизатори або комутатори 3 рівня можуть пріоритетно перенаправляти пакети за встановленим набору правил.

– Пакетна фільтрація (firewalling). Регулювання передачі пакетів та їх передача на основі вилучення інформації про те звідки він і куди повинен бути направлений. Тим самим створюються міжмережевий кордон.

– Маршрутизація між мережами VLAN і інші функції підтримки робочих груп.

– Рівень розподілу дозволяє створювати правила "шлюзірования" від і до різних мереж з різними топологіями.

3.2.3 Рівень доступу (Access Layer)

Самий нижній рівень трирівневої моделі. Рівень доступу містить пристрої, які дозволяють робочим групам і користувачам працювати з сервісами наданими рівнем ядра і рівнем розподілу. На рівні доступу можна організовувати домени колізій, використовуючи концентратори, ретранслятори або комутатори. Відносно рівня доступу можна не застосовувати потужне обладнання, яке застосовуються на рівнях вище.

3.2.4 Обмін інформацією у трирівневій моделі

У мережі Ethernet кожен вузол може безпосередньо з'єднуватися з мережевим пристроєм рівня доступу за допомогою двоточкового кабелю. Такі кабелі проводяться відповідно до конкретних стандартів Ethernet. Кожен кабель вставляється в роз'єм мережевого адаптера вузла і в порт мережевого пристрою. Для підключення вузлів на рівні доступу (включаючи концентратори і комутатори Ethernet) використовується декілька типів мережевих пристроїв.

Комутатор Ethernet використовується на рівні доступу. Як і концентратор, комутатор сполучає декілька вузлів з мережею. На відміну від концентратора, комутатор в змозі передати повідомлення конкретного вузла. Коли вузол відправляє повідомлення іншого вузла через комутатор, той приймає і декодує кадри і прочитує фізичну (MAC) адресу

У міру розширення часто доводиться ділити одну локальну мережу на декілька мереж рівня доступу. Це можна зробити по-різному, на основі різних критеріїв, зокрема:

- фізичне місцеположення;
- логічна функція;
- вимоги безпеки;
- вимоги додатку.

Мережеві пристрої рівня розподілу покликані зв'язувати не окремі вузли, а мережі. Окремі вузли підключаються до мережі через пристрої рівня

доступу, наприклад, комутатори і концентратори. Пристрої рівня доступу зв'язуються один з одним через пристрої рівня розподілу, наприклад, маршрутизатори.

Маршрутизатор – це мережевий пристрій, що зв'язує локальні мережі. На рівні розподілу вони направляють трафік і виконують інші важливі для ефективної роботи мережі функції. Як і комутатори, маршрутизатори можуть декодувати і читати отримані повідомлення.

На відміну від комутаторів, які декодують тільки кадри з MAC-адресою, маршрутизатори декодують пакети, що знаходяться усередині кадру.

3.3 Локальна мережа(LAN)

У ЛМ всі вузли можуть знаходитися в одній локальній мережі або розподілятися між декількома мережами, зв'язаними на рівні розподілу. Це залежить від бажаного результату. Якщо всі вузли знаходяться в одній мережі, вони можуть обмінюватися даними. Річ у тому, що вони утворюють один широкомовний домен і вузли знаходять один одного з використанням протоколу ARP.

Більшість локальних мереж створена на основі технології Ethernet. У правильно розробленій і сконструйованій мережі вона працює швидко і ефективно. Основна передумова для створення якісної мережі – попереднє планування. Для початку потрібного зібрати інформацію про те, як використовуватиметься нова мережа.

Сучасні локальні мережі будуються на основі топології «зірка» з використанням концентраторів (хабів), комутаторів (світчів) та кабелю UTP чи STP 5ї категорії («вита пара»). Дана технологія (вона носить назву Fast Ethernet) дозволяє проводити обмін інформацією на швидкості вище 100Мбіт/с. Ця величина достатня для того, щоб задовольнити більшість потреб користувачів мережі.

Ще один приклад – це інтегрований маршрутизатор Cisco, або ISR. У сімейство Cisco ISR входять найрізноманітніші товари, призначені як для невеликих офісних і домашніх мереж, так і для великих мереж. Багато пристроїв ISR сконструйовано за модульним принципом, і кожну функцію виконує окремий компонент (наприклад, вбудований маршрутизатор і комутатор). Відповідно, при необхідності можна додавати, замінювати і оновлювати компоненти.

3.4 Бездротові технології та пристрої (WLAN)

Бездротове мережеве обладнання призначене для передачі по радіоканалах інформації (даних, телефонії, відео та ін.) між комп'ютерами,

Сучасний стан бездротового зв'язку визначається ситуацією зі стандартом IEEE 802.11. Розробкою і вдосконаленням стандарту займається робоча група по бездротовим локальним мережам (Working Group for Wireless Local Area Networks) комітету з стандартизації Інституту Інженерів Електротехніки і Електроніки (Institute of Electrical and Electronic Engineers, IEEE) під головуванням Віка Хейса (Vic Hayes) з компанії Lucent Technologies . У групі близько ста членів з вирішальним і близько п'ятдесяти з дорадчим голосом; вони представляють практично всіх виробників обладнання, а також дослідницькі центри та університети. Чотири рази на рік група збирається на пленарні засідання та приймає рішення щодо вдосконалення стандарту.

3.5 Послідовність дій при проектуванні мережі

Будь-яке проектування, як відомо, являє собою сильно спрощене моделювання дійсності, що ще не настала. Саме тому передбачити всі можливі фактори, урахувати всі потреби, які можуть виникнути в майбутньому, практично неможливо.

Однак загальні підходи до проектування локальних комп'ютерних мереж все-таки можуть бути сформульовані, деякі корисні принципи такого

проектування пропонуються й з успіхом використовуються. Не варто тільки сприймати їх як щось придатне для будь-яких практичних випадків.

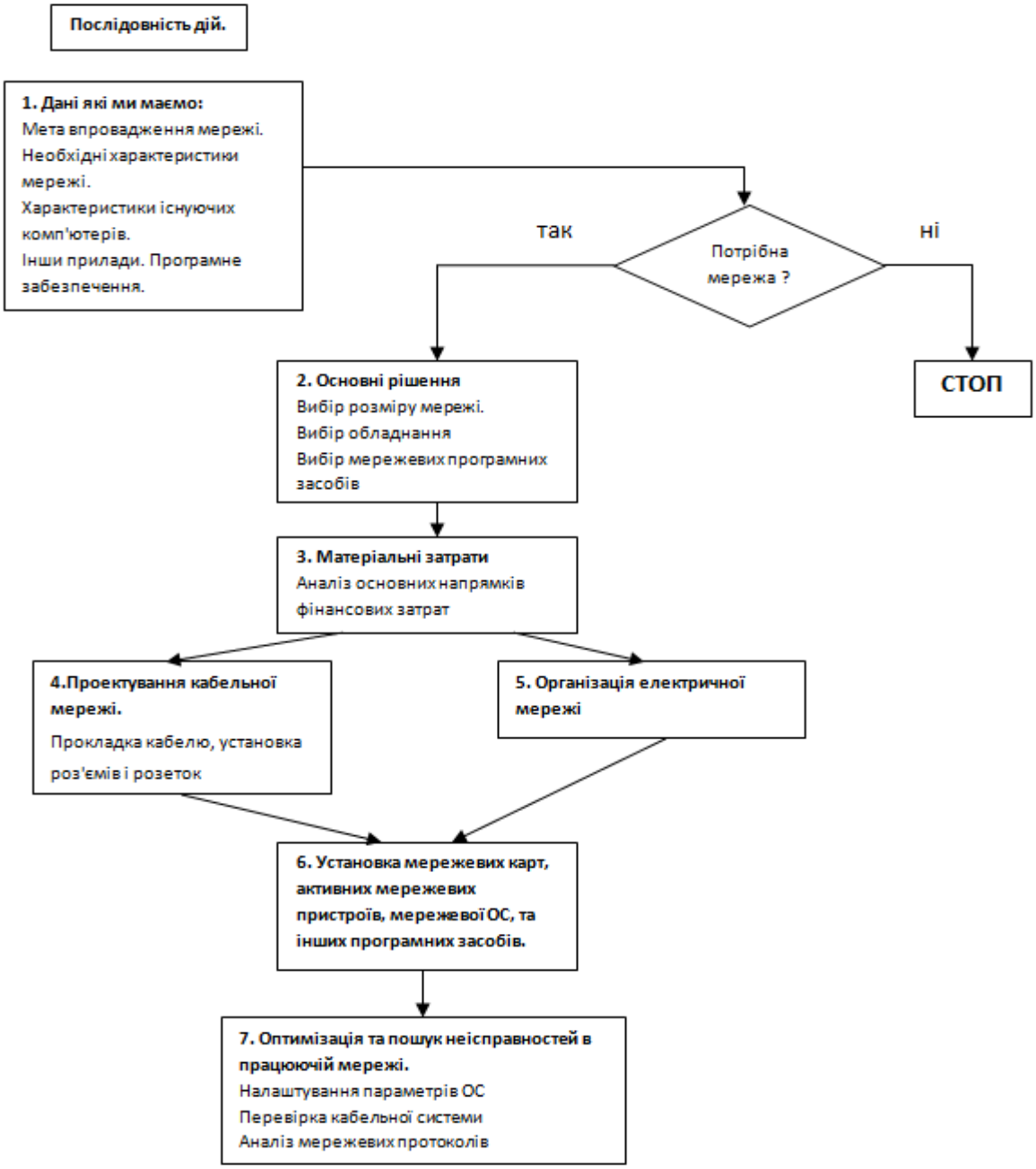


Рисунок 2 - Послідовність етапів іпри проектуванні ЛОМ

3.6 Блокчейн

3.6.1 Технологія блокчейн.

Для початку розглянемо деякі важливі особливості всієї системи:

– Блокчейн буде вести облік всіх типів обміну даними. Це називається системою бухгалтерського обліку(система Леджера)а обмін даними називається «Транзакціями»

– Він використовує різний вигляд розподіленої мережі, щоб переконатися, що кожна транзакція знаходиться в точці між вузлами P2P.

– Після того, як блок буде додано і перевірений ,цю інформацію не можливо буде змінити.

– Переваги маємо за допомоги цієї технологіїї:

– Захист конфіденційності. Забезпечить мережу антимонопльними структурами, а також структурами захисту конфіденційності.

– Блокчейн - це розподілена мережа, яка дозволяє прозоро зберігати дані в незмінному вигляді;

– Блокчейн зберігає інформацію в ланцюжку блоків, де кожен містить інформацію про попередньому;

– Інформація в блокчейне захищається за допомогою математичних алгоритмів.

– Дані, які передаються через мережу ,будуть повністю зашифровані. Крім того, користувачі зможуть вирішити, яку інформацію вони хочуть розділити.

– Буде діяти як міст між різними форматами даних і платформою.

– Розподілені системи менш схильні до переривання обслуговування. Оскільки немає центрального об’єкта для функціонування, стає важким для того, щоб розподілена відмова в обслуговуванні(DDoS) або інші форми збоїв служби.

3.6.2 Країни які використовують технологію блокчейн

Рисунок 3 - Використання блокчейн в Естонії

В Естонії розробили блокчейн-платформу для департаменту охорони здоров'я. На ній зберігається інформація, що стосується візитів до лікарів, рецепти, аналізи, історія хвороб і так далі. Дані зберігаються все життя пацієнта і будуть доступні, навіть якщо людина переїде, поміняє лікарів, а медкарта буде втрачена. Крім того, це може стати в нагоді, наприклад, коли лікаря швидкої допомоги потрібно буде з'ясувати, чи є у хворого алергія на ліки, а терапевта - призначити індивідуальний план лікування. При цьому пацієнт сам вирішує, кому відкрити доступ до своєї інформації

В кінці 2018 року IBM запустила платформу Food Trust, щоб допомогти компаніям боротися з контрафактом і вчасно реалізовувати товар, у якого закінчується термін придатності. Виробники, постачальники та продавці продуктів підключаються до платформи, щоб контролювати походження і терміни поставок і перевіряти сертифікати на продукцію. До платформи вже підключилися такі компанії, як Nestle, Unilever, мережі супермаркетів Walmart і Carrefour. Це обходиться їм в десятки тисяч доларів, але допомагає заощадити сотні тисяч.

Рисунок 4 - Використання технології компанією IBM

3.6.3 Типи блокчейн-мережі

Блокчейн-мережі бувають відкритими і закритими.

- Відкритий тип мережі підходить для системи с багатьма користувачами

- Закритий тип блокчейна з різним рівнем доступу для користувачів, якщо інформація всередині мережі не повинна бути доступна всім бажаючим

- У блокчейні є три ролі учасників: читачі, письменники і майнер;

- У кого буде роль майнера в блокчейне, залежить від алгоритму консенсусу;

- У блокчейні прийнято використовувати хешування, щоб підтверджувати справжність документів.

У блокчейні у кожного є ключі (вони різні і використовуються для різних цілей).

- Є відкритий ключ, який потрібен, щоб вас можна було знайти в мережі

- Є закритий ключ, який потрібен, щоб здійснювати операції

- За допомогою ключів можна створювати і розшифровувати цифрові підписи, щоб підтвердити особу відправника документа

3.6.4 Правила мережі: форк в блокчейне

Коли блокчейн запущений і ви починаєте користуватися ним через комп'ютери та мобільні телефони, може виявитися, що цю послугу можна використовувати і для інших завдань. Для цього треба внести зміни в блокчейн. Є два типи змін - це софтфорк і хардфорк.

Софтфорк - ми можемо зберегти в нових блоках інформацію про старих, а учасники зможуть користуватися тією ж програмою для роботи з блокчейном.

Хардфорк - вихідний блокчейн ділиться на два паралельні проекти: один існує за новими правилами, другий - за старими. Користувачі вибирають між поточною і новою версією ПО і починають працювати в різних мережах.

3.6.5 Майбутнє технології блокчейн

Блокчейн - це молода технологія, яка продовжує розвиватися і адаптуватися під мінливий світ: може бути, блокчейн знайде своє застосування зовсім не там, де ми думаємо.

Блокчейн може зробити багато процесів швидше, простіше і дешевше. Ось лише кілька сфер, де можна очікувати масштабне впровадження цієї технології в найближчі роки.

3.6.6 Електронний уряд

Блокчейн допоможе знизити кількість паперів і дій, які нам доводиться виконувати для оформлення документів і угод, наприклад, посвідчення особи, покупки нерухомості і ін. Завдяки новому виду баз даних не треба буде кожного разу завіряти оригінали у нотаріуса, пересилати їх рекомендованими листами і займатися всім тим, що зараз з'їдає час і нерви. Замість цього ми будемо один раз завантажувати цифрові копії документів в блокчейн-мережу і підписувати кожну операцію в ній без участі нотаріуса.

3.6.7 Фінанси

Сьогодні ми залежимо від фінансових посередників: банків, брокерів і так далі. Залежимо від їх умов і термінів. Але поява блокчейн-проектів у

фінансовій сфері змусило банки задуматися, як зробити обслуговування клієнтів більш прозорим і швидким. Наприклад, блокчейн може прискорити перекази між рахунками - вони перестануть залежати від «банківського дня». До того ж, технологія допоможе банкам знизити витрати на обслуговування за рахунок відмови від зайвої паперової роботи.

3.6.8 Юриспруденція

Один із принципів блокчейна: «код - це закон». В майбутньому юристи зможуть писати всередині блокчейн-мережі так звані розумні контракти, які будуть працювати автоматично. Наприклад, якщо постачальник домовився з магазином привозити товар щоп'ятниці, а магазин повинен оплачувати постачання щопонеділка, то це буде записано в блокчейн-контракті. Контракт не можна обдурити: якщо постачальник не привезе товар, то він не зможе вимагати гроші, а якщо привезе, то магазин не зможе затримувати оплату - вона спишеться автоматично. Зараз для угод використовується складна система з договорів на папері і інструментів впливу на кшталт пені за прострочення або судових позовів. В кінцевому підсумку все тримається на довірі між партнерами.

3.6.9 Медицина

Блокчейн-мережі для зберігання медичних даних вже зараз тестують деякі держави і компанії, і в майбутньому це цілком може стати буденною справою. Напевно у вас є паперова медична карта, а якщо ви лікувалися в різних клініках, то, можливо, і не одна. Сьогодні дані цих карт можна оцифрувати і об'єднати, і, якщо ви поїдете в інше місто або навіть країну, доступ до повної цифрової копії ваших медичних даних може стати справжнім порятунком.

3.7 Вибір мережевих технологій для магістральної мережі та мережі рівня доступу

Основною магістральною технологіэю на сьогодні є GigabitEthernet. Технологія GigabitEthernet (гігабітний стандарт Ethernet) - це

високошвидкісні локальні мережі стандарту IEEE 802.3z. Дана технологія дозволяє використовувати смугу пропускання в 10 разів більшу, ніж технологія FastEthernet.

Комплекс технологій GigabitEthernet призначений для побудови дуже швидкісних магістральних з'єднань в мережах IEEE 802.3/Ethernet. Як випливає з назви, технології цього комплексу забезпечують можливість передачі даних по магістральних з'єднаннях ЛВС Ethernet на швидкості 10 Гбіт/сек. У табл. 3 наведено порівняльні характеристики технологій ATM і GigabitEthernet.

Один з потенційних недоліків GigabitEthernet в тому, що технологія Ethernet у чистому виді не призначена для підтримки трафіку реального часу, такого, як мова і відео. Для таких пакетів повинні бути прийняті досить серйозні заходи щодо забезпечення якості обслуговування, щоб вони перебували вчасно і без затримки.

Таблиця 2 - Порівняльна характеристика технологій ATM і GigabitEthernet

Технологія ATM	Технологія Gigabit Ethernet
Підтримує механізм QoS як у локальних, так і в розподілених мережах. Дозволяє правилами QoS локальної мережі поширюватися на розподілену мережа	Засоби QoS реалізовані у вигляді шести рівнів пріоритетів, які не розповсюджуються в розподілену мережу
Заснована на концепції віртуальних каналів, що гарантує надійність і стійкість	Використовується шинна топологія. Може бути побудована в комутованих виділених або частково виділених сегментах
Дозволяє досягати швидкості передачі даних до 10 Гбіт / с і вище	Обмеження по швидкості - 1 Гбіт/с (без використання дуплексної передачі) та до 10 Гбіт/с

Базові контрольно-керуючі технології для магістральних мереж є: VLAN, Q-in-Q, STP, OSPF, MPLS.

Найбільш передовою технологією для побудови операторських мереж є Multi Protocol Label Switching (MPLS), як найбільш ефективна архітектура для передачі IP трафіку.

Для просування даних по мережі MPLS використовує техніку, відому як комутація пакетів за мітками. MPLS підтримує й інші додаткові сервіси: Traffic Engineering (TE), QoS, VPN, EoMPLS і AToM.

MPLS знаходиться між мережевих і канальним рівнями, і емулює різні властивості мереж з комутацією каналів поверх мереж з комутацією пакетів. Тим самим з його допомогою можна передавати різні протоколи за одним стандартом. У традиційній IP мережі пакети передаються від одного маршрутизатора іншому і кожен маршрутизатор читаючи заголовок пакета (адреса призначення) приймає рішення про те, за яким маршрутом відправити пакет далі.

3.8 Вибір топології для магістральної мережі

Магістральна мережа повинна забезпечувати високу відмовостійкість, так як на магістралі об'єднуються потоки всій мережі доступу. Існують дві топології, які забезпечують високу надійність: «кожний з кожним», та «кільце». Однак для топології «кожний з кожним» потрібно дуже багато кабелю, та портів, що не ефективним з боку економічності.

Тому для забезпечення підвищеної надійності та резервування широко застосовується топологічна модель кільця. Кільця, зазвичай створюють на рівнях опорної мережі і доступу. Для з’єднання мережі використовуються оптоволоконні лінії зв’язку, адже оптоволоконна лінія зв'язку — сама надійна й стабільна технологія для підключення абонента до вузла провайдера на будь-яких дистанціях, та забезпечує швидкості передачі до 10 Гбіт/с і вище, побудована на базі оптоволоконних кабелів.

3.9 *Вибір мережевих технологій для мережі рівня доступу*

Для з’єднання рівня доступу та магістралі необхідно використовувати оптичне волокно. Переваги оптоволоконного типу зв'язки:

– по оптоволоконній лінії можна передавати інформацію зі швидкістю порядку 1000 Гбіт/с і більше;

– дуже мале загасання світлового сигналу у волокні, що дозволяє будувати волоконно-оптичні лінії зв'язку довжиною до 100 км і більш без регенерації сигналів;

– стійкість до електромагнітних перешкод з боку навколишніх мідних кабельних систем, електричного устаткування (лінії електропередачі т.і.) і погодних умов;

– захист від несанкціонованого доступу. Інформацію, що передається по волоконно-оптичним лініям зв'язку, практично не можна перехопити не руйнуючим кабель способом;

– довговічність — термін служби волоконно-оптичних ліній зв'язку становить не менш 25 років.

Розвиток технології оптичних кабельних систем і поступове витіснення традиційних мідних кабелів оптичними, призвело до появи концепції оптичних широкосмугових мереж доступу.

3.10 *Вибір топології мережі доступу*

У сучасних оптичних мережах доступу можуть використовуватися різні топології мережі. Вибір оптимальної топології залежить від цілого ряду чинників, пов'язаних з конкретними умовами проектування (щільність абонентів, їх розташування, види послуг і т.д.), а також від базової оптичної технології. У табл. 8 наведено порівняння основних мережевих технологій.

Виходячи з порівняння основних мережевих топологій вирішено обрати топологію «кільце», та на центральному рівні топологію "зірка".

Таблиця 3– Порівняння мережевих топологій

Особливості	Зірка	Лінійна	Кільце
Можливість використання недорогого активного устаткування без підтримки STP	Так	Так	Немає
Збереження працездатності всіх користувачів мережі у випадку ушкодження кабелю.	Немає	Немає	Так
Можливість організації додаткового (резервного) каналу без перебудови топології мережі.	Немає	Так	Так
Збереження зв'язку між вузлами у випадку відмови центрального устаткування.	Немає	Чим ближче до головного вузла тим більше відкаже вузлів	Так
Мала залежність від особливостей місця будівництва.	Так	Так	Немає

Таке з’єднання не захистить від обриву кабелю, але зможе захистити при виході з ладу одного з комутаторів в ланцюзі. На Рис. 5 показані обрані варіанти топології для мережі доступу багатоповерхової забудови.

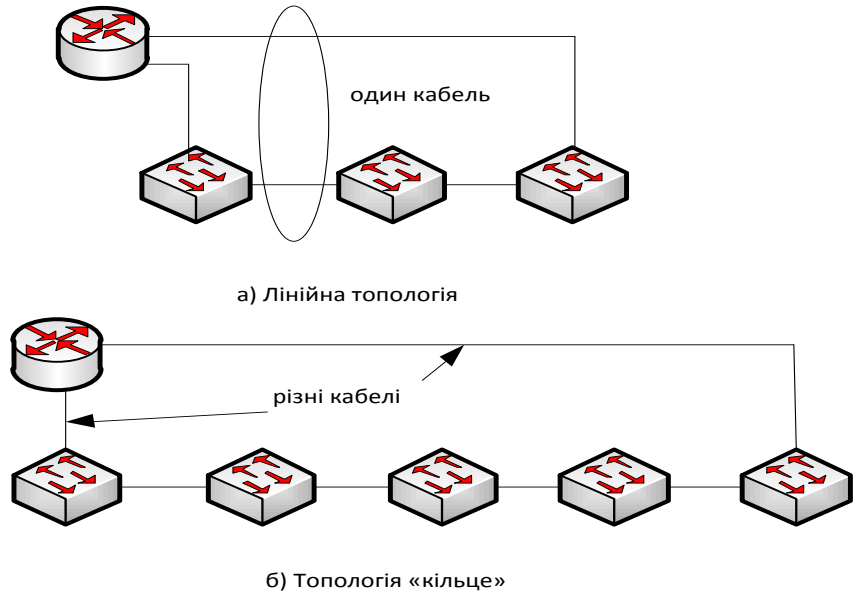


Рисунок 5 – Обрані топології мережі

3.11 Основні відомості про університет

Університет складається с 9 корпусів. Загальний вигляд університету представлений у див. Додаток А. На поверхах знаходяться кабінети аудиторій, приймальна, адміністрація, кабінети охорони, камери відеоспостереження, столові, кабінети викладачів тощо.

3.12 Практична реалізація у середовищі моделювання

У якості програми моделювання оберемо середовище моделювання Packet Tracer.

Packet Tracer – це програма структурно-логічного проектування комп'ютерних мереж. Вона дозволяє виконувати моделювання роботи мережі на основі устаткування корпорації Cisco, підтримує модульне мережеве устаткування. Завдяки наявності режиму симуляції і аналізатора протоколів можливо побачити як структуру пакетів, які генеруються різними мережевими протоколами, так і алгоритми роботи різних пристроїв.

3.13 Загальний вигляд мережі та її первісне налаштування.

За допомогою методу VLSM розіб'ємо блок мережевих адрес на необхідну кількість підмереж й установимо відповідні параметри для всіх обладнань.

Для розв'язку нашого завдання виділена наступна мережа: 15.1.0.0/23

Нам потрібно розбити дану мережу на 28 підмереж. Нижче я наведу табл. 9 масок підмереж, номеру віртуальних мереж, їхніх адрес та іншого.

Таблиця 4 - адрес підмереж, їх масок, номерів VLAN та діапазону адрес.

Ім'я підмережі	Розмір	Виділений розмір	Адрес	Маска	Десяткова маска	Інверсна маска	Діапазони доступних адрес	Номер vlan	Широкомовний адрес
VoIP	60	64	15.1.0.0	/26	255.255.255.192	0.0.0.63	15.1.0.1 - 15.1.0.62	10	15.1.0.63
Админи-стратор	30	32	15.1.0.64	/27	255.255.255.224	0.0.0.31	15.1.0.65 - 15.1.0.94	11	15.1.0.95
Деканат	30	32	15.1.0.96	/27	255.255.255.224	0.0.0.31	15.1.0.97 - 15.1.0.126	12	15.1.0.127
Служба Защиты	30	32	15.1.0.128	/27	255.255.255.224	0.0.0.31	15.1.0.129 - 15.1.0.158	13	15.1.0.159
Резервні кабінети	14	16	15.1.0.160	/28	255.255.255.240	0.0.0.15	15.1.0.161 - 15.1.0.174	14	15.1.0.175
Конференц зал	14	16	15.1.0.176	/28	255.255.255.240	0.0.0.15	15.1.0.177 - 15.1.0.190	15	15.1.0.191
Корпус 1 Поверх 1	14	16	15.1.0.192	/28	255.255.255.240	0.0.0.15	15.1.0.193 - 15.1.0.206	16	15.1.0.207
Корпус 1 Поверх 2	14	16	15.1.0.208	/28	255.255.255.240	0.0.0.15	15.1.0.209 - 15.1.0.222	17	15.1.0.223
Корпус 2 Поверх 1	14	16	15.1.0.224	/28	255.255.255.240	0.0.0.15	15.1.0.225 - 15.1.0.238	18	15.1.0.239
Корпус 2 Поверх 2	14	16	15.1.0.240	/28	255.255.255.240	0.0.0.15	15.1.0.241 - 15.1.0.254	19	15.1.0.255
Корпус 3 Поверх 1	14	16	15.1.1.0	/28	255.255.255.240	0.0.0.15	15.1.1.1 - 15.1.1.14	20	15.1.1.15
Корпус 3 Поверх 2	14	16	15.1.1.16	/28	255.255.255.240	0.0.0.15	15.1.1.17 - 15.1.1.30	21	15.1.1.31
Корпус 4 Поверх 1	14	16	15.1.1.32	/28	255.255.255.240	0.0.0.15	15.1.1.33 - 15.1.1.46	22	15.1.1.47
Корпус 4 Поверх 2	14	16	15.1.1.48	/28	255.255.255.240	0.0.0.15	15.1.1.49 - 15.1.1.62	23	15.1.1.63
Корпус 5 Поверх 1	14	16	15.1.1.64	/28	255.255.255.240	0.0.0.15	15.1.1.65 - 15.1.1.78	24	15.1.1.79
Корпус 5	14	16	15.1.1.80	/2	255.255.255.24	0.0.0.1	15.1.1.81 -	25	15.1.1.95

Поверх 2				8	0	5	15.1.1.94		
Корпус 7 Поверх 1	14	16	15.1.1.96	/28	255.255.255.240	0.0.0.15	15.1.1.97 - 15.1.1.110	26	15.1.1.111
Корпус 7 Поверх 14	14	16	15.1.1.112	/28	255.255.255.240	0.0.0.15	15.1.1.113 - 15.1.1.126	27	15.1.1.127
Корпус 10 Поверх 1	14	16	15.1.1.128	/28	255.255.255.240	0.0.0.15	15.1.1.129 - 15.1.1.142	28	15.1.1.143
Корпус 10 Поверх 2	14	16	15.1.1.144	/28	255.255.255.240	0.0.0.15	15.1.1.145 - 15.1.1.158	29	15.1.1.159
Серверна	6	8	15.1.1.160	/29	255.255.255.248	0.0.0.7	15.1.1.161 - 15.1.1.166	30	15.1.1.167
Wi-Fi	6	8	15.1.1.168	/29	255.255.255.248	0.0.0.7	15.1.1.169 - 15.1.1.174	31	15.1.1.175
External_Isp 1	2	4	15.1.1.176	/30	255.255.255.252	0.0.0.3	15.1.1.177 - 15.1.1.178	32	15.1.1.179
External_Isp 2	2	4	15.1.1.180	/30	255.255.255.252	0.0.0.3	15.1.1.181 - 15.1.1.182	33	15.1.1.183
Адмін	2	4	15.1.1.184	/30	255.255.255.252	0.0.0.3	15.1.1.185 - 15.1.1.186	34	15.1.1.187

Таким чином ми отримали, що адрес вхідної мережі становить 15.1.0.0/23 кількість доступних адрес в цій мережі: 510. Ми використали 398 адрес, що становить близько 89% доступного адресного простору мережі.

Далі потрібно розробити адресацію в мережі. Для цього нам треба придбати блок адрес розміром у 512 IP-Адрес. Спочатку ці адреси треба зареєструвати у RIPE NCC. Це дає змогу клієнтам університету зв'язатись з будь ким, через, наприклад, VPN (віртуальну приватну мережу) для обміну конфіденційними даними. Зменшується навантаження на головний маршрутизатор, так як йому не треба робити мережеву трансляцію адрес, таким чином ми підіймаємо його швидкодію. Ці адреси ми будемо

присвоювати динамічно, за допомогою DHCP, це полегше користувачам вихід до мережі Інтернет.

Мережу університету побудуємо на віртуальних підмережах. Це вигідно, коли нам, наприклад, треба розмістити камери відеоспостереження на окремих поверхах, і щоб не прокладати нові кабелі, достатньо вказати на комутаторі, що ці порти належать до цієї підмережі. Таким чином ми отримуємо одну велику віртуальну підмережу, на окремих комутаторах.

3.14 Налаштування VLAN

VLAN (від англ. Virtual Local Area Network) — віртуальна локальна обчислювальна мережа, відома так само як VLAN, являє собою групу хостів із загальним набором вимог, які взаємодіють так, ніби вони були підключені до широкомовного домену, незалежно від їхнього фізичного місцезнаходження. VLAN має ті ж властивості, що й фізична локальна мережа, але дозволяє кінцевим станціям, групуватися разом, навіть якщо вони не перебувають в одній фізичній мережі. Така реорганізація може бути зроблена на основі програмного забезпечення замість фізичного переміщення обладнання.

На пристроях Cisco, протокол VTP (VLAN Trunking Protocol) передбачає Vlan-Домени для спрощення адміністрування. VTP також виконує «чищення» трафіка, направляючи VLAN трафік тільки на ті комутатори, які мають цільові Vlan-Порти. Cisco комутатори в основному використовують протокол ISL (Inter-Switch Link) для забезпечення сумісності інформації.

Налаштування VTP на Switch Layer 3 :

– Switch> enable

– Switch# configure terminal

– Switch(config)# vtp domain hotel

– Switch(config)# vtp mode server

– Switch(config)# vtp password pass

– Switch(config)# exit

Для всіх комутаторів у мережі треба налаштувати VTP, щоб вони отримали всі VLAN, налаштування наступне:

– Switch> enable

– Switch# configure terminal

– Switch(config)# vtp domain hotel

– Switch(config)# vtp mode client

– Switch(config)# vtp password pass

– Switch(config)# exit

Native VLAN — кожний порт має параметр, названий постійний віртуальний ідентифікацією (Native VLAN), який визначає VLAN, призначений одержувати не таргетировані кадри.

Для позначення членства в VLAN існують наступні розв'язки:

– По портові (Port-based, 802.1Q): порту комутатора вручну призначається один VLAN. У випадку, якщо одному порту повинні відповідати декілька VLAN (наприклад, якщо з'єднання VLAN проходить через декілька світчей), то цей порт повинен бути членом транка. Тільки один VLAN може одержувати всі пакети, не віднесені до жодного VLAN. Комутатор буде додавати мітки даного VLAN до всіх прийнятих кадрів, що не мають ніяких міток. VLAN побудовані на базі портів мають деякі обмеження. Крім того, вносити зміни в VLAN на основі портів досить складно, оскільки при кожній зміні потрібне фізичне перемикання пристроїв.

– По Mac-Адресі (Mac-based): членство в Vlane ґрунтується на Mac-Адресі робочої станції. У такому випадку світч має таблицю Mac-Адрес усіх пристроїв разом з Vlanами, до яких вони належать.

– По протоколу (Protocol-based): дані 3-4 рівня в заголовку пакета використовуються щоб визначити членство в Vlan'e. Основний недолік цього методу в тому, що він порушує незалежність рівнів, тому, наприклад, перехід з Ipv4 на Ipv6 приведе до порушення працездатності мережі.

– Методом аутентифікації (Authentication based): Пристрої можуть бути автоматично переміщені в VLAN ґрунтуючись на даних аутентифікації користувача або пристрою, при використанні протоколу 802.1x

Налаштування Switch Layer3:

Для початку створемо всі VLAN, які є в нашій мережі

– Switch> enable

– Switch# configure terminal

– Switch(config)# vlan 10

– Switch(config-vlan)# name VoIP

– Switch(config-vlan)# exit

– ....

– Switch> enable

– Switch# configure terminal

– Switch(config)# vlan 34

– Switch(config-vlan)# name Admin

– Switch(config-vlan)# exit

Для комутаторів на рівні доступу треба налаштувати потри, та віртуальні мережі, які відносяться до цих портів.

Далі для кожного використовуваного інтерфейсу визначимо свої параметри

– Switch> enable

– Switch# configure terminal

– Switch(config)# interface fastethernet 0/1

– Switch(config-if)# switchport mode access

– Switch(config-if)# switchport access vlan 11

– Switch(config-if)# exit

Для використання IP телефонії налаштування будуть такі:

– Switch> enable

– Switch# configure terminal

– Switch(config)# interface fastethernet 0/2

– Switch(config-if)# switchport mode access

– Switch(config-if)# switchport voice access 10

– Switch(config-if)# exit

У нашій мережі використовується 32 порта у магістральному режимі.

Налаштування магістральних портів наступне:

–Switch> enable

–Switch# configure terminal

–Switch(config)# interface gigabitEthernet 0/23

–Switch(config-if)# switchport mode trunk

–Switch(config-if)# exit

Створення логічного під-інтерфейсу адміністрації (VLAN 11) на Main_Router:

– Main> enable

– Main# configure terminal

– Main(config)# interface gigabitEthernet 8/0.11

– Main(config-subif)# no shutdown

– Main(config-subif)# encapsulation dot1Q 11

– Main(config-subif)# ip address 15.1.0.64 255.255.255.224

– Main(config-subif)# exit

Створення логічного під-інтерфейсу для VoIP (VLAN 10) на VOIP:

– VoIP> enable

– VoIP# configure terminal

– VoIP(config)# interface fastEthernet 0/0.1

– VoIP(config-subif)# no shutdown

– VoIP(config-subif)# encapsulation dot1Q 10

– VoIP(config-subif)# ip address 15.1.0.1 255.255.255.192

– VoIP(config-subif)# exit

3.15 Маршрутизація у середині мережі та ззовні

Будь-яка мережа передачі даних з комутацією пакетів спирається на протоколи мережевого рівня. Основною задачею мережевого рівня є задача маршрутизації. Маршрутизація — процес визначення маршруту прямування інформації між мережами. Най простіший спосіб маршрутизації – це статична маршрутизація. Але тут є багато мінусів:

– Дуже погане масштабування;

– Низька стійкість до пошкоджень ліній зв'язку (особливо, в ситуаціях, коли обрив відбувається між пристроями другого рівня і порт маршрутизатора не отримує статус down);

– Відсутність динамічного балансування навантаження;

– Необхідність у веденні окремої документації до маршрутів, проблема синхронізації документації і реальних маршрутів.

Для вирішення цих проблем використовують динамічну маршрутизацію. Існує ціла низка алгоритмів динамічної маршрутизації, починаючи від простих дистанційно векторних і закінчуючи протоколами стану каналів.

3.16 Налаштування протоколу OSPF

OSPF (англ. Open Shortest Path First) — протокол динамічної маршрутизації, оснований на технології відстеження стану каналу (link-state technology), який використовує для знаходження найкоротшого шляху Алгоритм Дейкстри (Dijkstra's algorithm).

Опис роботи протоколу:

– Маршрутизатори обмінюються hello-пакетами через усі інтерфейси, на яких активований OSPF. Маршрутизатори, що розділяють загальний канал передачі даних, стають сусідами, коли вони приходять до домовленості про певні параметри, які вказані в їхніх hello-пакетах.

– На наступному етапі роботи протоколу маршрутизатори будуть намагатися перейти в стан сусідства з маршрутизаторами, що перебувають із

ним у межах прямого зв'язку (на відстані одного хопа). Перехід у стан сусідства визначається типом маршрутизаторів, що обмінюються hello-пакетами, і типом мережі, по якій передаються hello-пакети. OSPF визначає кілька типів мереж і кілька типів маршрутизаторів. Пари маршрутизаторів, що перебувають у стані сусідства, синхронізують між собою базу даних стану каналів.

– Кожний маршрутизатор посилає оголошення про стан каналу маршрутизаторам, з якими він перебуває в стані сусідства.

– Кожний маршрутизатор, що одержав оголошення від сусіда, записує передану в ньому інформацію в базу даних стану каналів маршрутизатора й розсилає копію оголошення всім іншим своїм сусідам.

– Кожний маршрутизатор будує таблицю маршрутизації зі свого дерева найкоротшого шляху.

Налаштування протоколу OSPF на маршрутизаторі Main Router виглядає так:

– Main> enable

– Main# configure terminal

– Main(config)# router ospf 1

– Main(config-router)# network 15.0.0.0 0.255.255.255 area 0

– Main(config-router)# network 32.0.0.0 0.255.255.255 area 0

– Main(config-router)# exit

3.17 Налаштування протоколу RIP

Протокол RIP (англ. Routing Information Protocol) - один з найпоширеніших протоколів маршрутизації в невеликих комп'ютерних мережах, який дозволяє маршрутизаторам динамічно обновляти маршрутну інформацію (напрямок і дальність у хопах), одержуючи її від сусідніх маршрутизаторів.

Прототип протоколу RIP - Gateway Information Protocol, частина пакета PARC Universal Packet.

Технічна інформація: RIP - так званий дистанційно-векторний протокол, який оперує хопами в якості метрики маршрутизації. Максимальна кількість хопів, дозволена в RIP - 15 (метрика 16 означає «нескінченно велику метрику»). Кожний Rip-Маршрутизатор за замовчуванням віщає в мережу свою повну таблицю маршрутизації один раз в 30 секунд, генеруючи досить багато трафіка на низькошвидкісних лініях зв'язку. RIP працює на прикладному рівні стека TCP/IP, використовуючи UDP порт 520.

У сучасних мережевих середовищах RIP - не найкраще рішення для вибору як протоколу маршрутизації, тому що його можливості уступають більш сучасним протоколам, таким як EIGRP, OSPF. Обмеження на 15 хопів не дає застосовувати його у великих мережах. Перевага цього протоколу - простота конфігурування.

Я використовую протокол RIP у маршрутизаторах для бездротового, доступу до мережі Інтернет. Так як його не треба конфігурувати, за мене це зробив Packet Tracert, я наведу приклад конфігурування цього протоколу на маршрутизаторі Main для мереж, які його оточують:

– Main> enable

– Main# configure terminal

– Main(config)# router rip

– Main(config-router)# version 2

– Main(config-router)# no auto

– Main(config-router)# network 15.0.0.0

– Main(config-router)# network 32.0.0.0

– Main(config-router)# exit

За для забезпечення безпеки в мережі, я відмінив маршрутизацію між окремими мережами, але підмережа адміністрації, та охорони, можуть "бачити" всі комп'ютери у мережі, для завчасного виявлення зловмисників, тощо.

3.18 Налаштування HTTP сервера

Веб-сервер — це сервер, що ухвалює HTTP-Запити від клієнтів, зазвичай веб-браузерів, та видає їм HTTP-Відповіді, разом з HTML-Сторінкою, зображенням, файлом, медіа-потоком або іншими даними. Веб-сервери — основа Всесвітньої павутини.

Веб-сервером називають як програмне забезпечення, що виконує функції веб-сервера, так і комп'ютер, на якому це програмне забезпечення працює.

Клієнти одержують доступ до веб-сервера по URL адресі потрібної їм веб-сторінки або іншого ресурсу.

Для Налаштування HTTP сервера нам необхідно:

– Включити на сервері підтримку HTTP сервісу в програмі Packet Tracer;

– Заповнити “Default Page Content(index.html)” у програмі Packet Tracer, яка буде стартовою сторінкою нашого HTTP сервера;

– Указати IP адрусу й маску підмережі нашого сервера;

– Указати шлюз, через який наш сервер з'єднаний з іншою мережею.

На Рис.6 умовно, я створив два сервери, котрі символізують собою вихід до мережі Інтернет. Сервер 15.1.1.190/30 э DNS сервером всієї мережі 15.0.0.0/23. На ньому розміщується сайт компанії-провайдера, url адреса котрого "http://www.nmu.org.ua/ua/". Цей сервер перетворює зовнішній адрес 32.15.47.45/8 у читабельний url сайту, котрий перебуває по за межами нашої мережі, а саме "https://do.nmu.org.ua/"

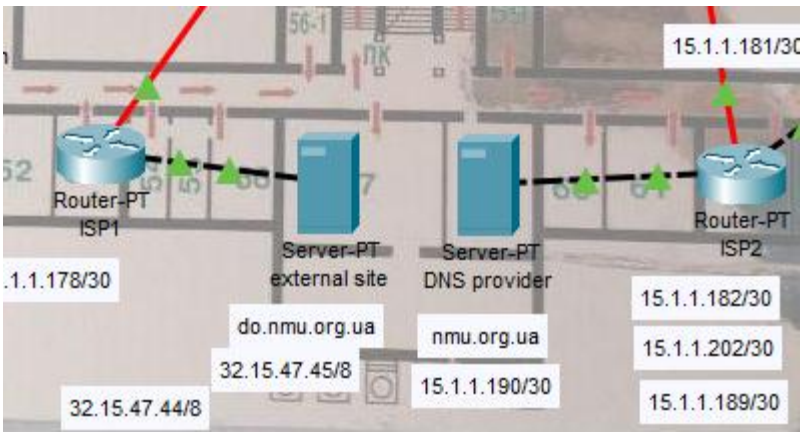


Рисунок 6 - Сервери провайдерів Інтернету, під'єднаних до нашої мережі

Також я створив сторінки, на яких наглядно видно, на якому сайті перебуває користувач, та який IP-адрес цього сайту

На Рис. 7 зображено, як користувач Інтернету потрапляє на сайт, який знаходиться в мережі Інтернет

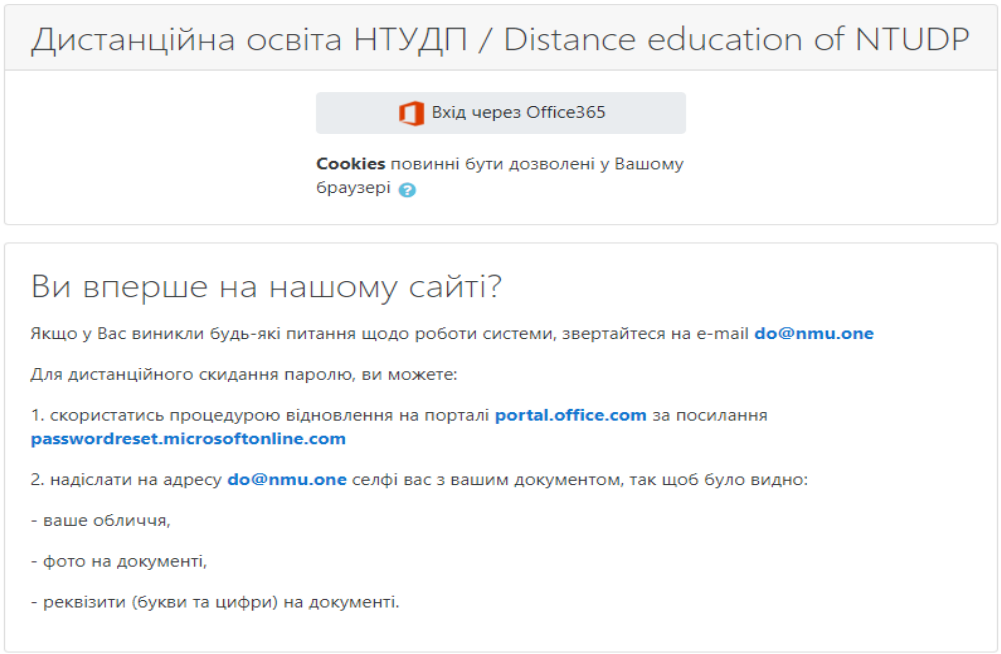


Рисунок 7 - Сайт do.nmu.org.ua

На рис. 8 показано, що користувач перейшов на сайт, який знаходиться в межах нашої мережі.

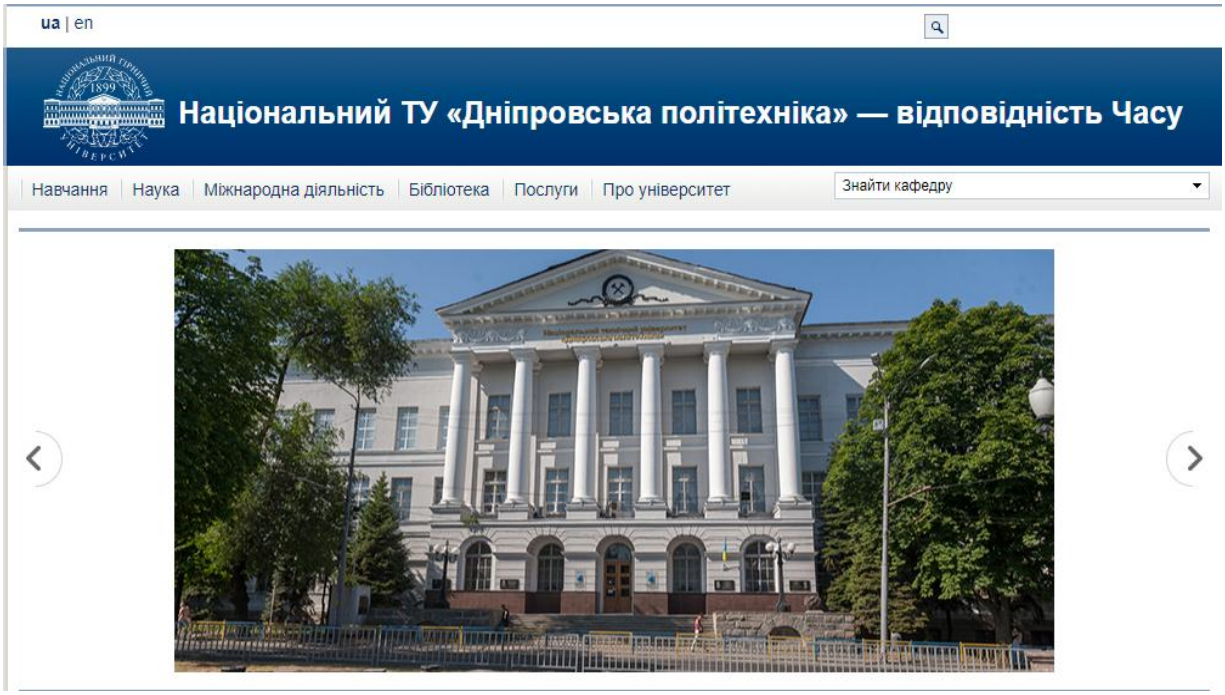


Рисунок 8 - сайт nmu.org.ua

3.19 Налаштування DNS сервера

DNS-Сервер — додаток, призначений для відповідей на DNS-Запити по відповідному протоколу. Також DNS-Сервером можуть називати хост, на якому запущений додаток.

Я розмістив DNS сервер на стороні провайдеру, котрий видає мережеві адреси, та дає доступ до мережі Інтернет. Це вигідно, бо ми маємо з провайдером одну підмережу 15.0.0.0/16, це дає змогу нам не купувати додаткове обладнання (Рис. 9).

Конфігурування DNS серверу, адрес якого 15.1.1.190/30 , який є DNS сервером нашої мережі.

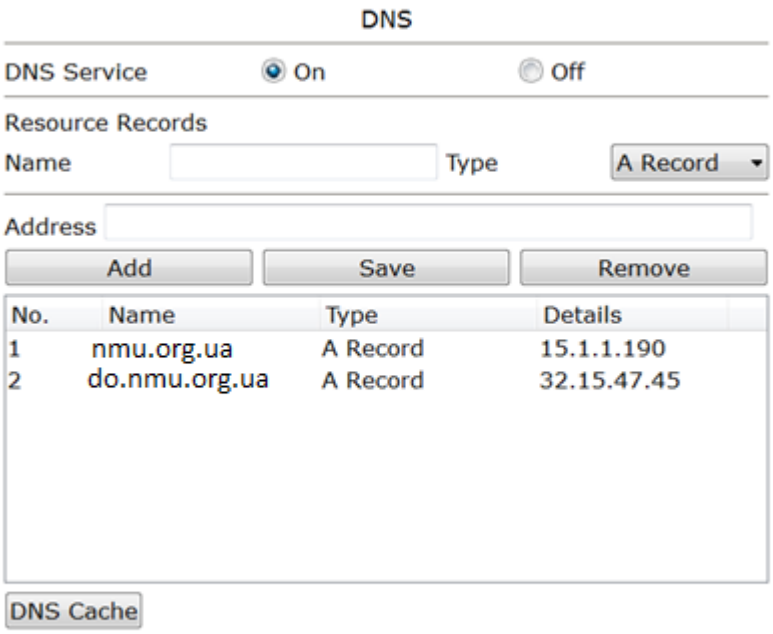


Рисунок 9 - конфігурація DNS серверу у середовищі Packet Tracer.

3.20 Налаштування DHCP сервера

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамічної конфігурації вузла) — це мережевий протокол, що дозволяє комп'ютерам автоматично одержувати IP-Адресу й інші параметри, необхідні для роботи в мережі TCP/IP. Для цього комп'ютер звертається до спеціального сервера, названного сервером DHCP. Мережевий адміністратор може задати діапазон адрес, що розподіляються серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості великих (і не дуже) мереж TCP/IP.

3.20.1 Розподіл IP-Адрес

Протокол DHCP надає три способи розподілу IP-Адрес:

– Ручний розподіл. При цьому способі мережевий адміністратор складає апаратній адресі (звичайно Mac-Адресі) кожного клієнтського комп'ютера певний IP-Адрес. Фактично, даний спосіб розподілу адрес відрізняється від ручного налаштування кожного комп'ютера лише тим, що відомості про адреси зберігаються централізовано (на сервері DHCP), і тому їх простіше змінювати при необхідності.

– Автоматичний розподіл. При даному способі кожному комп'ютеру на постійне використання виділяється довільний вільний IP-Адрес з певного адміністратором діапазону.

– Динамічний розподіл. Цей спосіб аналогічний автоматичному розподілу, за винятком того, що адреса видається комп'ютеру не на постійне користування, а на певний строк. Це називається орендою адреси. Після закінчення строку оренди, IP-Адреса знову вважається вільною, і клієнт зобов'язаний запросити новий (він, втім, може виявитися тим же самим адресом).

Деякі реалізації служби DHCP здатні автоматично обновляти записи DNS, відповідні до клієнтських комп'ютерів, при виділенні їм нових адрес.

Це проводиться за допомогою протоколу відновлення DNS, описаного в RFC 2136.

Для динамічного присвоювання адрес в мережі, я використовую два DHCP сервера, на різних маршрутизаторах, тобто, один DHCP відповідає тим підмережам, котрі приєднані до маршрутизатору.

3.20.2 Опції DHCP

У університеті і є два DHCP сервера, котрі розподіляють адреси, один адміністрації, охороні, та відділам продаж, тощо, другий розподіляє адреси між IP телефонами та поверхами університету, у котрих розташовуються постояльці. Це дає змогу рівномірно розподілити навантаження між маршрутизаторами, та біль чітко розподілити навантаження трафіку в мережі.

Одновною з основних задач DHCP є оповіщення клієнта, який IP адрес йому належить, також DHCP може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями DHCP. Список стандартних опцій можна знайти в RFC 2132.

Деякими з найбільш часто використовуваних опцій є:

– IP-Адреса маршрутизатора за замовчуванням;

– маска підмережі;

– адреси серверів DNS;

– ім'я домена DNS.

Деякі постачальники програмного забезпечення можуть визначати власні, додаткові опції DHCP.

Протокол DHCP є клієнт-серверним, тобто в його роботі беруть участь клієнт DHCP і сервер DHCP. Передача даних проводиться за допомогою протоколу UDP, при цьому сервер ухвалює повідомлення від порт 67 і відправляє повідомлення на порт 68.

3.20.3 Приклад процесу одержання адреси

Приведу приклад процесу одержання IP-Адреси клієнтом від сервера DHCP. Припустимо, клієнт ще не має власного IP-Адреса, але йому відома його попередня адреса — 192.168.1.100. Процес складається із чотирьох етапів.

– Виявлення DHCP:

На початку клієнт виконує широкомовний запит по всій фізичній мережі з метою виявити доступні DHCP-Сервери. Він відправляє повідомлення типу DHCPDISCOVER, при цьому в якості IP-Адреси джерела вказується 0.0.0.0 (тому що комп'ютер ще не має власного IP-Адреси), а в якості адреси призначення — широкомовна адреса 255.255.255.255.

Клієнт заповнює декілька полів повідомлення початковими значеннями:

- У полі xid міститься унікальний ідентифікатор транзакції, який дозволяє відрізняти даний процес одержання IP-Адреси від інших, що протікають у той же час.

- У полі chaddr міститься апаратну адресу (Mac-Адреса) клієнта.

- У полі опцій вказується останній відомий клієнтові IP-Адреса. У даному прикладі це 192.168.1.100. Це необов'язково й може бути проігнороване сервером.

Повідомлення DHCPDISCOVER може бути поширене за межі локальної фізичної мережі за допомогою спеціально настроєних агентів ретрансляції DHCP, що перенаправляють поступаючі від клієнтів повідомлення DHCP серверам в інших підмережах.

– Пропозиція DHCP:

Одержавши повідомлення від клієнта, сервер визначає необхідну конфігурацію для клієнта відповідно до зазначених мережевим адміністратором налаштувань. У цьому випадку DHCP-Сервер згодний із запитаним клієнтом адресом 192.168.1.100. Сервер відправляє йому відповідь (DHCPOFFER), у якій пропонує конфігурацію. Пропонований клієнтові IP-

Адрес вказується в полі yiaddr. Інші параметри (такі, як адреси маршрутизаторів і DNS-Серверів) вказуються у вигляді опцій у відповідному полі.

Це повідомлення DHCP-Сервер відправляє хосту, що послав (DHCPDISCOVER) на його MAC, при певних обставинах може поширюватися, як широкомовне розсилання. Клієнт може одержати кілька різних пропозицій DHCP від різних серверів; з них він повинен вибрати те, яке його «улаштовує».

– Запит DHCP:

Вибравши одну з конфігурацій, запропонованих DHCP-Серверами, клієнт відправляє запит DHCP (DHCPREQUEST). Він розсилається широкомовно; при цьому до опцій, зазначених клієнтом у повідомленні DHCPDISCOVER, додається спеціальна опція - ідентифікатор сервера -, що вказує адресу DHCP-Сервера, обраного клієнтом (у цьому випадку - 192.168.1.1).

– Підтвердження DHCP:

Нарешті, сервер підтверджує запит і направляє це підтвердження (DHCPACK) клієнтові. Після цього клієнт повинен настроїти свій мережний інтерфейс, використовуючи надані опції.

3.20.4 Налаштування DHCP

Налаштування DHCP для підмережі адміністрації, на маршрутизаторі Main виглядає наступним чином:

– Main> enable

– Main# configure terminal

– Main(config)# ip dhcp pool Administration

– Main(dhcp-config)# default-router 15.1.0.65

– Main(dhcp-config)# network 15.1.0.65 255.255.255.224

– Main(dhcp-config)# dns-server 15.1.1.190

– Main(dhcp-config)# exit

Налаштування DHCP для підмережі IP телефонії, на маршрутизаторі VoIP виглядає наступним чином:

– VoIP> enable

– VoIP# configure terminal

– VoIP(config)# ip dhcp pool VoIP

– VoIP(dhcp-config)# network 15.1.0.0 255.255.255.192

– VoIP(dhcp-config)# default-router 15.1.0.1

– VoIP(dhcp-config)# option 150 ip 15.1.0.1

– VoIP(dhcp-config)# exit

3.21 Налаштування списків доступу ACL

Access Control List або ACL - список контролю доступу, який визначає, хто або що може отримувати доступ до конкретного об'єкта, і які саме операції дозволено або заборонено цьому суб'єкту проводити над об'єктом.Списки контролю доступу є основою систем з виборчим управлінням доступу.

Налаштуємо список доступу для користувачів Wi-Fi. Нам потрібно відокремити їх від користувачів у середині мережі, щоб запобігти ймовірному пошкодженню конфіденційних даних, тощо.

Налаштування проведемо на маршрутизаторі Main, тому що саме він відповідає за маршрутизацію та видачу Інтернет адрес підмережі користувачів бездротового виходу до мережі Інтернет(Wi-Fi):

– Main> enable

– Main# configure terminal

– Main(config)# ip access-list extended wifi

– Main(config-ext-nacl)# ip access-list extended wifi

– Main(config-ext-nacl)# deny ip any 0.0.0.0 255.255.0.0

– Main(config-ext-nacl)# permit udp any eq domain any

– Main(config-ext-nacl)# permit icmp any 0.0.0.2 255.255.255.252

– Main(config-ext-nacl)# permit ip any 0.0.0.2 255.255.255.252

– Main(config-ext-nacl)# permit udp any 0.0.0.2 255.255.255.252

– Main(config-ext-nacl)# exit

Щоб цей список працював, його треба налаштувати на інтерфейсі:

– Main> enable

– Main# configure terminal

– Main(config-subif)# interface GigabitEthernet8/0.31

– Main(config-subif)# ip access-group wifi in

– Main(config-subif)# exit

У середині мережі також можуть бути зловмисники серед робітників університету, котрі можуть зашкодити мережі. Усіма правами доступу в мережі університету будуть наділені лише адміністрація та охорона.

Для того, щоб охорона могла "бачити" любий комп'ютер в мережі, а любий комп'ютер в мережі не зміг "побачити" охоронців, треба створити такий список доступу на маршрутизаторі Main:

– Main> enable

– Main# configure terminal

– Main(config)# ip access-list extended sec

– Main(config-ext-nacl)# permit icmp any any echo-reply

– Main(config-ext-nacl)# permit tcp any any established

– Main(config-ext-nacl)# permit udp any eq domain any

– Main(config-ext-nacl)# exit

Також, його треба призначити інтерфейсу:

– Main> enable

– Main# configure terminal

– Main(config-subif)# interface GigabitEthernet8/0.31

– Main(config-subif)# ip access-group sec out

– Main(config-subif)# exit

3.22 Налаштування протоколу STP

Spanning Tree Protocol — мережевий протокол, що працює на другому рівні моделі OSI. Основним завданням STP є приведення мережі Ethernet із множинними зв'язками до деревоподібної топології, що виключає цикли пакетів. Відбувається це шляхом автоматичного блокування непотрібних у цей момент для повної зв'язності портів. Протокол описаний у стандарті IEEE 802.1D.

Принцип дії:

– У мережі вибирається один кореневий міст (англ. Root Bridge).

– Далі кожний, відмінний від кореневого міст, прораховує найкоротший шлях до кореневого. Відповідний порт називається кореневим портом (англ. Root Port). У будь-якого не кореневого комутатора може бути тільки один кореневий порт!

– Після цього для кожного сегмента мережі прораховується найкоротший шлях до кореневого порту. Міст, через який проходить цей шлях, стає призначеним для цієї мережі (англ. Designated Bridge). Безпосередньо підключений до мережі порт мосту — призначеним портом.

– Далі на всіх мостах блокуються всі порти, що не є кореневими й призначеними. У підсумку виходить деревоподібна структура (математичний граф) з вершиною у вигляді кореневого комутатора.

Алгоритм дії STP (Spanning Tree Protocol):

– Після включення комутаторів у мережу, за замовчюванням кожний комутатор важає себе кореневим (root).

– Потім комутатор починає посилати по всіх портах конфігураційні Hello BPDU пакети раз у 2 секунди.

– Виходячи з даних Hello BPDU пакетів, той або інший комутатор здобуває статус root, тобто кореня.

– Після цього всі порти крім root port і designated port блокуються.

– Відбувається посилка Hello-Пакетів раз в 2 секунди, з метою перешкоди появи петель у мережі.

Саме Налаштування в середовищі імітаційного моделювання Packet Tracer виглядає в такий спосіб:

Центральний комутатор потрібно призначити root-овим для всіх vlan

– Switch> enable

– Switch# configure terminal

– Switch(config)# spanning-tree mode rapid-pvst

– Switch(config)# spanning-tree portfast default

– Switch(config)# spanning-tree vlan 1-4096 priority 4096

– Switch(config)# exit

3.23 Налаштування VoIP

VoIP (англ. voice over IP — технологія передачі медіа даних в реальному часі за допомогою сімейства протоколів TCP/IP. IP-телефонія — система зв'язку, при якій аналоговий звуковий сигнал від одного абонента дискретизується (кодується в цифровий вигляд), компресія і пересилається по цифрових каналах зв'язку до другого абонента, де проводиться зворотна операція — декомпресія, декодування і відтворення аналогового сигналу.

Для роботи будь-якого VoIP потрібне широкосмугове підключення до Інтернету(виділена лінія, ADSL і т.д.), і чим швидше буде канал, тим краще. Відзначу, що для одного користувача підключення зі швидкістю 256 кбіт / с для вхідного потоку і 128 кбіт / с для вихідного буде цілком достатньо.

Налагодження VoIP у середовищі Packet Tracer виглядає наступним чином:

Для початку треба налагодити пул адрес, для VoIP пристроїв:

– VoIP> enable

– VoIP# configure terminal

– VoIP(config)# ip dhcp pool VoIP

– VoIP(dhcp-config)# network 15.1.0.0 255.255.255.192

– VoIP(dhcp-config)# default-router 15.1.0.1

– VoIP(dhcp-config)# option 150 ip 15.1.0.1

– VoIP(dhcp-config)# exit

Потім, за допомогою команди telephony service нам потрібно визначити кількість пристроїв, що будуть використовуватись, та який адрес нам буде видавати динамічні IP адреси, у нашому випадку це маршрутизатор VoIP.

– VoIP> enable

– VoIP# configure terminal

– VoIP(config)# telephony-service

– VoIP(config-telephony)# max-ephones 42

– VoIP(config-telephony)# max-dn 60

– VoIP(config-telephony)# ip source-address 15.1.0.1 port 2000

– VoIP(config-telephony)# exit

Тепер нам треба назначити номера телефонам, які будуть прив'язані до MAC адрес телефону, у автоматичному режимі, в порядку лічильника телефонам видадуться скорочення клавіш швидкого набору.

– VoIP> enable

– VoIP# configure terminal

– VoIP(config)# ephont-dn 1

– VoIP(config-ephone-dn)# number 151

– VoIP(config-ephone-dn)# exit

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Техніко-економічне обгрунтування розробки

В кваліфікаційній роботі розглядається приєднання blockchain до мережі університету. Для виконання поставленої задачі необхідно побудувати мережу, написати програму на Python та підключити її за допомоги технології Cisco. Це дозволить прискорити процес навчання студентів та заощадити їх час.

Для обґрунтування економічної доцільності, необхідно виконати:

– розрахунок капітальних витрат на придбання техніки та обладнання;

– розрахунок річних витрат проектної апаратури;

4.2 Розрахунок капітальних витрат на придбання обладнання

Капітальні вкладення – це кошти, призначені для створення і придбання основних фондів та нематеріальних активів, що підлягають амортизації.

Кошторис капітальних витрат на обладнання, яке необхідно для реалізації комп'ютерної системи, приведена в таблиці 6.1.

Капітальні витрати розраховуються за формулою:

$$Кпр = Коб + Ктр + Кмн + Кпз, \quad 6.1$$

де Коб – вартість обладнання, грн.,

Ктр – вартість транспортно-заготівельних витрат, грн.,

Таблиця 6.1- Кошторис капітальних витрат на обладнання

№ п/п	Найменування обладнання	Од. виміру	Кіль-кість	Вартість од. обладнання, грн	Сума, грн.

1	Обладнання та техніка	шт	100	10000	1000000
2	Оплата інтернету та мережі	Місяць	1	200	200
3	Оплата працівникам	місяць	30	5000	150000
Всього					1150200

Загальна вартість обладнання Коб=1150200 грн.

Вартість транспортно-заготівельних і складських витрат становить 7% від вартості обладнання.

Ктр=1150200*7%=80 514 грн.

Вартість монтажно-налагоджувальних робіт становить 8% від вартості обладнання.

Кмн=1150200*8%=92 016 грн.

4.2.1 Розрахунок капітальних витрат на програмне забезпечення

4.2.1.1 Розрахунок часу на розробку програмного забезпечення

Трудомісткість розробки програмного забезпечення:

$$t = t_o + t_д + t_a + t_n + t_{нал} + t_{док}, \quad (6.2)$$

где t_o - витрати праці на підготовку й опис поставленого завдання

$t_д$ - витрати праці на дослідження алгоритму розв'язку завдання;

t_a - витрати праці на обробку блок-схеми алгоритму;

t_n - витрати праці на програмування по готовій блок-схемі;

$t_{нал}$ - витрати праці на налаштування програм на ЕОМ;

$t_{док}$ - витрати праці на підготовку документації за завданням.

Складові частини витрат праці визначаються на підставі умовної кількості оброблюваних операторів у програмному забезпеченні. До них відносять ті оператори, які необхідно написати в процесі роботи над програмою з урахуванням можливих уточнень у постановці завдання й удосконалення алгоритму.

Умовна кількість операторів у програмі:

$$Q = q \cdot c \cdot (1+p), \qquad (6.3)$$

де q –кількість операторів, використовуваних у програмі.

Виходячи з ПЗ q = 25;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її обробки.

Коефіцієнт складності «c» програми визначає відносну складність програми відносно типового завдання, складність якого відповідає 1. c = 1,25.

Коефіцієнт корекції програми «p» визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму в результаті уточнення постановки завдання. Ухвалюємо p=0,1, це відповідає внесенню 3…5 корекцій, що тягнуть за собою переробку 5-10% готової програми.

Таким чином, для програми, описаної в кваліфікаційній роботі:

$$Q = 25*1,25(1+0,1) = 34,4$$

Оцінка витрат праці на підготовку й опис завдання становлять t_0=40 люд.-годин.

Витрати праці на вивчення опису завдання визначаються з урахуванням уточнення опису й кваліфікації програміста по формулі:

$$t_д = \frac{Q \cdot B}{(75...85) \cdot k} \text{ люд.-годин} \qquad (6.4)$$

де B – коефіцієнт збільшення витрат праці, B=1,4;

k – коефіцієнт кваліфікації програміста, які визначається залежно від стажу роботи зі спеціальності. У нашому випадку коефіцієнт кваліфікації програміста становить k= 1,2.

Для розроблюваного програмного забезпечення:

$$t_{Д} = \frac{34,4*1,4}{80*1,2} = 0,50 \text{ люд.-годин.}$$

Витрати на розробку алгоритму розв'язку завдання:

$$t_a = \frac{Q}{(20...25) \cdot k} \text{ люд.-годин} \qquad (6.5)$$

Для розроблювального програмного забезпечення:

$t_a = \frac{34,4}{20 \cdot 1,2}$ =1,43 люд.-годин.

Витрати праці на складання програми по готовій блок-схемі алгоритму:

$$t_n = \frac{Q}{(20...25) \cdot k} \text{ люд.-годин} \qquad (6.6)$$

Для розроблюваного програмного продукту:

$t_n = \frac{34,4}{20 \cdot 6\ 1,2} = 1.14$ люд.-годин

Витрати праці на налагодження програми на ЕОМ розраховуються по формулі:

$$t_{нал} = \frac{Q}{(4...5) \cdot k} \text{ люд.-годин} \qquad (6.7)$$

Для конкретного програмного продукту:

$$t_{нал} = \frac{34,4}{5 \cdot 1,2} = 5,7 \text{ люд.-годин.}$$

Витрати праці на підготовку документації за завданням визначаються по формулі:

$$t_Д = t_{ДР} + t_{ДО} \text{ люд.-годин} \qquad (6.8)$$

де $t_{ДР}$ – трудомісткість підготовки матеріалів до написання;

$t_{ДО}$ – трудомісткість редагування, друку й оформлення документації.

$$t_{ДР} = Q/(15…20) \cdot k, \qquad (6.9)$$

$t_{ДР} = 27,5/18 \cdot 1,2 = 1,59$ люд.-година;

$$t_{ДО} = 0,75 \cdot t_{ДР}, \qquad (6.10)$$

$t_{ДО} = 0,75 \cdot ,159 = 1,19$ люд.-година.

Для розроблюваного програмного забезпечення витрати праці на підготовку документації за завданням будуть становити:

$t_Д = 1,59 + 1,19 = 2,78$ люд.-година.

Трудомісткість розробки програмного забезпечення буде становити:

t = 40 + 0,50 + 1,43 + 1,14 + 5,7 + 2,78 = 51,55 людино-годин.

4.2.1.2 Розрахунки витрат на розробку програмного продукту

Витрати на розробку програмного продукту $К_{пз}$ містять витрати на заробітну плату розробника програми $З_{зп}$ і вартість машинного часу, необхідного для налаштування програми на ЕОМ $З_{мч}$

$$К_{пз} = З_{зп} + З_{ми}, \text{ грн.} \quad (6.11)$$

Заробітна плата розробника програмного забезпечення:

$$З_{зп} = t \cdot С_{пр}, \text{ грн.} \quad (6.12)$$

де t – загальна трудомісткість обробки програмного забезпечення;

$С_{пр}$ – середня годинна тарифна ставка програміста становить:

$С_{пр}$ = 69 грн./година.

Заробітна плата за розробку програмного забезпечення дорівнює:

$З_{зп}$ = 51,55 ·69 = 3556,95грн.

Вартість машинного часу, необхідного для налаштування програми на ЕОМ:

$$З_{мч} = t_{нал} \cdot С_{мг}, \text{ грн} \quad (6.13)$$

де:

$t_{отл}$ – трудомісткість налаштування програми на ЕОМ, людино-годин;

$С_{мг}$ – вартість машино-години ЕОМ, грн./година. $С_{мг}$ = 5 грн./година.

$З_{мч}$ = 5,7·5 = 28,5 грн.

Витрати на розробку програмного забезпечення системи керування будуть становити:

$К_{пз}$ = 3556,95+ 28,5= 3585,45грн.

Ці витрати на створення програмного забезпечення є частиною одноразових капітальних витрат на створення системи керування.

Очікувана тривалість розробки програмного забезпечення:

$$T = \frac{t}{B_к \cdot F_р}, \text{ міс} \quad (6.14)$$

де, $B_к$ – кількість розробників. Програма розроблялася однією людиною, тому $В_к$ = 1;

$F_р$ – місячний фонд робочого часу (Fр = 176 годин).

Визначимо тривалість розробки ПО:

$$T = \frac{51{,}55}{1 \cdot 176} = 0{,}29 \text{ міс}$$

Таким чином, капітальні витрати розраховані за формулою (6.1) дорівнюють:

$К_{пр}$ = 1150200 +80 514 +92 016 +3585,45= 1 326 315,45 грн.

4.3 Розрахунок річних експлуатаційних витрат

Експлуатаційні витрати визначаються за такими статтями витрат:

- амортизаційні відрахування (Са);
- заробітна плата обслуговуючого персоналу (Сзп);
- відрахування на соціальні заходи (Сс);
- витрати на технічне обслуговування і поточний ремонт обладнання (Сто);
- вартість спожитої електроенергії (Се)
- інші (Сі).

Таким чином, експлуатаційні витрати розраховуються за формулою:

$$С = С_а + С_{зп} + С_с + С_{то} + С_е + С_і \qquad (6.15)$$

Для розрахунку показників економічної ефективності необхідно розрахувати експлуатаційні витрати по проектному варіанту КС

4.3.1 Розрахунок амортизаційних відрахувань

Комп'ютерні системи відносяться до четвертої групи відповідно до класифікації груп основних засобів та інших необоротних активів. Для систем на базі комп'ютерної техніки мінімальний термін експлуатації становить 5 років. Амортизація визначається методом прискореного зменшення залишкової вартості.

Норма амортизації розраховується за формулою:

$$Ha = \frac{2}{T} \qquad (6.16)$$

де , Т – строк корисного використання КС.

$Ha = 2/5 = 0{,}4$

Таким чином, амортизаційні відрахування по обладнанню, будуть визначаться по формулі 6.17:

$$С_а = К_{пр} \cdot Н_а, \text{ грн.} \quad (6.17)$$

Амортизаційні відрахування (за перший рік експлуатації) для апаратного забезпечення системи становитимуть:

Са.п = 9508,93*0,4= = 1 326 315,45 грн.

Існуючої системи немає.

4.3.2 Розрахунок річного фонду заробітної плати

Розрахунок річного фонду заробітної плати обслуговуючого персоналу, згідно форми, наведено в таблиці 6.2.

«Адміністративний відділ» університету має в своєму складі 4 працівників які дбають про мережу та начальник відділу. Робочій день має тривалість 8 годин.

Номінальний річний фонд робочого часу одного працівника визначається за формулою 6.5.

$$F_{ном} = (Т_к - Т_{пр} - Т_{вих} - Т_{відп}) * Т_{см}, \text{ годин} \quad (6.5)$$

Номінальний річний фонд робочого часу працівника:

$F_{ном}$=(365-9-104-21)*8=1848 годин

Номінальний річний фонд робочого часу керівника відділу:

$F_{ном}$=(365-9-104-28)*8=1792 годин

Таблиця 1.1 – Річний фонд заробітної плати

№ п/п	Найменування професії працівників	Кількість працюючих, люд.	Годинна тарифна ставка, грн	Номінальний річний фонд	Всього пряма заробітна плата,	Додаткова заробітна плата	Доплати (7%)	Всього заробітна плата, грн.

		явочне	списочне						
1	2	3	4	5	6	7	8	9	10
Існуючий варіант									
1	Працівник	3	3	50	1848	277200	27720	19404	324324
2	Керівник	1	1	60	1792	107520	10752	7526,4	125798,4
Всього									450122,4
Проектний варіант									
4	Працівник	3	3	50	1848	277200	27720	19404	324324
5	Керівник	1	1	60	1792	107520	10752	7526,4	125798,4
Всього									450122,4

4.3.3 Розрахунок відрахувань на соціальні заходи

Відрахування на соціальні заходи становлять 22% від заробітної плати (формула 4.19):

$$C_c = C_{зп} * 22\%, \text{ грн.} \qquad (4.19)$$

Сс.і=450122,4 *0,22=99026,93 грн.

Сс.п=450122,4*0,22= 99026,93 грн.

4.3.4 Визначення річних витрат на технічне обслуговування і поточний ремонт

Витрати на технічне обслуговування і поточний ремонт включають витрати на матеріали, запасні частини, заробітну плату ремонтним робітником. Вони складають 20% від капітальних витрат:

$$C_{тр} = K_{пр} * 20\%, \text{ грн.} \quad (6.20)$$

Сто.п=$К_{пр}$*0,2=1 326 315,45 *0,2= 26 526,309 грн.

4.3.5 Розрахунок вартості споживаної електроенергії

Вартість спожитої електроенергії визначається за формулою:

$$C_е = M * F_p * а, \text{ грн,} \quad (6.21)$$

де М – встановлена потужність апаратури,

F_p – річний фонд робочого часу апаратури (2 920 годин – обладнання працює 8 годин на добу),

а – тариф на електроенергію для підприємств (на передачу 1,5540 грн/КВт·ч, на послуги диспетчерського управління – 0,1023 грн/КВт·ч, а= 1,5563 грн).

Сумарна споживана потужність принтера складе 100 Вт. Споживання електроенергії одним персональним комп'ютером (близько 200 шт) по 300 Вт. Споживання електроенергії маршрутизатором (3 шт) – 150 Вт. Разом – 120 550 Вт (60,55 Квт).

Се.п=60,55*2920*1,5563= 275 163,8грн.

4.3.6 Визначення інших витрат

Інші витрати по експлуатації об'єкта проектування включають витрати на навчання персоналу підприємства обслуговування нового обладнання, з охорони праці, придбання спец одягу та ін. Ці витрати складають 4% від річного фонду заробітної плати обслуговуючого персоналу.

$$C_і = C_{зп} * 4\%, \text{ грн.} \quad (6.22)$$

Сі.п = 450122,4 ·0,04= 18004,9 грн.

Сі.і = 450122,4 ·0,04= 18004,9 грн.

Відповідно до формули 4.15 експлуатаційні витрати для КС складуть:

Сп=578085,64 грн.

Сі=656124,68грн.

4.4 Визначення та аналіз показників економічної ефективності проекту

Результати розрахунків експлуатаційних витрат по проектованому і існуючому варіантам зведені в табл. 6.3.

Таблиця 6.3 – Річні експлуатаційні витрати

Найменування показника	Проектний варіант	Існуючий варіант
Амортизація	1 326 315,45	652 800
Фонд заробітної плати	450 122,4	650 000
Відрахування на соц. виплати	99 026,93	99 026,93
Ремонт і тех.обслуговування	26 526,309	2 226 400
Електроенергія	275 163	227 700
Інші	580 000	580 000
Разом	2 757 154,089	4 435 926,93

Річна економія на експлуатаційних витратах становить:

$$\Delta C = Сі - Сп, \quad (6.23)$$

ΔС = 4 435 926,93–2 757 154,089=1 678 772,841грн.

Термін окупності (Тр) проектованої системи:

$$T_р = К_{пр}/ \Delta C, \text{ лет} \quad (6.24)$$

Тр =1 326 315,45 /1 678 772,841= 0,79 года

Отже, капітальні витрати на впровадження проектної системи окупляться через 0,79 року.

Коефіцієнт ефективності капітальних витрат визначається за формулою:

Кэфф =1/ Тр, грн. (6.25)

$К_{эфф}$ =1/0,79= 1,3 грн

Отже, на 1 грн. капітальних витрат припадає 1,3 грн. прибутку

Висновок

Удосконалення комп'ютерної системи університету з опрацюванням побудови, налаштування та безпеки корпоративної мережі доцільно, так як при капітальних витратах в 1 326 315,45 грн., капіталовкладення окупляться через 0,79 року. Коефіцієнт ефективності капітальних витрат дорівнює 1,3 грн. при мінімальному терміні експлуатації в 5 років.

5 ОХОРОНА ПРАЦІ

5.1 Фактори, що впливають на функціональний стан програміста

Трудовий процес суттєво впливає на психофізіологічні можливості користувачів комп'ютерів, оскільки їх діяльність характеризується значними статичними фізичними навантаженнями; недостатньою руховою активністю; напруженнями сенсорного апарату, вищих нервових центрів, які забезпечують функції уваги, мислення, регуляції рухів. Окрім того, трудовий процес користувачів комп'ютерів відзначається значними інформаційними навантаженнями.

Трудова діяльність користувачів комп'ютерів відбувається у певному виробничому середовищі, яке впливає на їх функціональний стан. Найбільш значимі – фізичні фактори виробничого середовища, до яких належать електромагнітні хвилі різних частотних діапазонів, електростатичні поля, шум, параметри мікроклімату та ціла низка світлотехнічних показників.

Вплив хімічних та, особливо, біологічних факторів виробничого середовища на користувачів комп'ютерів – значно менший.

Сучасна професія користувача візуальних дисплейних терміналів (ВДТ) належить до розумової праці, яка характеризується: високою напруженістю зорових функцій; одноманітною позою; великою кількістю стереотипних високо координованих рухів, що виконуються лише м'язами кистей рук на фоні малої загальної рухової активності; значним нервово-емоційним компонентом, особливо в умовах дефіциту часу; роботою з великими масивами інформації, що викликає активізацію уваги та інших вищих психічних функцій. Крім того, при роботі з дисплеями на електронно-променевих трубках виникає вплив на користувача цілої низки факторів фізичної природи – електростатичні поля, радіочастотне та рентгенівське випромінювання тощо. Діяльність професіоналів можна поділити на три групи:

– діяльність, яка пов'язана з виконанням нескладних багаторазово повторюваних операцій, що не вимагають великого розумового напруження;

– діяльність, яка пов'язана із здійсненням логічних операцій, що постійно повторюються;

– діяльність, коли в процесі роботи необхідно приймати рішення за відсутності заздалегідь відомого алгоритму.

Інформаційне перевантаження користувачів ВДТ супроводжується низкою специфічних захворювань, які називають інформаційними.

Дослідження, показали, що робота з обслуговування ВДТ супроводжується підвищеним напруженням зору, інтенсивністю і монотонністю праці, збільшенням статичних навантажень, нервово-психічним напруженням, впливом різного виду випромінювань та ін.

Внаслідок цього серед операторів ВДТ, як зазначають фахівці Всесвітньої організації охорони здоров'я, частіше, ніж в інших групах працюючих, трапляються такі професійні захворювання, як передчасна стомлюваність, погіршення зору, м'язові і головні болі, психічні й нервові розлади, хвороби серцево-судинної системи, онкологічні захворювання та ін. Вважається, що стан організму операторів ВДТ визначається комплексним впливом факторів трудового процесу і середовища, значення яких є неоднаковим.

5.2 Вимоги до організації робочих міст

Організація робочого місця оператора повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСанПіН 3.3.2.007-98

Відстань від екрана до ока працівника визначається згідно з вимогами.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана ВДТ, зручність ручного керування пристроєм введення-виведення інформації в

зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98 (v0007282-98).

Під матричні принтери потрібно підкладати вібраційні килимки для гасіння вібрації та шуму.

За потреби особливої концентрації уваги під час виконання робіт суміжні робочі місця операторів необхідно відділяти одне від одного перегородками висотою 1,5 - 2 м.

При організації робочого місця, яке передбачає роботу з ЕОМ з ВДТ і ПП для керування технологічним обладнанням (станки з програмним управлінням, роботизовані технологічні комплекси, обладнання для гнучкого автоматизованого виробництва тощо), слід передбачати: достатній простір для оператора ЕОМ з ВДТ і ПП; вільну досяжність органів ручного керування в зоні моторного поля (відстань по висоті - 900-1330 мм, по глибині - 400-500 мм); розташування екрана ВДТ у робочій зоні, яке буде забезпечувати зручність зорового спостереження у вертикальній площині під кутом +-30 □ від лінії зору оператора, а також зручність використання ВДТ під час коригування керуючих про- грам одночасно з виконанням основних виробничих операцій; можливість повертання екрана ВДТ навколо горизонтальної та вертикальної вісей.

5.3 Вимоги до електробезпеки

З метою запобігання ушкодженням, що можуть статися через ураження електричним струмом, загоряння, коротке замикання тощо, розроблено загальний стандарт безпеки IEC 950. Загальним стандартом електробезпечності для країн Європейської співдружності є Cemark.

Приміщення із робочими місцями користувачів комп’ютерів для забезпечення електробезпеки обладнання, а також для захисту від ураження електричним струмом самих користувачів ПК повинні мати достатні технічні засоби захисту відповідно до НПАОП 40.1-1.07-01 “Правила експлуатації електрозахисних засобів”, НПАОП 40.1-1.21-98 “Правила безпечної

експлуатації електроустановок споживачів”, НПАОП 40.1-1.32-01 “Правила будови електроустановок. Електрообладнання спеціальних установок”

ЕОМ, периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ, інше устаткування (апарати управління, контрольно-вимірювальні прилади, світильники тощо), електропроводи та кабелі за виконанням та ступенем захисту мають відповідати класу зони за ПУЕ, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів.

Під час монтажу та експлуатації ліній електромережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, перейти на негорючу ізоляцію.

Лінія електромережі для живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ виконується як окрема групова трипровідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів.

Використання нульового робочого провідника як нульового захисного провідника забороняється. Нульовий захисний провід прокладається від стійки групового розподільчого щита, розподільчого пункту до розеток живлення. Не допускається підключення на щиті до одного контактного затискача нульового робочого та нульового захисного провідників. Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі повинна бути не менше площі перерізу фазового провідника.

У приміщенні, де одночасно експлуатується або обслуговується більше п'яти персональних ЕОМ, на помітному та доступному місці встановлюється

аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

Усі провідники повинні відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам ПУЕ.

ПЕОМ, периферійні пристрої ПЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ повинні підключатися до електромережі тільки з допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників повинні мати спеціальні контакти для підключення нульового захисного провідника. Конструкція їх має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Необхідно унеможливити з'єднання контактів фазових провідників з контактами нульового захисного провідника.

Неприпустимим є підключення ПЕОМ та периферійних пристроїв ПЕОМ до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв.

Індивідуальні та групові штепсельні з'єднання та електророзетки необхідно монтувати на негорючих або важкогорючих пластинах з урахуванням вимог ПУЕ та Правил пожежної безпеки в Україні.

Електромережі штепсельних з'єднань та електророзеток для живлення ПЕОМ, периферійних пристроїв слід виконувати за магістральною схемою, по 3…6 з’єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 36 В за своєю конструкцією повинні відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В і мають бути пофарбовані в колір, який візуально значно відрізняється від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

Електромережу штепсельних розеток для живлення ПЕОМ, периферійних пристроїв ПЕОМ при розташуванні їх уздовж стін приміщення прокладають по підлозі поряд зі стінами приміщення, як правило, в металевих трубах і гнучких металевих рукавах з відводами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання.

При розташуванні в приміщенні за його периметром до 5 ПЕОМ, використанні трипровідникового захищеного проводу або кабелю в оболонці з негорючого або важкогорючого матеріалу дозволяється прокладання їх без металевих труб та гнучких металевих рукавів.

Електромережу штепсельних розеток для живлення ПЕОМ при розташуванні їх у центрі приміщення, прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах. При цьому не дозволяється застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, що містять сірку.
Відкрита прокладка кабелів під підлогою забороняється. Металеві труби та гнучкі металеві рукави повинні бути заземлені. Заземлення повинно відповідати вимогам НПАОП 40.1-1.21-98.

Є неприпустимими:

– експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;

– застосування саморобних подовжувачів, які не відповідають вимогам ПВЕ до переносних електропроводок;

– застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;

– користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;

– підвішування світильників безпосередньо на струмопровідних проводах, обгортання електроламп і світильників папером, тканиною та іншими горючими матеріалами, експлуатація їх зі знятими ковпаками (розсіювачами);

– використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

Для підключення переносної електроапаратури застосовують гнучкі проводи в надійній ізоляції.

Тимчасова електропроводка від переносних приладів до джерел живлення виконується найкоротшим шляхом без заплутування проводів у конструкціях машин, приладів та меблях. Доточувати проводи можна тільки шляхом паяння з наступним старанним ізолюванням місць з'єднання.

5.4 Перша допомога при ураженні електричним струмом

Основною умовою успішного надання першої допомоги при ураженні електричним струмом є швидка та правильна дія тих, хто надає допомогу. В той же час зволікання, запізніле та некваліфіковане надання допомоги може призвести до смерті потерпілого. Ось чому важливо, щоб кожен знав і вмів правильно та швидко надати необхідну допомогу потерпілому.

Перша допомога при ураженні електричним струмом складається з двох етапів: звільнення потерпілого від дії електричного струму; надання йому необхідної долікарської допомоги.

При ураженні електричним струмом необхідно, перш за все, негайно звільнити потерпілого від дії струму, оскільки від тривалості такої дії суттєво залежить важкість електротравми. Необхідно пам'ятати, що діяти треба швидко, але в той же час обережно, щоб самому не потрапити під напругу. Найбезпечніший спосіб звільнення потерпілого від дії електричного струму - це вимкнення електроустановки, до якої доторкається потерпілий, за

допомогою найближчого вимикача, рубильника чи іншого апарата для знеструмлення.

Способи звільнення потерпілого від дії електричного струму:

– знеструмлення установки за допомогою вимикача (рубильника);

– відкидання проводу сухою палицею;

– перерубування проводів сокирою;

– відтягнення потерпілого від електромережі.

Якщо вимкнути установку досить швидко немає змоги, то необхідно звільнити потерпілого від струмовідних частин, до яких він доторкається.

Для звільнення потерпілого від струмовідних частин або проводу напругою до 1000 В необхідно скористатись палицею, дошкою або будь-яким іншим сухим предметом, що не проводить електричний струм.

При цьому бажано ізолювати себе від землі (стати на суху дошку, неструмопровідну підстилку). Можна також перерубати проводи сокирою з сухим дерев'яним топорищем або перекусити їх інструментом з ізолювальними рукоятками (кусачками, пасатижами тощо). Перерубувати чи перекусувати проводи необхідно пофазно, тобто кожен провід окремо, та на різній висоті.

Для звільнення потерпілого від струмовідних частин можна також відтягнути його за одяг (якщо він сухий і відстає від тіла), наприклад, за поли халата чи піджака. При цьому необхідно уникати доторкання до навколишніх металевих предметів та відкритих частин тіла. Для ізоляції рук, особливо коли необхідно доторкнутися до тіла потерпілого, рятівник повинен надягнути діелектричні рукавички або обмотати руку сухим одягом (наприклад, шаликом або сухою тканиною). Відтягувати потерпілого від струмопровідних ділянок рекомендується однією рукою.

Якщо електричний струм проходить у землю через потерпілого і він судомно стискає у руці один струмопровідний елемент (наприклад, провід), то простіше припинити дію струму, відокремивши потерпілого від землі

(підсунувши під нього суху дошку або відтягнувши ноги від землі мотузкою, чи за сухі штани). При цьому необхідно пам'ятати про власну безпеку.

Для звільнення потерпілого від струмовідних частин та проводів, що знаходяться під напругою понад 1000 В, необхідно надягнути діелектричні рукавички та боти і діяти ізолювальною штангою або кліщами, що розраховані на відповідну напругу. При цьому необхідно пам'ятати про небезпеку крокової напруги, якщо провід лежить на землі.

5.5 Пожежна безпека

Пожежі у обчислювальних центрах (ОЦ) становлять особливу небезпеку, тому що пов'язані з великими матеріальними втратами. Характерна особливість ОЦ - невеликі площі приміщень. Як відомо пожежа може виникнути при взаємодії горючих речовин, окислення і джерел запалювання. У приміщеннях ОЦ присутні всі три основні чинника, необхідні для виникнення пожежі.

Горючими компонентами на ОЦ є: матеріали для акустичної і естетичної обробки приміщень, перегородки, двері, підлоги, перфокарти і перфострічки, ізоляція кабелів і ін..

Протипожежний захист - це комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, запобігання пожежі, обмеження її розповсюдження, а також на створення умов для успішного гасіння пожежі.

Джерелами запалювання у ОЦ можуть бути електронні схеми від ЕОМ, прилади, застосовувані для технічного обслуговування, пристрої електроживлення, кондиціонування повітря, де внаслідок різних порушень утворюються перегріті елементи, електричні іскри та дуги, здатні викликати загоряння горючих матеріалів.

У сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються сполучні дроти, кабелі. При протіканні по них електричного

струму виділяється значна кількість теплоти. При цьому можливо оплавлення ізоляції. Для відведення надлишкової теплоти від ЕОМ служать системи вентиляції та кондиціонування повітря. При постійному дії ці системи представляють собою додаткову пожежну небезпеку.

Енергопостачання ОЦ здійснюється від трансформаторної станції і двигун-генераторних агрегатів. На трасформаторних підстанціях особливу небезпеку представляють трансформатори з масляним охолодженням. У зв'язку з цим перевагуслід віддавати сухим транформатором.

Пожежна небезпека двигун-генераторних агрегатів обумовлена можливістю коротких замикань, перевантаження, електричного іскріння. Для безпечної роботи необхідний правильний розрахунок і вибір апаратів захисту. При поведінці обслуговуючих, ремонтних і профілактичних робіт використовуються різні мастильні речовини, легкозаймисті рідини, прокладаються тимчасові електропровідниками, ведуть пайку та чистку окремих вузлів. Виникає додаткова пожежна небезпека, яка потребує додаткових заходів пожежного захисту. Зокрема, при роботі з паяльником слід використовувати неспалену підставку з нескладними пристроями для зменшення споживаної потужності в неробочому стані.

Для більшості приміщень ОЦ встановлена II категорія пожежної небезпеки В.

Однією з найбільш важливих завдань пожежної захисту є захист будівельних приміщень від руйнувань та забезпечення їх достатньої міцності в умовах впливу високих температур при пожежі. З огляду на високу вартість електронногоустаткування ОЦ, а також категорію його пожежної небезпеки, будинки для ОЦ і частини будинку іншого призначення, в яких передбачено розміщення ЕОМ повинні бути 1 і 2 ступеня вогнестійкості.

Для виготовлення будівельних конструкцій використовуються, як правило, цегла, залізобетон, скло, метал та інші негорючі матеріали. Застосування дерева повинна бути обмежено, а в разі використання необхідно просочувати його вогнезахисними складами. У ОЦ протипожежні

перешкоди у вигляді перегородок з негорючих матеріалів встановлюють між машинними залами.

До засобів гасіння пожежі, призначених для локалізації невеликих загранй, відносяться пожежні стовбури, внутрішні пожежні водопроводи, вогнегасники, сухий пісок, азбестові ковдри і т. п.

У будинках ОЦ пожежні крани встановлюються в коридорах, на майданчиках сходових клітин та входів. Вода використовується для гасіння пожеж у приміщеннях програмістів, бібліотеках, допоміжних і службових приміщеннях. Застосування води в машинних залах ЕОМ, сховищах носіїв інформації, приміщеннях контрольно-вимірювальних приладів, зважаючи на небезпеку пошкодження або повного виходу з ладу дорогого устаткування можливо у виняткових випадках, коли пожежа приймає загрозливо великі розміри. При цьому кількість води повинна бути мінімальною, а пристрої ЕОМ необхідно захистити від попадання води, накриваючи їх брезентом або полотном.

Для гасіння пожеж на початкових стадіях широко застосовуються вогнегасники. По виду використовуваного вогнегасної речовини вогнегасники поділяються на такі основні групи.

Пінні вогнегасники, застосовуються для гасіння палаючих рідин, різних матеріалів, конструктивних елементів і устаткування, крім електрообладнання, що знаходиться під напругою.

Газові вогнегасники застосовуються для гасіння рідких і твердих речовин, а також електроустановок, що знаходяться під напругою.

Для виявлення стадії загоряння та оповіщення службу пожежної охорони використовують системи автоматичної пожежної сигналізації (АПС). Крім того, вони можуть самостійно забезпечувати дію установки пожежогасіння, коли пожежа ще не досяг великих розмірів. Системи АПС складаються з пожежних сповіщувачів, ліній зв'язку і прийомних пультів (станцій).

Ефективність застосування систем АПС визначається правильним вибором типу сповіщувачів та місць їх встановлення. При виборі пожежних

сповіщувачів необхідно враховувати конкретні умови їхньої експлуатації: особливості приміщення і повітряного середовища, наявність пожежних матеріалів, характер можливого горіння, специфіку технологічного процесу і т.п.

Відповідно до "Типових правил пожежної безпеки для промислових підприємств" зали ЕОМ, приміщення для зовнішніх запам'ятовуючих пристроїв, підготовки даних, сервісної апаратури, архівів, копіювально-розмножувального устаткування і т.п. необхідно обладнати димовими пожежними сповіщувачами.

ВИСНОВОК

В рамках дипломної роботи мною було розроблено мережу для університету " НГУ".

Топології мережі було обрано такі: "зірка" на центральному та розподільчому рівні, та "кільце" на рівні розподілу та доступу Так як в мережі використовується топологія "кільце" необхідно було прийняти міри, для того щоб широкомовна розсилка пакетів не займала всю пропускну здатність каналу передачі даних. З цією проблемою було вирішено боротися за допомогою протоколу STP, котрий виявляє кільця у мережі.

На центральному рівні було обрано два маршрутизаторі, котрі забезпечать рівномірний доступ до мережі Інтернет, один для перших двох поверхів, другий для поверхів, в котрих розташовуються студенти та викладачі, також він забезпечує достатньою пропускною смугою технологію VoIP. За допомоги blockchain буде прискоренно процесс навчання студентів та поліпшення обміну данних.

У програмі імітаційного моделювання Packet Tracer було розроблено повністю функціональну модель університету. Були впроваджені такі технології, як: VoIP, DHCP, OSPF, BGP, RIP, ACL, DNS,VLAN.

ЛІТЕРАТУРА

1.Олифер В. Г., Олифер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи. Підручник для вузів. Спб. Питер 2006. 958с.

2. Документація з настройки обладнання фірми Cisco. http://www.cisco.com
3. Виденье отказоустойчивой, надежной, масштабируемой сети передачи данных -2010 - http://habrahabr.ru/blogs/personal/93629/
4. Новиков Ю. В., Кондратенко С. В. «Локальні мережі: архітектура, алгоритми, проектування.» - М.: Видавництво ЭКОМ, 2000
5. https://nplus1.ru/material/2020/02/21/course-blockchain
6. https://ru.euronews.com/2018/09/07/blockchain-long-read-ru

ДОДАТОК А

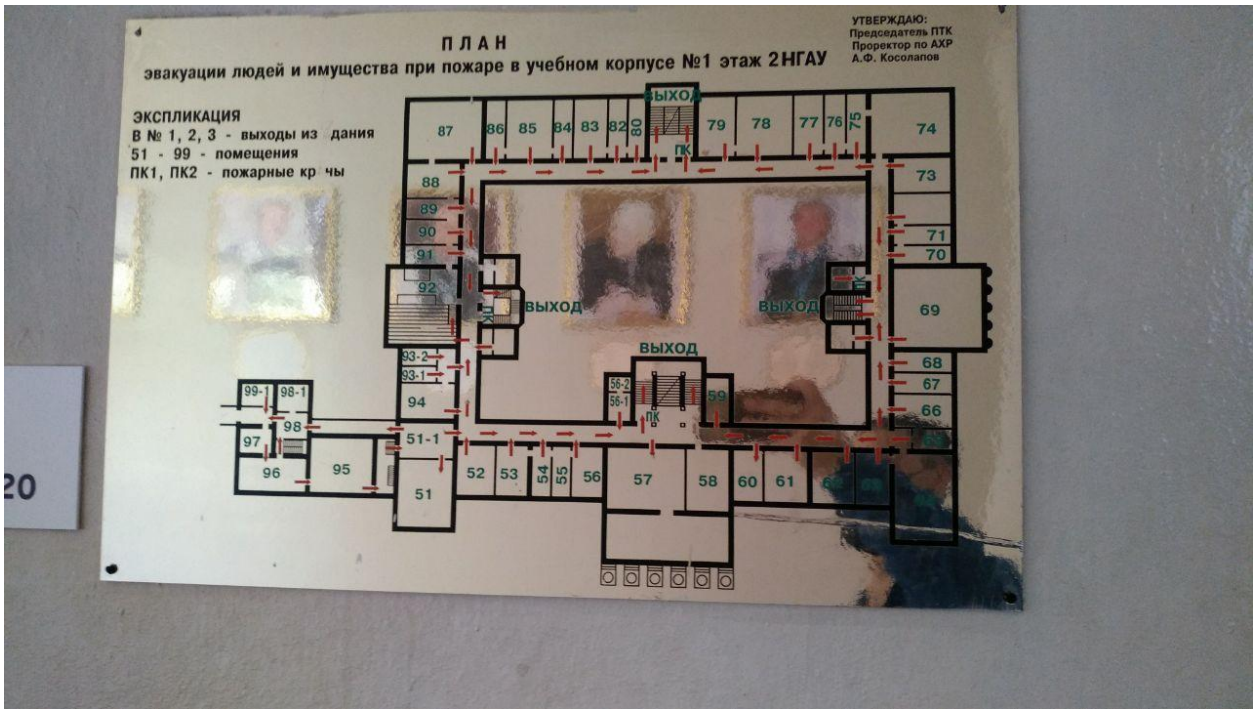
Загальний вигляд

ДОДАТОК Б

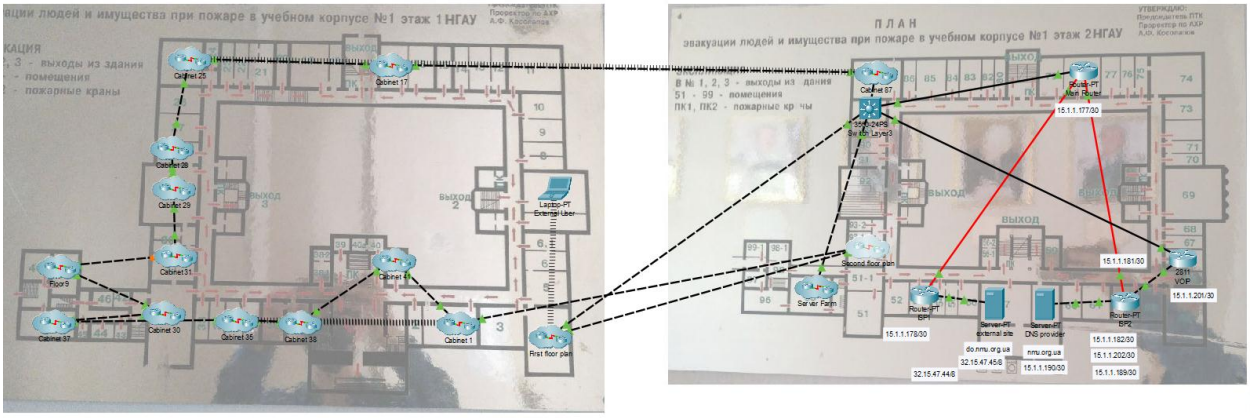
План розташування на карті

ДОДАТОК Б

План розташування мережевого обладнання на другому поверсі



ДОДАТОК В



Логічна схема мережі.

ДОДАТОК В.1

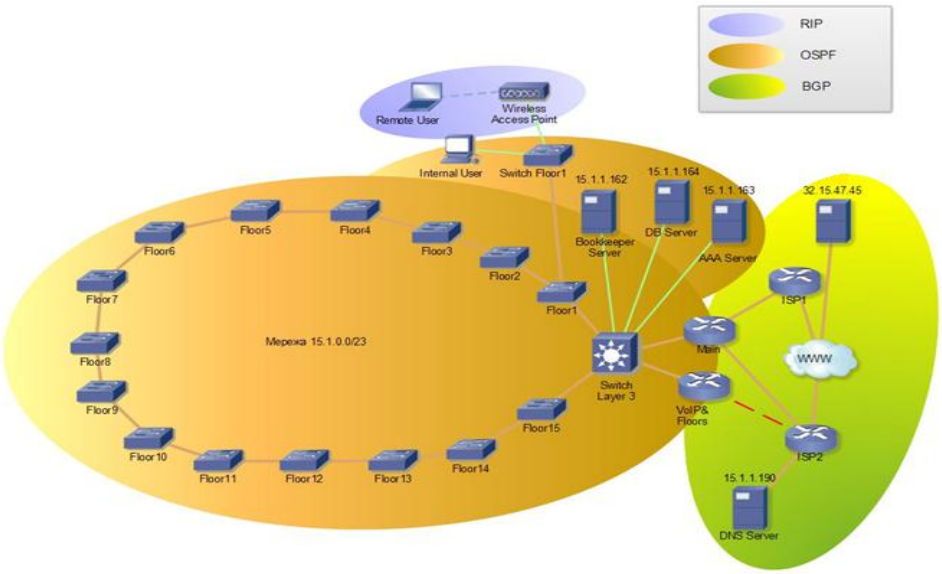


Схема зон використання протоколів маршрутизації у мережі та за його межами.

ДОДАТОК Г

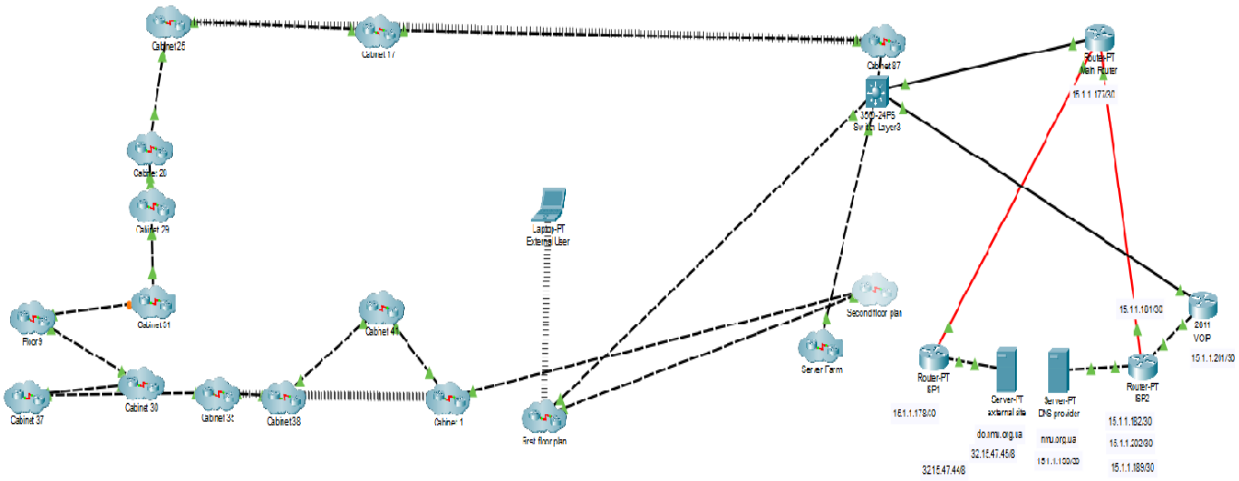


Схема мережі створенна у програмі Cisco