МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКАРЇНИ
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

ГОРАЙСЬКИЙ Руслан Володимирович

Корпоративна мережа підприємства на основі технології VLAN засобами Cisco Packet Tracer / Enterprise corporate network based on VLAN technology with Cisco Packet Tracer

Спеціальність: 123 – Комп'ютерна інженерія
Освітньо-професійна програма – Комп'ютерна інженерія

Випускна кваліфікаційна робота

Виконав: студент групи КСМ-43/2
Руслан Володимирович Горайський

Науковий керівник
Вербовий С.О.

ТЕРНОПІЛЬ 2019

РЕЗЮМЕ

Бакалаврська робота містить 72 сторінки пояснюючої записки, 8 рисунків, 5 таблиць, 3 додатки. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою бакалаврської роботи є проектування комп'ютерної мережі підприємства на основі технології VLAN засобами Cisco Packet Tracer.

Методи дослідження включають методи фізичної і логічної структуризації комп'ютерних мереж, методи структурного програмування, теорія графів, елементи математичної логіки.

Виконано аналіз існуючої мережі, в ході якого було вирішено вибрати технологію VLAN. Проведено теоретичне ознайомлення з технологією VLAN, можливості реалізації, тенденції розвитку, його переваги та недоліки. Була побудована функціональна модель корпоративної мережі програмі Cisco Packet Tracer, де були використані образи справжнього обладнання. Проведено конфігурацію клієнтських маршрутизаторів, а саме налаштовано протокол маршрутизації з клієнтом. Налаштовано EIGRP всередині мережі провайдера, в якості протоколу маршрутизації для VLAN; налаштовано Рег- VLAN Spanning Tree (PVST), що призначений для роботи з декількома VLAN.

Ключові слова: БЕЗПРОВІДНА КОМП'ЮТЕРНА МЕРЕЖА, VLAN, SRANNING TREE, НАДІЙНІСТЬ.

RESUME

The bachelor's thesis contains 66 pages of explanatory note, 8 figures, 5 tables, 3 appendices. Volume of graphic material 2 sheets of A3 format.

The purpose of the bachelor's thesis is to design an enterprise computer network based on VLAN technology using Cisco Packet Tracer.

Research methods include methods of physical and logical structuring of computer networks, methods of structural programming, graph theory, elements of mathematical logic.

An analysis of the existing network was performed, during which it was decided to choose VLAN technology. Theoretical acquaintance with VLAN technology, possibilities of realization, development tendencies, its advantages and disadvantages is carried out. A functional model of the corporate network was built for the Cisso Rasket Tracer program, where images of real equipment were used. The client routers are configured, namely the routing protocol with the client is configured. Configured EIGRP within the provider's network, as a routing protocol for VLAN; Configured VLAN Sranning Tree, which is designed to work with multiple VLANs.

Keywords: WIRELESS COMPUTER NETWORK, VLAN, SRANNING TREE, RELIABILITY.

ЗМІСТ

Вступ 9
1 Аналіз корпоративних мереж 11
1.1 Корпоративна мережа 11
1.2 Види корпоративних мереж 13
1.3 Етапи створення корпоративної мережі 18
1.4 Структура корпоративної мережі 21
1.5 Постановка задачі 26
2 Проектування архітектури мережі 28
2.1 Рівнева архітектура мереж CISCO 28
2.2 Моделювання мережі в Cisco Packet Tracer 31
2.3 Захист корпоративної мережі 34
3 Моделювання комп'ютерної мережі 41
3.1 Налаштування комутаторів 41
3.2 Налаштування маршрутизаторів 42
3.3 Налаштування робочих станцій 44
3.4 Організація безпеки комутаторів та маршрутизаторів 46
3.5 Перевірка працездатності мережі 47
4 Техніко-економічний розділ 50
4.1 Визначення витрат на оплату праці та відрахувань на соціальні заходи 50
4.2 Розрахунок ціни проекту 57
4.3 Визначення економічної ефективності і терміну окупності капітальних вкладень 58
Висновки 60
Список використаних джерел 60
Додаток А Конфігурація комутаторів PTMV 1, VTMV1 та VTMV 2**Ошибка! Закладка**
Додаток Б Таблиці IP-адресації ..... **Ошибка! Закладка не определена.**
Додаток В Схема мережі підприємства. Схема структурна 72
Додаток Г ..... **Ошибка! Закладка не определена.**
Довідка про використання ..... **Ошибка! Закладка не определена.**

ВСТУП

Сьогодні все навколо нас так чи інакше пов’язане з комп’ютерами, телефонами, планшетами і т.д.. В кожного у власності є хоча б один подібний пристрій, який може працювати у всесвітній мережі Інтернет. Понад 80% з них об’єднанні в мережі інформаційно-обчислювального характеру, від маленьких локальних мереж, до глобальних (як сама мережа Інтернет).

Сучасні технології дозволяють обмінюватись інформацією з двох максимально віддалених одна від одної точок земної кулі на великих швидкостях, навіть не помічаючи ніяких затримок в передачі даних.

Такі технології криють в собі величезний потенціал, який при цьому відчуває інформаційний комплекс, і значний стрибок усього виробничого процесу не дозволяють нам не приймати це до уваги і не застосовувати їх на практиці. І цей потенціал активно почали використовувати як світові лідери в сфері послуг, так і малий та середній бізнеси.

Кожна компанія — це група певних елементів, що належать внутрішній структурі, які щосекунди взаємодіють між собою і будь-якому з елементів властива та чи інша особливість. Ці елементи (підрозділи) функціонально зв’язані між собою, вони виконують певого роду задачі в межах одного бізнес процесу та інформаційно пов’язані, обмінюються усними і письмовими розпорядженнями, документами, файлами і так далі. Крім того, такі елементи обов’язково контактують з певними системами ззовні, дотого ж, цей контакт може бути як функціональним, так і інформаційним.

По мірі розвитку і зростання організації, в її керівництва рано чи пізно виникають наступні питання: як запровадити максимально ефективну і гнучку систему управління поточними підрозділами? Як забезпечити хорошу якість і надійність зв’язку між головним офісом і всіма філіями чи підрозділами,

проводити конфіденційну передачу даних, знизити витрати на телекомунікаційне забезпечення, затрачувати менше часу на збір звітів, вчасно обробляти великі потоки інформації, що циркулюють між підрозділами?

Зараз, в умовах величезних потоках інформації, які ростуть з кожним роком, вже майже неможливо уявити собі точну взаємодію банківських структур, фірм, що займаються торгівлею, державних установ та інших підприємств, без сучасних комп'ютерних мереж і обчислювальної техніки. В іншому випадку потрібно було б наймати безліч працівників для обробки документів в паперовому вигляді та кур'єрів, при цьому надійність та швидкодія такої системи так чи інакше була б далекою від ідеалу. Тому що кожна запинка в передачі важливої інформації може перетворитись у чималі грошові затрати і іміджеві крахи.

Кінцевою метою використання таких мереж на підприємстві є збільшення ефективності його роботи, для прикладу, зростання доходів підприємства.

Для побудови мережі подібного масштабу потрібно ретельно підібрати обладнання, його налаштування, гнучкість та здатність до модернізації. Тому, для реалізації проекту потрібна модель, щоб його спроектувати. Вибір падає на всім відому програму Cisco Packet Tracer. Її інструменти можуть задовольнити всі потреби в процесі моделювання мережі та, навіть, в подальшому розширенні. Перевагою вибору є також і те, що програма хоч і безкоштовна, але досить гнучка та варіативна в плані проектування.

Метою бакалаврської роботи є проектування комп'ютерної мережі для офісу підприємства.

У процесі виконання буде складено та розроблено структурну схему, фізичну й логічну топологію, схему з'єднань й IP - адресації цієї мережі. Також буде здійснено конфігурування пристроїв та моделювання роботи мережі у середовищі Cisco Packet Tracer.

1 АНАЛІЗ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Корпоративна мережа

В даний час в діяльності майже кожного підприємства важливу роль відіграє розробка комп'ютерної мережі, тому з її допомогою здійснюється зв'язок як між працівниками всередині офісу (підприємства, будівлі), так і в рамках міжрайонного, міжміського або навіть міжнародного сполучення. Ефективне управління підприємством неможливо без безперервного відстеження інформаційних потоків, без оперативної координації діяльності всіх підрозділів і співробітників.

Корпоративна мережа (КМ) — це мережа, яка існує для підтримки роботи певного підприємства, яке володіє даною мережею. Користувачами корпоративної мережі є тільки працівники цього підприємства. Корпоративні мережі, як правило, не надають послуг стороннім організаціям чи користувачам, як, наприклад, оператори зв’язку. Залежно від розмірів підприємства, а також від складності і різновидності вирішуваних завдань розрізняють мережі відділу, мережі кампусів і корпоративні мережі.

Комп’ютерні мережі є варіантом співпраці людей і комп’ютерів, вони забезпечують прискорення доставки та обробки інформації. Об’єднувати комп’ютери в мережі почали більше 30 років тому. Коли можливості комп’ютерів виросли і ПК стали доступні кожному, розвиток мереж значно прискорився.

Сучасні мережі можна класифікувати за різними ознаками: по віддаленості комп’ютерів, топології, призначенню, переліку послуг, принципами управління, методами комутації, методами доступу, видами середовища передачі, швидкостями передачі даних.

Концептуальною перевагою корпоративних мереж є здатність виконувати паралельні обчислення. За рахунок цього в системі з декількома оброблювальними вузлами в принципі може бути досягнута продуктивність, що перевищує максимально можливу на даний момент продуктивність будь-якого окремого, скільки завгодно могутнього процесора.

Узагальнену схему КМ представлено на рисунку 1.1.

Рисунок 1.1 — Узагальнена схема корпоративної мережі

Для користувача розподілені системи дають такі переваги, як можливість сумісного використання даних і пристроїв, а також можливість гнучкого розподілу робіт по всій системі. Подібне розділення дорогих периферійних пристроїв, таких як дискові масиви великої ємкості, кольорові принтери, графічні пристрої, модеми, оптичні диски, у багатьох випадках є основною причиною розгортання мережі на підприємстві.

В умовах жорсткої конкурентної боротьби в будь-якому секторі ринку виграє, в кінці кінців, та компанія, співробітники якої можуть швидко і

правильно відповісти на будь-яке питання клієнта — про можливості їх продукції, про умови її застосування, про вирішення будь-яких можливих проблем і тому подібне.

1.2 Види корпоративних мереж

Мережа кампусів (CAN — Campus Area Network) — це група деяких локальних мереж, розміщених на відносно невеликій території (кампусі) будь-якої організації, які обслуговують лише цю організацію — підприємство, офіси, порт, університет, оптові склади, державної установи і т.д.. В такому випадку все мережеве обладнання (маршрутизатори, комутатори) і середовище передачі даних (оптичне волокно, мідний завод, Cat5 кабелі та ін.) є власністю орендаря чи власника кампусу, університету, підприємства, державної установи і так далі.

Кампусна мережа (CAN) — це просто велика багатосегментна локальна мережа, розміщена на території до декількох кілометрів в діаметрі і яка об’єднує між собою локальні мережі будівель, які близько розташовані між собою. Одними з перших, хто впровадив використання кампусних мереж для університетів були: Стенфордський університет зі своєю одноіменною мережею, “Project Athena” в Массачусетському технологічному інституті, і проект “Andrew” в університеті Карнегі-Меллона.

Великої популярності та поширення кампусні мережі набули в Сполучених Штатах Америки. Такі мережі, як правило, почали активно впроваджувати коледжі та університети. Найчастіше вони об’єднують різні віддалені одна від одної будівлі, в тому числі адміністративні, навчальні корпуси, гуртожитки та інші споруди, такі як конференц-центри, технологічні центри та інші навчальні заклади.

Діапазон дії CAN приблизно становить від 1 км до 5 км. Якщо дві будівлі знаходяться в одному і тому ж домені, і пов'язані між собою спільною мережею, то це буде розглядатися тільки як CAN. Хоч і CAN в основному використовується для корпоративних кампусів, канал передачі даних буде мати високу швидкість.

Послуги такої мережі включають взаємодію між мережами відділів, доступ до якихось загальних баз даних підприємства, доступ до загальних факс-серверів, високошвидкісним модемам і принтерам. В результаті працівники кожного відділу підприємства мають доступ до деяких файлів і ресурсів мереж інших відділів. Важливою аспектом кампусної мережі є те, що у працівників є доступ до корпоративних баз даних незалежно від того, на яких типах комп'ютерів ці бази розташовуються.

Саме на рівні мережі кампуса виникають проблеми інтеграції неоднорідного апаратного і програмного забезпечення. Типи мережевих операційних систем, комп’ютерів, мережевого апаратного забезпечення можуть відрізнятися в кожному відділі. Звідси випливають складності управління мережами кампусів. А оскільки мережі відділів, які входять до мережі кампусу, досить незалежні і часто побудовані на базі різних технологій, об’єднуючою технологією зазвичай є IP.

Правильно побудована кампусна мережа підприємства являє собою ієрархічну структуру, яка складається з трьох рівнів:

- магістральний рівень (Core);
- рівень розподілу (Distribution);
- рівень доступу(Access).

Приклад структури мережі кампусу подано на рисунку 1.2.

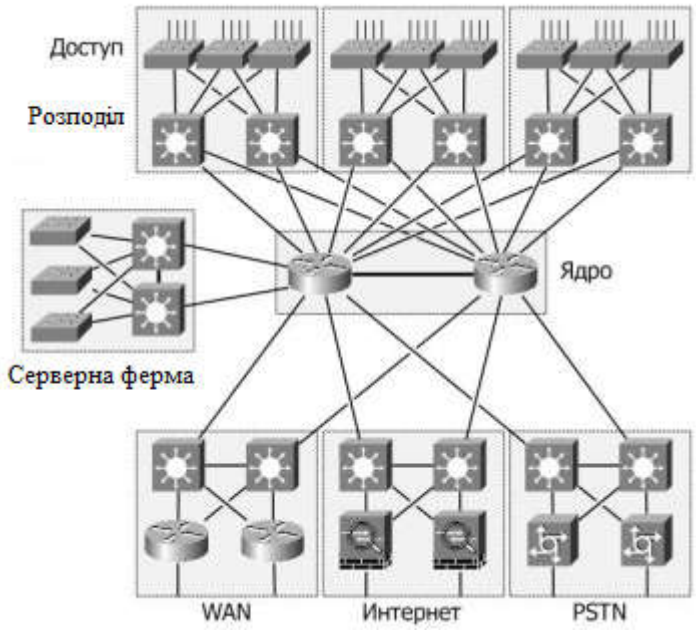

Рисунок 1.2 — Приклад структури мережі кампусів

Такий підхід до опису мережі дає можливість вибрати обладнання, що найбільш точно задовольняє функціональним потребам конкретної мережевої структури.

Магістральний рівень (ядро мережі). Ядро, центральний елемент мережі всього підприємства, становить основні магістральні канали зв'язку. Обладнання ядра мережі володіє наступними характеристиками:

– висока надійність, що досягається, зокрема, за рахунок надмірності і толерантності до збоїв;

– здатність адаптуватися до змін в мережевому середовищі;

– мала затримка при передачі даних;

– хороша керованість і передбачувана продуктивність.

Рівень розподілу. На цьому рівні вирішується завдання доступу в різні частини мережі і до різноманітних послуг. Тут функціонують такі механізми, як політика безпеки, політика доступу до інформаційних ресурсів, управління якістю послуг, що надаються, декілька різних середовищ передачі даних,

маршрутизація між логічними сегментами мережі, визначення мультимедійних доменів і ін.

Рівень доступу. Забезпечується доступ до корпоративних ресурсів для робочих груп і мережевих сегментів. У локальних мережах рівень доступу характеризується комутованим або розділеним доступом користувачів до середовища передачі даних.

Очевидно, що майбутнє локальних мереж пов’язано з різними варіантами технології Ethernet (Fast Ethernet, Gigabit Ethernet і 10G-40G Ethernet). Ця технологія є фактичним стандартом при побудові кампусних мереж. Технологія Ethernet забезпечує:

– ефективний високошвидкісний обмін даними;

– невисоку вартість мережевого рішення;

– просту практичну реалізацію;

– сумісність з усіма поширеними типами додатків, включаючи мультисервісні.

Мережі відділів — це мережі, суть яких випливає з їх назви. Вони використовуються відносно невеликою кількістю працівників, які працюють в одному відділі підприємства. Перед цими працівниками поставлені групи певних задач, наприклад, бухгалтерський облік, маркетингові рішення, робота з персоналом, контроль товарообігу на складі і т.д.. Окремий відділ може нараховувати приблизно 50-150 працівників. Мережа відділу – це така локальна мережа, яка охоплює всю територію приміщення, що належить відділу. Це можуть бути кілька кімнат, залів або цілий поверх будівлі.

Головне призначення мережі відділу полягає в розподілі локальних ресурсів, таких як програми, дані, лазерні принтери, модеми і т.д. Мережі відділів, як правило, не ділять на окремі підмережі, оскільки їх масштаби і так незначні. В їх склад входять один чи два файлових сервери і не близько

тридцяти користувачів. Приклад схеми мережі відділу подано на рисунку 1.3. В такій мережі проходить значна частка всього трафіку підприємства. Мережі відділів зазвичай створюються на основі однієї мережевої технології: Ethernet (або кілька технологій з сімейства Ethernet - Ethernet, Fast Ethernet, рідше Gigabit Ethernet), Token Ring. Для такої мережі характерний один або максимум два типи операційних систем (Linux, Windows чи ін.).

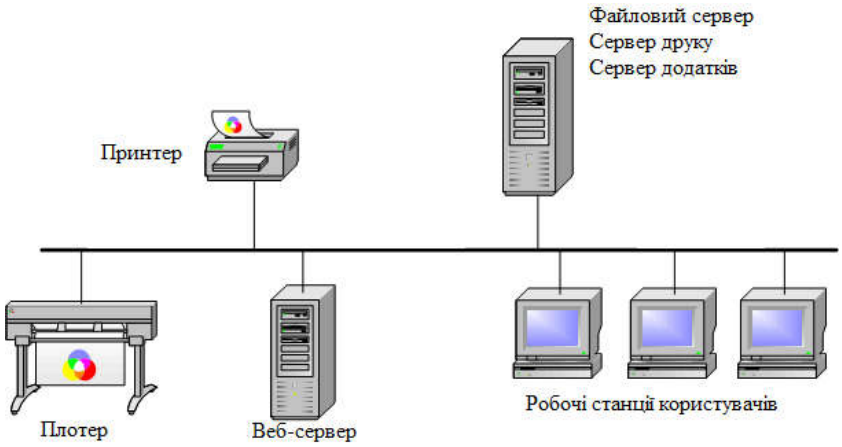

Рисунок 1.3 — Приклад схеми мережі відділів

Задачі мережевого адміністрування на рівні відділу відносно прості: встановлення нових вузлів, додавання нових користувачів, нових версій програмного забезпечення і усунення простих неполадок чи відмов. Таку мережу підтримувати може навіть працівник, який не займає посади системного адміністратора, а лише приділяє деяку частину свого робочого часу для підтримки її працездатності. В наш час, системні адміністратори не обов’язково люди з спеціальною підготовкою, а просто співробітники компанії, які краще за інших розбираються в комп’ютерах, в тому, як працює мережа та іншій офісній техніці.

Є ще такий тип мереж, схожий до мереж відділів — це мережі робочих груп. До таких мереж відносять зовсім невеликі мережі, що включають в себе до

10-20 комп’ютерів. Опис принципів побудови і роботи мереж робочих груп практично не відрізняються від описаних характеристик мереж відділів. Такі властивості, як простота мережі і однорідність, тут проявляються найбільшою мірою, в той час як мережі відділів в деяких випадках можуть виростати до наступного за масштабом типу мереж - мереж будівель і кампусів.

У мережах робочих груп ще часто використовуються технології локальних мереж на поділюваних середовищах. У міру просування по ієрархії вгору — до мереж відділів, будівель і кампусів, колективні середовища зустрічаються все рідше і рідше, поступаючись місцем комутацією каналів.

Мережа відділу може входити до складу мережі будівлі (кампусу) або ж являти собою мережу віддаленого офісу підприємства. У першому випадку мережа відділу підключається до мережі будівлі або кампуса за допомогою технології локальної мережі, якої сьогодні, скоріш за все, буде одна з представниць сімейства Ethernet. У другому випадку, мережа віддаленого офісу підключається безпосередньо до магістралі мережі за допомогою будь-якої технології WAN, наприклад Frame Relay.

1.3 Етапи створення корпоративної мережі

Виділяють три основні етапи для створення корпоративної мережі для підприємства :

– здійснити інформаційну діагностику підприємства;

– вибрати архітектуру системи та програмно-апаратні засоби її реалізації, опираючись на результати попереднього пункту;

– після проведених обстежень, вибрати головні компоненти цієї системи і розробити їх.

Кожній організації потрібна інформаційна система для інформаційно-комунікаційної підтримки її основної та допоміжної діяльностей. Тому, перед тим, як говорити про функціональне наповнення і структуру інформаційної системи (ІС), потрібно зрозуміти цілі і задачі самої організації, щоб зрозуміти, які її сегменти потребують автоматизації.

Цілі інформаційного обстеження:

– визначення кількості робочих місць в кожному структурному підрозділі компанії, відображення технології на структуру, визначення її функціонального складу, опис функцій, які будуть виконуватися на кожному робочому місці;

– алгоритми проходження вхідних, внутрішніх і вихідних документів, опис головних шляхів і технології для їх обробки;

– опис і формулювання функцій всіх підрозділів компанії, а також задачі, які ними вирішуються;

– опис технології роботи кожної секції і пов’язаних з ними потоків інформації;

– опираючись на результати попереднього пункту, зрозуміти, які саме моменти потребують автоматизації і в якій послідовності.

Результатом виступають моделі діяльності компанії та її інформаційної інфраструктури. На їх основі буде розроблятись проект корпоративної ІС, специфікації на розробку прикладного ПЗ, якщо це необхідно, вимоги до апаратно-програмних засобів.

Аналізуючи ці результати, потрібно визначити, якого вигляду набуде архітектура системи. Для корпоративних систем рекомендованою є архітектура клієнт/сервер.

Архітектура клієнт-сервер є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні

розподілених мережних застосунків і передбачає взаємодію та обмін даними між ними. Вона передбачає такі основні компоненти:

– набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них;

– набір клієнтів, які використовують сервіси, що надаються серверами;

– мережа, яка забезпечує взаємодію між клієнтами та серверами.

Інформаційне обстеження дозволяє вибрати апаратно-програмну реалізацію системи.

Одним з основних завдань в розробці ІС є вибір системи управління для корпоративної бази даних(БД). Великі підприємства та організації України використовують СУБД міжнародного рівня, такі як: Oracle, Informix, Sybase, Ingres. Тільки після попереднього обстеження і отримання інформаційних моделей діяльності можна вирішит, яку СУБД використовувати на підприємстві.

Управління інформаційними ресурсами має для діяльності будь-якої установи особливе значення. У сучасному світі установи стикаються з необхідністю обробки колосального обсягу інформації. Незалежно від правового статусу або організаційних форм діяльності установи покликані активно взаємодіяти з органами виконавчої та законодавчої влади, структурами, які беруть участь у регулюванні економіки. Все це в свою чергу породжує специфічний документообіг.

Система електронного документообігу (СЕД) або EDMS (Electronic Document Management Systems) - це система автоматизації роботи з документами протягом всього їх життєвого циклу (створення, зміна, зберігання, пошук, класифікація тощо), а також процесів взаємодії між співробітниками. При цьому під документами в першу чергу маються на увазі неструктуровані

документи (файли Word, Excel та ін.) Як правило, СЕД включає в себе електронний архів документів і систему автоматизації ділових процесів.

Ефективне управління документацією на основі СЕД засноване на трьох складових системи:

– технологія (на основі сучасних комп'ютерних комплексів);

– корпоративні правила створення і використання інформаційних ресурсів (і їх закріплення в розпорядчих документах);

– психологія користувачів та їх навчання (при необхідності індивідуальне).

1.4 Структура корпоративної мережі

Якщо враховувати введені класифікаційні ознаки, то отримаємо деяку узагальнену структуру корпоративної мережі, подано на рисунку 1.5. По суті, будь-яка корпоративна мережа містить в собі фрагменти даної узагальненої структури. В межах даної мережі має бути реалізована вторинна мережа зв’язку - система управління (СУ), подано на рисунку 1.4. В даному випадку також можуть бути використані виділені канали (пунктиром на рисунку 1.5 позначено функціональний зв’язок - фізичний канал проходить через певні засоби захисту, маршрутизації, тощо). Основою системи керування корпоративної мережі повинні бути наступні принципи:

– реалізація адаптивного керування безпекою адекватною зміною відповідних подій в межах системи безпеки;

– реалізація функції системи автоматичного керування в межах керуючої системи. В системі повинна виконуватись автоматична обробка

особливо важливих впливів для збільшення швидкості реакції системи керування на важливі події;

– розподілене чи централізоване адміністрування (основні задачі адміністрування мають вирішуватися з центру); вторинні задачі (в рамках віддалених секторів, наприклад) засобами керування окремих підсистем;

– необхідно створити експертну систему для підвищення ефективності і надійності системи керування – систему «підказок» для здійснення керуючих впливів на події різного характеру;

– поєднання адміністрування окремих функціональних підсистем (проблема безпеки не може бути вирішеною без обліку живучості та ефективності, а питання ефективності без розгляду проблеми живучості мережі (тобто, при зміні рівня безпеки змінюється і ефективність, це має враховуватись).

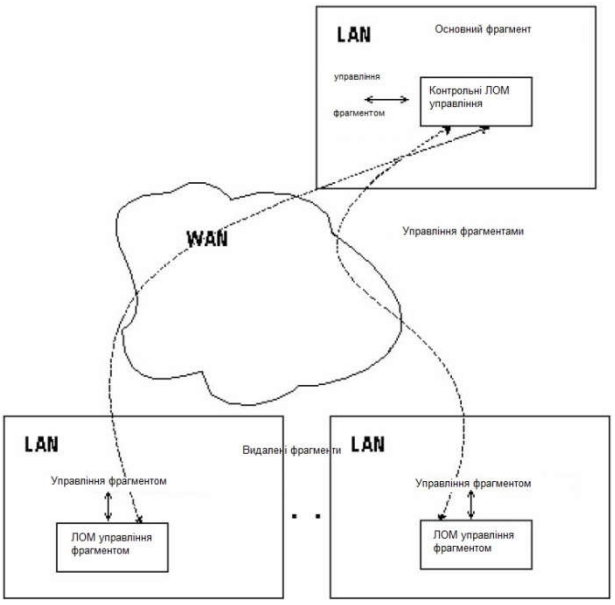

Рисунок 1.4 – Система управління корпоративною мережею

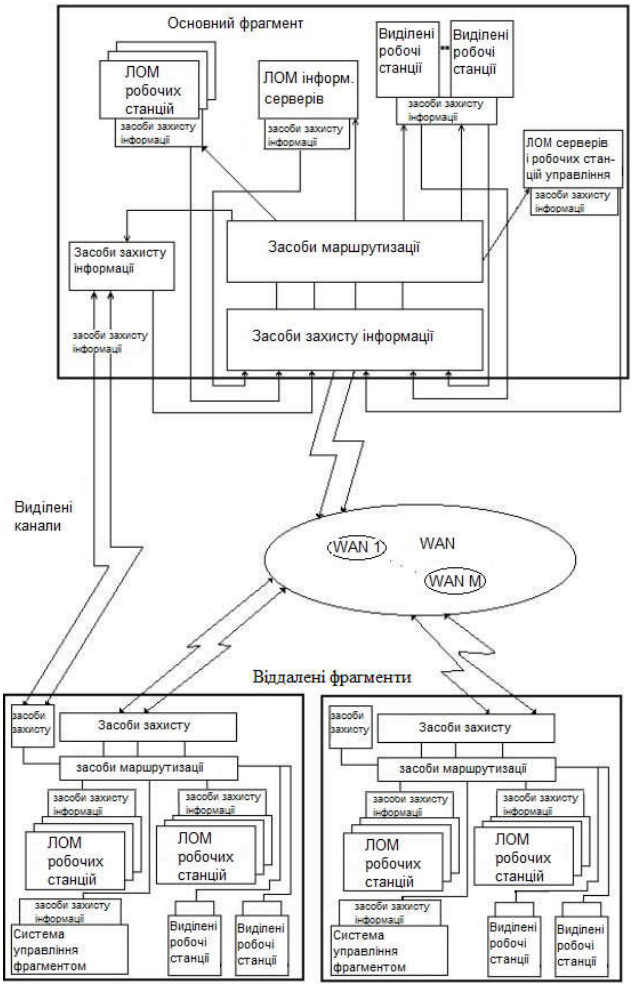

Рисунок 1.5 – Узагальнена структура корпоративної мережі

Узагальнений випадок (див. рисунок 1.5) відрізняється перш за все тим, що структури віддаленого і основного фрагментів співпадають (за функціями вони різні - основний фрагмент реалізує централізоване керування мережею зв'язку). Зазвичай, у цих фрагментів різна складність. Але слід позначити, що для спрощення структури мережі, в частці зменшення складності віддалених фрагментів, з перенесенням певних функцій на елементи основного фрагмента, скоріш за все, є місце для наступних компонентів:

– сервери інформації (щоб захистити свою мережу, є доцільним забезпечуючи для інформаційних серверів необхідний захист, сконцентрувати ці нформаційні сервери);

– під’єднання до серверів, які знаходяться в загальному доступі (наприклад, глобальна Інтернет мережа) проводиться з конкретних робочих місць основного фрагмента (при цьому використовуються доцільні засоби захисту, в загальному випадку, підключення до глобальних мереж відрізняються від інших);

– концентрація в основному фрагменті адміністрування усіма підсистемами функціонального походження для мереж, де використовується обмежена кількість додаткових засобів реалізації такиї підсистем(наприклад, маршрутизаторів).

Устаткування та багатошарове представлення корпоративної мережі.

Корпоративна мережа являє собою складну структуру, яка експлуатує різноманітні типи мережевого зв’язку, способи підключення ресурсів і комунікаційні протоколи.

Комп’ютерна мережа може бути представлена у вигляді багатошарової моделі, яка складається з наступних елементів:

– робочі станції (комп’ютери);

– обладнання і програмне забезпечення для комунікації;

– мережеві додатки;

– операційні системи.

Поверх транспортної системи працюють декілька мережевих операційних систем, іменуємих шаром. Цей шар реалізує роботу програмних додатків в комп’ютерах і за допомогою транспортної системи розподіляє ресурси свого комп’ютера в загальне користування.

Поверх операційної системи функціонують різного роду додатки, та через особливість значення СУБД, які зберігають у сортованому вигляді всю основну інформацію підприємства і виконують в ній базові операції пошуку, такий тип

системних додатків зазвичай відокремлюють від інших додатків корпоративної мережі.

Далі виконують свою роль такі системні сервіси, які, використовуючи СУБД, як інструмент для пошуку певної інформації, дають кінцевим користувачам цю інформацію в впорядкованій та зручній для опрацювання формі. Водночас, ці системи реалізують деякі функції для обробки інформації, що являються загальними для більшості підприємств. До таких сервісів належать система електронної пошти, служба “World Wide Web” (WWW), системи контролю версій та багато інших.

Верхівкою в корпоративній мережі являються спеціальні програмні системи чи комплекси, які займаються задачами вже безпосередньо конкретного підприємства. Прикладом такої системи є автоматизація проектування, керування технологічним процесом, банківські системи, система медичного діагностування і т.п.

Хоч прикладні програми верхнього рівня, які описані вище, і є головними інструментами під час робочого процесу, та їх успішна робота абсолютно залежить від коректної та безперебійної роботи усіх інших підсистем в межах корпоративної мережі.

В корпоративній мережі працюють різні типи комп’ютерів, з різною конфігурацією. Саме комп’ютери та їх характеристики диктують можливості локальних мереж.

До обладнання для комунікації належать: мережеві карти, модеми, міжмережеві екрани, мережеві кабелі та проміжне мережеве обладнання. До такого обладнання належать: комутатори (switches), мости (bridges), приймачі (traceivers), репітери (repeaters), шлюзи (gateways), концентратори (hubs), маршрутизатори (routers).

Для простоти реалізації і запобігання конфлікту міжмережевої взаємодії програмно-апаратних комплексів в мережах, було прийнято правила (стандарт),

які диктують алгоритми для передачі даних в комп'ютерних мережах. Такими правилами стали мережеві протоколи, які задають порядок та принципи взаємодії мережевого обладнання.

В наш час взаємодію мережевого обладнання неможливо описати одним мережевим протоколом, тому було затверджено багаторівневу мережеву модель. Результатом цих домовленностей стала семирівнева модель взаємодії відкритих локальних мереж - OSI.

В цій моделі засоби взаємодії мережевого обладнання поділено на сім рівнів, кожен з яких виконує певні унікальні функції. Рівні цієї моделі звучать наступним чином: прикладний, показний, сеансовий, транспортний, мережевий, канальний і фізичний.

Набір протоколів, яких достатньо для організації взаємодії мережевого обладнання, носить назву — стек комунікаційних протоколів. Найбільшої популярності набув стек — TCP/IP. Стек протоколів TCP/IP робить можливим зв'язок комп'ютерів в межах мережі Інтернет та в корпоративних мережах.

Реалізація протоколів здійснюється мережевими і автономними операційними системами (засобами, які входять до складу операційної системи), а також телекомунікаційним обладнанням (маршрутизаторами, мостами, комутаторами та іншими).

Мережевими додатками вважаються, наприклад, поштові програми (Outlook Express, The Bat, Eudora та інші) і браузери - ПЗ для перегляду веб-сторінок (Microsoft Edge, Google Chrome, Opera, Mozzila Firefox та інші).

1.5 Постановка задачі

В даному проекті необхідно спроектувати корпоративну мережу для організації, що займається виготовленням і збутом електротехніки.

Дана організація має 3 основних будівлі (головний офіс і дві філії), іменовані далі “Центральний офіс” та дві віддаленні філії.

У всіх будівлях використовуються програми 1С: Підприємство, 1С: Склад.

Також необхідно провести розрахунок витрат на мережеве обладнання, мережеве ПО і обслуговування даної мережі.

Головна будівля має чотири поверхи, на кожному поверсі розташовується кілька відділів, в кожному з яких є певна кількість комп’ютерів. Всього серверів - 4.Оптоволоконний кабель, що з’єднує всі три будівлі в одну загальну мережу, прокладений по зовнішньому середовищі.

Необхідно виконати:

– визначення типу мережі, топології і мережної архітектури,

– вибір кабельної системи;

– вибору мережевого і периферійного обладнання;

– вибір ОС для серверів;

– розрахунок витрат на придбання обладнання, монтаж і обслуговування мережі.

2 ПРОЕКТУВАННЯ АРХІТЕКТУРИ МЕРЕЖІ

2.1 Рівнева архітектура мереж CISCO

Поняття “ієрархії” нагадує ставлення в сім'ї. Структура ієрархічного типу дає можливість поділити об’єкти за рівнями, вказати зв’язок між деякими об’єктами і функції, що ними виконуються. Ієрархія дає можливість організації складної моделі, а в сімейних відносинах, привласнити кожному члену певну роль.

В проектуванні мереж також використовується ієрархія. Потрібно поділити всі об’єкти мережі за ієрархічними рівнями, відповідно до виконуваних об’єктами функцій. Як правило, проаналізувавши один із ієрархічних рівнів мережі, функції інших рівнів ми можемо не враховувати.

Мережі нашого часу є дуже складними, тому що їх визначає безліч конфігурацій, протоколів і технологій. Для впорядкування всіх компонентів в легко аналізовану модель, можна використати ієрархію. Дотого ж, вона буде предписувати характеристики кожного рівня ієрархії. Ієрархічна модель Cisco сприяє в створенні, експлуатації і обслуговуванні масштабних, ефективних і надійних об’єднаних мереж. Компанія Cisco оприділила три ієрархічні рівні. На кожному з цих рівнів реалізуються певні специфічні мережеві функцій.

У цій моделі визначено три рівні:

- базовий рівень (Core layer);
- рівень поширення (Distribution layer);
- рівень доступу (Access layer).

На кожному рівні реалізуються певні функції. Але ці рівні є логічними і не завжди збалансовані з фізичними пристроями. В другій ієрархічній моделі - OSI також реалізуються логічні рівні ієрархії. Для передачі трафіку було реалізовано сім таких рівнів. Але кожен з протоколів не завжди відповідає відповідним

функціям. Деколи протокол може працювати відразу на декількох рівнях моделі OSI, а деколи, кілька протоколів відповідають одному рівню. Так само, при організації фізичного виконання ієрархічної мережі, кілька пристроїв можуть працювати в межах одного рівня, або один конкретний пристрій буде виконувати задачі декількох рівнів. Отож, рівні моделі є логічними поняттями, а не фізичними.

Базовий рівень формує ядро мережі. Базовий рівень відповідає за надійний і швидкий обмін великими об'ємами трафіку. Швидка комутація трафіку — це єдина задачі базового рівня. На базовому рівні трафік спільно пересилається для кількох користувачів. Призначені для користувача дані обробляються на рівні розподілу, що може привести до додаткових запитів в базовий рівень.

Якщо на базовому рівні стається помилка, то вона також вплине і на всіх користувачів. Отож, важливою задачею є забезпечення високої надійності на базовому рівні. Тут обробляються великі обсяги трафіку, тому одинаково важливим є і враховування швидкості та затримки передачі даних.

Іншою назвою рівня поширення є "рівень робочих груп". Цей рівень знаходиться поміж базового рівня та рівнем доступу. Маршрутизація, фільтрація і доступ до регіональних мереж, а також, якщо потрібно, визначення правил доступу пакетів до базового рівня — це основні функції рівня поширення. Цей рівень повинен встановлювати найоптимальніший спосіб обробки запитів до служб. Після детермінації на рівні поширення найоптимальнішого шляху доступу, запит буде передано на базовий рівень, в якому реалізовано швидкісне транспортування запиту до певної службі. На рівні поширення створюється деяка політика мережі і проводиться гнучкий опис операцій мережевих. На рівні поширення здійснюються такі функції:

– відбувається перерозподіл в середині протоколів маршрутизації, в тому числі і реалізація статичних шляхів;

– розробка системи безпеки і мережевих політик, в тому числі і встановлення брандмауерів і трансляція адрес;

– VLAN-маршрутизація та інші функції для підтримки робочих груп;

– встановлення доменів багатоадресних і широкомовних розсилок;

– розробка чи впровадження інструментів, схожими до списків доступу, фільтрації механізму запитів або вхідних/вихідних пакетів.

На рівні розподілу не слід виконувати ті функції, які властиві двом іншим рівням.

Рівень доступу характерний керуванням робочими групами і користувачами під час звернення до ресурсів об’єднаної мережі. Для коректної і безперебійної роботи, більша частка потрібних мережевих ресурсів має бути доступна локально для користувачів мережі. На цьому рівні відбувається перенаправлення трафіку до віддалених служб. Рівень доступу вирішує наступні задачі:

– сегментація;

– зв’язок між робочими групами та рівнем розподілу;

– безперервне контролювання доступу і політики за допомогою рівня розподілу.

Як правило, на рівні доступу використовуються комутація Ethernet або технологія DDR. В цьому випадку використовується статична маршрутизація (в якості заміни для протоколів динамічної маршрутизації). Як вже говорилось раніше, ці три окремих рівня не зв’язані з трьома спеціальними типами маршрутизаторів. Таких пристроїв можна використовувати в будь-якій кількості, але слід пам’ятати про поділ втратити зв’язку із мережею за рівнями моделі.

2.2 Моделювання мережі в Cisco Packet Tracer

Для моделювання комп’ютерної мережі було використано програму Cisco Packet Tracer 7.0.

Packet Tracer - симулятор мережі передачі даних, що випускається фірмою Cisco Systems. Дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори і комутатори, взаємодіяти між декількома користувачами (через хмару). У симуляторі реалізовані серії маршрутизаторів Cisco 800, 1800, 1900, 2600, 2800, 2900 і комутаторів Cisco Catalyst 2950, 2960, 3560, а також міжмережевий екран ASA 5505. Бездротові пристрої представлені маршрутизатором Linksys WRT300N, точками доступу і стільниковими вишками. Крім того є сервери DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP і EMAIL, робочі станції, різні модулі до комп'ютерів і маршрутизаторів, IP-фони, смартфони, хаби, а також хмара, що емулює WAN. Об'єднувати мережеві пристрої можна за допомогою різних типів кабелів, таких як прямі і зворотні пасивне, оптичні і коаксіальні кабелі, послідовні кабелі та телефонні пари.

Успішно дозволяє створювати навіть складні макети мереж, перевіряти на працездатність топології. Однак, варто зауважити, що реалізована функціональність пристроїв обмежена і не надає всіх можливостей реального обладнання. Cisco Packet Tracer доступний безкоштовно для учасників Програми Мережевий Академії Cisco.

Спочатку було спроектовано фізичну схему мережі кожного з поверхів підприємства, подано на рисунку 2.1.

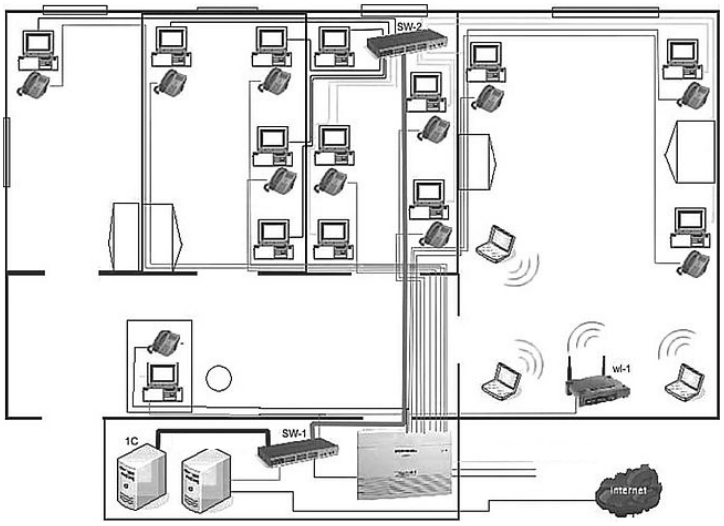

Рисунок 2.1 — Фізична схема мережі одного з поверхів

Наведена вище схема показує приблизне розташування комп'ютерної техніки на підприємстві по кабінетах. Комп'ютери з інших кабінетів, виведено в окрему підмережу, яка для підвищення швидкодії підключена до серверів по виділеній лінії. Для кращого розуміння принципів даної мережі, на рисунку 2.2 наведено логічну схему мережі з аналогічним обладнанням до використовуваного на підприємстві розроблену з допомогою Cisco PackeTracer.

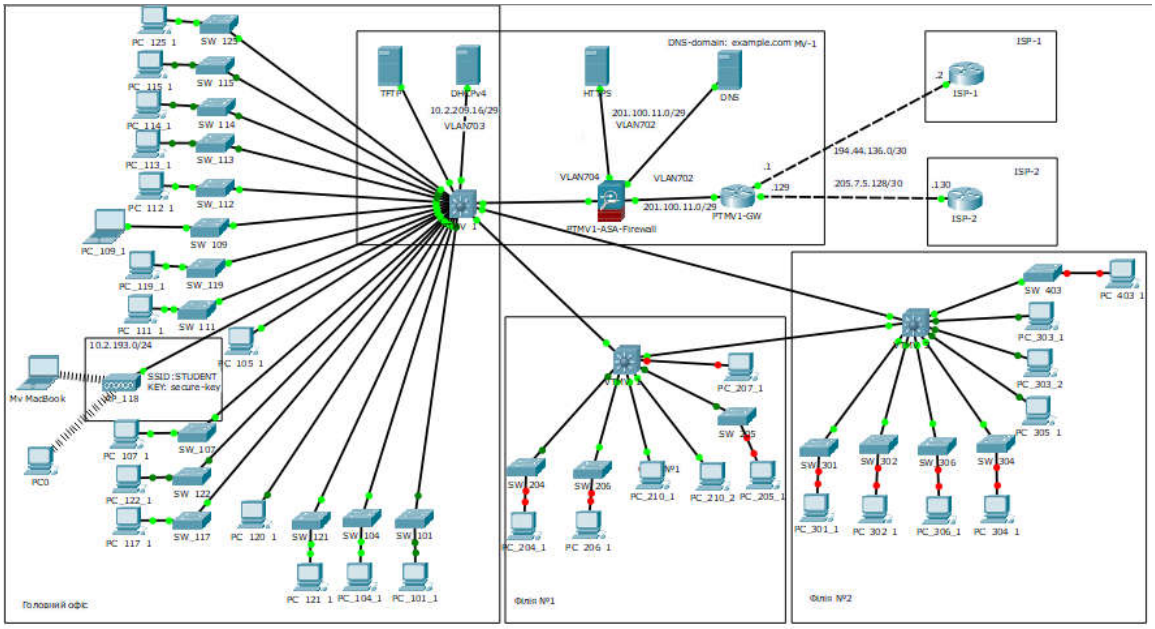

Рисунок 2.2 – Логічна схема корпоративної мережі організації

Подана вище логічна схема показує, що на підприємстві встановлено 4 сервери:

– DHCP-сервер;
– DNS-сервер;
– TFTP-сервер;
– HTTPS-сервер.

Також від центрального (серверного) комутатора йде підключення усіх пристроїв до глобальної мережі через файрвол. Підключення до глобальної мережі здійснене за допомогою оптоволоконного кабелю зі швидкістю 2-4 Гбіт/с.

Налаштовано наступні види мережевого трафіку:

– http;
– database;
– ftp;
– program-access;
– VPN;
– SMTP.

Основними логічними сегментами комп’ютерної мережі офісу є:

– мережа для серверів публічного доступу;
– мережа для серверів загального доступу;
– мережа для точки бездротового доступу;
– мережа для з’єднання мережевих пристроїв.

Кожен із сегментів комп’ютерної мережі повинен мати доступ до мережі інтернет.

Для захисту від атак ззовні використовується міжмережевий екран.

Структурну схему мережі подано в БР.КСМ.07162/17.00.00.000 С1.

2.3 Захист корпоративної мережі

Якщо говорити про захист інформації в корпоративній мережі, то спочатку необхідно визначити, що ж все таки є об’єктом захисту. Це — складно структурована гетерогенна мережа, призначена для розподіленої обробки даних.

Характерною особливістю корпоративної мережі є те, що її побудова здійснюється як правило, на протязі декількох років, що є причиною того, що в одній мережі може функціонувати обладнання від різних виробників чи поколінь, де можна зустріти як найсучасніше, так і дуже примітивне програмне забезпечення, яке може не підтримувати функцію спільної обробки даних.

Якщо в мережі відбувається обробка даних, що становлять комерційну або іншу таємницю, то для забезпечення безпеки цієї інформації повинні бути вжиті певні заходи.

Науково-інженерне підприємство “Інформзахист” запропонувало поетапний план побудови цілісної системи захисту інформації під назвою “Комплексний підхід до забезпечення інформаційної безпеки”. Далі коротко перераховані назви його етапів:

– обстеження автоматизованої системи і розробка організаційно-розпорядчих документів;

– вибір, придбання, установка, настройка і експлуатація засобів захисту;

– навчання персоналу роботи з наявними засобами захисту;

– інформаційне обслуговування з питань інформаційної безпеки;

– періодичний аудит системи інформаційної безпеки.

– Застосуємо цей підхід до корпоративної мережі.

Першим етапом є обстеження корпоративної мережі. За підсумками обстежень розробляється комплект документів (Концепція інформаційної безпеки і План захисту), на основі яких будуть проводитися всі роботи по захисту.

Ці документи повинні розроблятися після вивчення структури мережі і отримання цілісного уявлення про технології обробки даних в ній. Бажано, щоб подібні роботи були виконані професіоналами, так як прорахунки на етапі проектування системи інформаційної безпеки можуть обернутися серйозними проблемами і втратами при її побудові і експлуатації.

З урахуванням особливостей корпоративної мережі, розроблені документи повинні передбачати рішення наступних завдань:

– захист від проникнення в корпоративну мережу і від витоку інформації з мережі по каналах зв'язку;

– розмежування потоків інформації між сегментами мережі;

– захист найбільш критичних ресурсів мережі від втручання в нормальний процес функціонування;

– захист важливих робочих місць і ресурсів від несанкціонованого доступу (НСД);

– криптографічний захист найбільш важливих інформаційних ресурсів.

Захист від проникнення в мережу і від витоку інформації з мережі. В якості основного засобу, що дозволяє реалізувати подібну загрозу, розглядається канал підключення корпоративної мережі до глобальної мережі Internet. Звичайно, ймовірність реалізації загрози залежить від багатьох факторів, тому говорити про єдиний спосіб захисту в кожному конкретному випадку не можна. Найбільш поширеним рішенням є застосування міжмережевих екранів, які дозволяють визначити і реалізувати правила

розмежування доступу як для зовнішніх, так і для внутрішніх користувачів корпоративної мережі, приховати при необхідності структуру мережі від зовнішнього користувача, блокувати відправку інформації “забороненими” адресами і, нарешті, просто контролювати використання Internet.

Зазвичай міжмережеві екрани (МЕ) захищають внутрішню мережу компанії від “вторгнень” з мережі Internet. Однак вони можуть використовуватися і для захисту від “нападів”, наприклад, з корпоративної інтрамережі, до якої підключена мережа даного підприємства. Як і в разі реалізації будь-якого іншого механізму мережевого захисту, організація, що виробляє конкретну політику безпеки, крім усього іншого, повинна визначити тип трафіку TCP / IP, який буде сприйматися брандмауером як “авторизований”. Наприклад, необхідно вирішити, чи буде обмежений доступ користувачів до певних служб на базі TCP / IP, і якщо буде, то до якої міри. Вироблення політики безпеки дозволить з’ясувати, які компоненти брандмауера необхідні і як їх налаштувати, щоб забезпечити обмеження доступу, задані підприємством.

Розмежування потоків інформації між сегментами мережі. Залежно від характеру оброблюваної в тому чи іншому сегменті мережі інформації і від способу взаємодії між сегментами реалізують один з варіантів:

Ніякого розмежування — варіант, який можна застосовувати у випадках, коли ні в одному з взаємодіючих сегментів не зберігається і не обробляється важлива інформація або коли сегменти мережі містять інформацію з однаковою важливістю і знаходяться в одній будівлі, тобто в межах контрольованої зони. Реалізація не вимагає ніяких зусиль, але й захист просто відсутній.

Розмежування засобами комунікаційного обладнання (маршрутизаторів, інтелектуальних перемикачів і т.п.). Реалізація подібного розмежування вимагає ретельного вивчення можливостей комунікаційного обладнання і глибокого знання структури мережі та інформаційних потоків, що циркулюють в ній, так як результат повністю залежить від грамотної настройки. При цьому

комунікаційне обладнання спочатку, як правило, не є засобом захисту, тому подібне розмежування не дозволяє реалізувати захисні функції в повному обсязі.

Застосування міжмережевих екранів - рекомендується при організації взаємодії між сегментами через мережу Internet. Як правило, даний спосіб застосовується тоді, коли в мережі вже є міжмережеві екрани, призначені для контролю за потоками інформації між внутрішньою мережею і Internet.

Захист найбільш критичних ресурсів мережі від втручання в нормальний процес функціонування. Найбільш критичними ресурсами в корпоративної мережі є сервери. Основним способом втручання в нормальний процес їх функціонування є проведення атак з використанням вразливостей мережевого апаратного і програмного забезпечення. При цьому атака може бути реалізована як із зовнішньої (Internet), так і з внутрішньої мережі, наприклад, одним з штатних працівників. Основна проблема полягає не тільки в своєчасному виявленні та реєстрації атаки, що дозволяють зробити багато засобів, але і в протидії їй, так як навіть піймання зловмисника (на основі результатів реєстрації) буде служити слабкою втіхою, якщо корпоративна мережа буде паралізована на деякий час через успішно проведену атаку.

Одним з найбільш потужних інструментів, призначених для оперативного реагування на подібні напади була система RealSecure, вироблена американською корпорацією Internet Security Systems, Inc, яку 16 жовтня 2006 року викупила компанія IBM і продовжила подальшу розробку і підтримку цієї системи. Система RealSecure дозволяє своєчасно виявити і запобігти всім відомі на сьогоднішній день атаки, що проводяться по мережі.

Захист важливих робочих місць і ресурсів від несанкціонованого доступу (НСД). Наступні рекомендації можна розглядати як загальні при виборі засобів захисту від несанкціонованого доступу:

– орієнтуватися необхідно тільки на сертифіковані продукти;

– вибирати постачальника систем захисту, який забезпечить повний комплекс обслуговування, тобто не тільки продаж і гарантії, які є у всіх, але і послуги по встановленню та налагодженню (при необхідності), з навчанням співробітників роботі із засобами захисту, по супроводу придбаних систем;

– вибирати систему захисту, що забезпечує розмежування доступу в різних операційних системах;

– орієнтуватися на системи з кращими експлуатаційними характеристиками, такими як: висока надійність, сумісність з різним програмним забезпеченням, мінімальне зниження продуктивності робочої станції, обов'язкова наявність коштів централізованого управління захисними механізмами з робочого місця адміністратора безпеки, оперативне оповіщення адміністратора про всі події НСД на робочих станціях;

– при виборі звертати увагу не тільки на вартість подібних засобів, але і на рівень передбачуваних витрат на їх експлуатацію і супровід.

Криптографічний захист найбільш важливих інформаційних ресурсів. Шифрування є найбільш надійним способом захисту даних від НСД. Всі засоби шифрування мають істотний недолік - значне (в деяких випадках більш ніж в 2 рази) зниження продуктивності комп'ютерів, на яких вони встановлені і працюють. Специфіка продуктів, призначених для шифрування, призводить до того, що в даний час в корпоративних мережах подібні продукти встановлюються тільки на тих робочих місцях, на яких зберігається інформація, що має дуже високу важливість, або обробляються електронні грошові платежі (наприклад, в системах Банк-Клієнт) - всього не більше 1-5% від загального числа робочих станцій.

По закінченню робіт першого етапу складається повне уявлення про те, в якому стані знаходиться корпоративна мережа зараз, і про те, що потрібно зробити, щоб забезпечити захист інформації в ній.

На основі даних обстежень можна перейти до другого етапу плану - вибору, придбання, встановлення, налаштування та експлуатації систем захисту відповідно до розроблених рекомендацій.

Питанню вибору відповідних засобів потрібно приділити достатньо уваги. Підприємству слід віддавати собі звіт, що будь-який засіб захисту створює додаткові перешкоди в роботі звичайного користувача, при цьому перешкод буде тим більше, чим менше часу буде приділятися налаштування цих систем. Адміністратор безпеки повинен щодня обробляти дані реєстрації для того, щоб своєчасно корегувати налаштування систем, що забезпечують адаптацію до змін в технології обробки інформації. Без цього будь-яка система, якою б гарною вона не була, приречена на повільне і болісне (для кінцевих користувачів) вимирання.

Третій етап — навчання адміністраторів безпеки роботи з набутими засобами захисту. В процесі навчання адміністратор набуває базові знання про технології забезпечення інформаційної безпеки, глибокі знання про наявні в операційних системах підсистемах безпеки і можливості досліджуваних систем захисту, про технологічні прийоми, які використовуються при їх налаштування і експлуатації.

Четвертий етап — інформаційне обслуговування з питань безпеки. Наявність своєчасної інформації про виявлені вразливості і про способи захисту від них, безумовно, допоможе зробити деякі заходи задовго до того, як “вдарить грім”. Джерел даних такого роду в даний час дуже багато - це книги, журнали, Web-сервери, списки розсилки і т.п. На жаль, адміністратор безпеки не завжди має достатню кількість часу для пошуку крупинок знань в цьому морі інформації. Щоб не платити за час, витрачений ним на читання величезної кількості літератури, підприємству слід надати йому якусь квінтесенцію, підготовлену фахівцями.

П’ятий етап - періодичний аудит системи інформаційної безпеки — необхідний тому, що корпоративна мережа, подібно до живого організму, є структурою, що постійно змінюється. З’являються нові сервери і робочі станції, змінюється програмне забезпечення та його налаштування, змінюється склад і важливість інформації, змінюються люди, що працюють в організації і т.д. Все це призводить до того, що захищеність системи постійно знижується.

Важливою складовою частиною робіт цього етапу є корегування плану захисту відповідно до реального стану корпоративної мережі. Найдосконаліша інструкція рано чи пізно застаріє і стане серйозною перешкодою на шляху розвитку технології обробки даних.

3 МОДЕЛЮВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Налаштування комутаторів

Задля оптимізації мережевого трафіку й підвищення безпеки комп'ютерної мережі офісу, логічну мережу 10.2.0.0./16 було сегментовано до маски IP-адреси мережі /20. З отриманих 16 підмереж /20 IP- адреси мережі виділено на поверхи діапазони IP-адрес з маскою /20, на точку бездротового доступу /20, на магістральні канали між ТМВ /20, на сервера обмеженого доступу /20.

У додатку А наведено детальну схему IP-адресації мережі.

Базове налаштування комутатора включає в себе:

- задання ім'я пристрою;
- налаштування бази даних користувачі комутаторі з відповідними логінами і паролями;
- налаштування паролю на конфігураційних режимах;
- налаштування доступу по віртуальних лініях зв'язку;
- налаштування доступу по фізичних (консоль) лініях зв'язку;
- налаштування банерів;
- включення криптування паролів в конфігураційному файлі;
- початкове закриття всіх комунікаційних інтерфейсів;
- налаштування безпеки.

У додатку Б наведено лістинги конфігураційних файлів комутаторів 3 рівня PTMV_l, VTMV_1, VTMV_2.

Досить ефективним рішення при використанні резервних з'єднань є протокол зв'язуючого дерева (Spanning Tree Protocol (STP)) - це протокол канального рівня, який використовується для підтримки такого стану мережі, у

якому в ній немає петель. Cisco має власну реалізацію STP протоколу PVST (Рег- VLAN Spanning Tree), що розширює функціонал STP й призначений для роботи з декількома VLAN. У PVST для кожного VLAN існує свій STP процес, що дозволяє незалежне і гнучке налаштування під потреби кожного VLAN, й також дозволяє використовувати балансування навантаженням за рахунок того, що конкретний фізичний лінк може бути заблокований в одному VLAN, але працювати в іншому.

Задля забезпечення бездротовим доступом на першому поверсі необхідно налаштувати DHCP Server в діапазоні 10.2.193.0/24 й відповідно налаштувати точку бездротового доступу.

3.2 Налаштування маршрутизаторів

З метою забезпечення усіх вузлів мережі офісу безперебійним доступом до мережі Інтернет до маршрутизатора PTMV1-GW здійснено підключення одночасно двох Інтернет провайдерів (основного і резервного).

Налаштування інтерфейсів маршрутизатора PTMV1-GW:

ip address 194.44.136.1 2ББ.255.255.252 ip nat outside duplex auto speed auto i

interface FastEthernet0/l description link-to-isp2 ip address 205.7.5.129 255.255.255.252 ip nat outside duplex auto speed auto !

interface FastEthernetl/0

description link-to-inside

ip address 201.100.11.6 255.255.255.248

ip nat inside

duplex auto

speed auto

Задания пулу зовнішніх адрес, в які транслюватимуться внутрішні адреси:

ip nat pool NAT-POOL 201.100.11.8201.100.11.15 netmask
255.255.255.248

Ввімкнення NAT на маршрутизаторі PTMV 1-GW:

ip nat inside source list NAT-ACL pool NAT-POOL overload

Дана команда говорить маршрутизатору, що у всіх пакетів, які отримані на внутрішній інтерфейс і дозволені списком доступу NAT-ACL, адрес відправника буде трансльований на адресу з NAT пулу “NAT-POOL”. Ключ “overload” вказує, що трансляції будуть перевантажені, дозволяючи кільком внутрішнім вузлам транслюватися на один IP адрес.

В якості проколу маршрутизації для VLAN у мережі офісу використовується протокол EIGRP.

EIGRP - це пропрієтарний протокол маршрутизації, що базується на старому протоколі IGRP. EIGRP – дистанційно-векторний протокол.

Після змін топології мережі, уникнення проблеми зациклення маршруту та більш ефективного і економного використання потужностей маршрутизатора.

Алгоритм визначення маршруту базується на алгоритмі Дейкстрі пошуку в глибину на графі. EIGRP обчислює і враховує 5 параметрів для кожної ділянки маршруту між вузлами мережі:

– total Delay - загальна затримка передачі (з точністю до мікросекунди);

– minimum Bandwidth - мінімальна пропускна спроможність (в Кб/с - кілобіт/секунду);

– reliability - надійнсть (оцінка від 1 до 255; 255 найбільш надійно);

– load - завантаження (оцінка від 1 до 255; 255 найбільш завантажено);

– maximum Transmission Unit (MTU) (не враховується при обчисленні оптимального маршруту, береться до уваги окремо) — максимальний розмір блоку, що можливо передати по ділянці маршруту.

Налаштуваня EIGRP протоколу на комутаторах PTMVl, VTMV1 та VTMV 2 наведено у додатку Б.

Один із способів налаштування маршрутизації є задання маршруту по замовчуванню. Для налаштування на комутаторі PTMV1 того, щоб всі пакети, адреси призначення яких не вказані в таблиці маршрутизації відправлялися на міжмережевий екран (Firewall) виконується наступна команда:

ip route 0.0.0.0 0.0.0.0 10.2.224.18

Команда “ip classless” на комутаторі PTMV1 визначає, якщо в таблиці маршрутизації немає мережі отримувача, то усі пакети будуть відправлені за маршрутом по замовчуванню.

3.3 Налаштування робочих станцій

Налаштування і конфігурація робочих станцій не несе в собі нічого особливого. Як правило, це просто інсталяція базових програмних додатків для

роботи з мережею Інтернет, та налаштування статичної чи динамічної IP-конфігурації.

Приклад IP-налаштування стаціонарної робочої станції подано на рисунку 3.1, приклад IP-налаштування робочих станцій, що підключаються по мережі Wi-Fi - подано на рисунку 3.2.

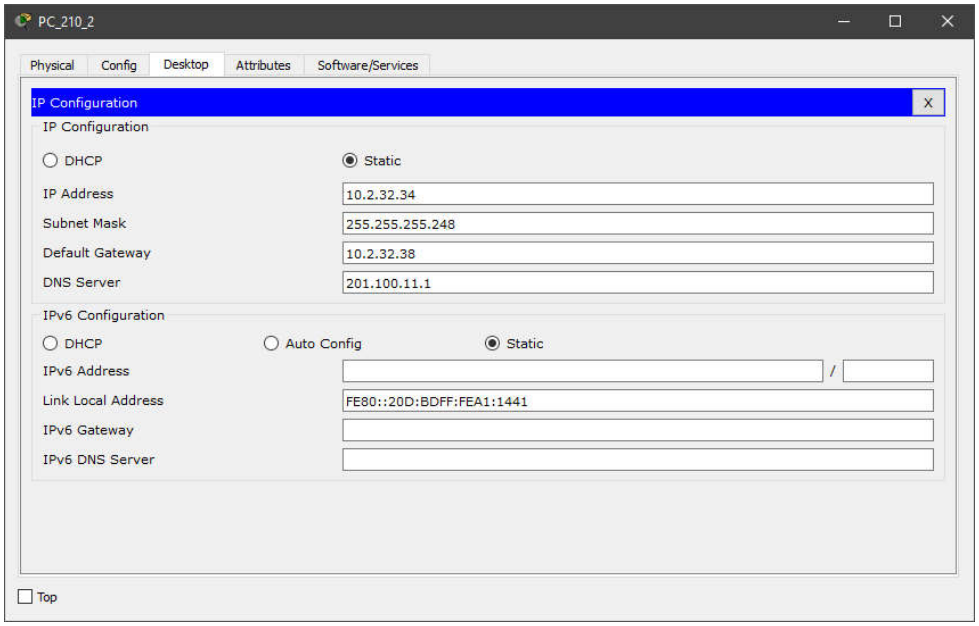

Рисунок 3.1 — Налаштування робочої станції

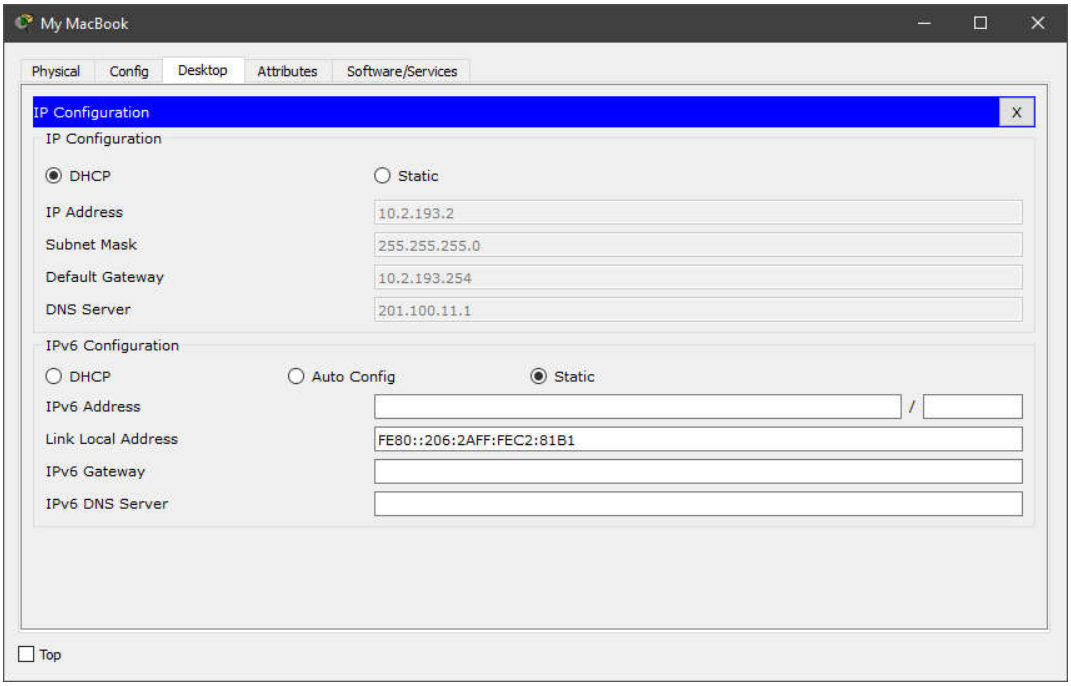

Рисунок 3.2 — Налаштування ноутбука

3.4 Організація безпеки комутаторів та маршрутизаторів

Міжмережевий екран (Firewall) - пристрій контролю доступу в мережу, призначений для блокування усього трафіку, за винятком дозволених даних. Цим він відрізняється від маршрутизатора, функцією якого є доставка трафіку в пункт призначення в максимально короткі терміни.

Міжмережевий екран також приховує схему внутрішньої адресації мережі.

Для забезпечення безпечної, надійної й ефективної взаємодії пристроїв локальної мережі з мережею Інтернет, необхідно також налаштувати списки прав доступу (Access Control Lists).

З допомогою технології NAT (Network Address Translation) використовуючи одну або кілька зовнішніх IP адрес, виданих провайдером можна підключити до мережі практично будь-яку кількість комп'ютерів.

NAT - це механізм зміни мережевої адреси в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою відображення одного адресного простору в інший.

Для забезпечення доступу до мережі Інтернет в офісі, використовуються послуги двох інтернет провайдерів (основного і резервного). Для цього було обрано такий граничний пристрій, як маршрутизатор Cisco 2811.

Для забезпечення безпеки мережі офісу використовується міжмережевий екран Cisco ASA5505-K8. Даний пристрій здійснює моніторинг вхідного і вихідного мережевого трафіку й на підставі встановленого набору правил безпеки приймає рішення пропустити або блокувати конкретний трафік.

Віртуальна локальна мережа (VLAN) використовується задля убезпечення мережі від несанкціонованого доступу. Тобто, на канальному рівні кадри з інших VLAN будуть відкидатися портом комутатора незалежно від того, з якою вихідною IP-адресою пакет у даному кадрі. Також VLAN дозволяє будувати мережі, логічна структура якої не залежить від фізичної.

У додатку А наведено список усіх віртуальних локальних мереж та їх імен відповідно до розробленої IP-адресної схеми.

У додатку Б наведено у конфігураційних файлах комутаторів PTMV1, VTMV1, VTMV 2 усі здійснювані налаштування VLAN.

3.5 Перевірка працездатності мережі

Останнім етапом проектування мережі офісу є перевірка роботи усіх вузлів та усунення можливих помилок.

Для цього було перевірено коректність налаштувань мережевих пристроїв шляхом консольної команди “ping” між декількома робочими станціями. Результат цієї перевірки подано на рисунку 3.3.

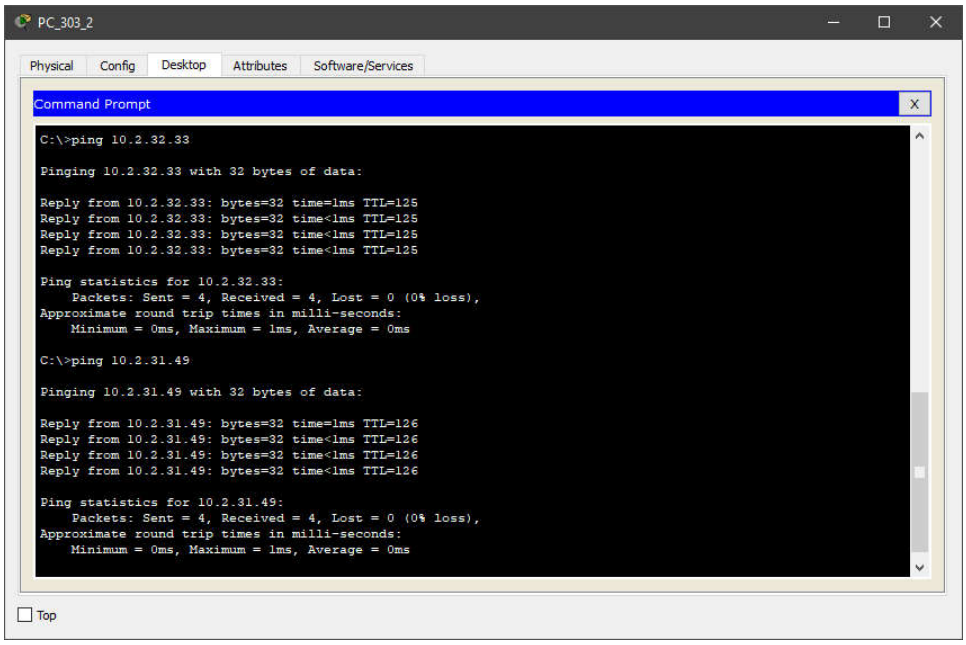

Рисунок 3.3 — Перевірка з’єднання між робочими станціями різних підмереж

Перевірка потоку трафіку в режимі симуляції від Cisco Packet Tracer, подано на рисунку 3.4, також показує, що всі налаштування працюють коректно.

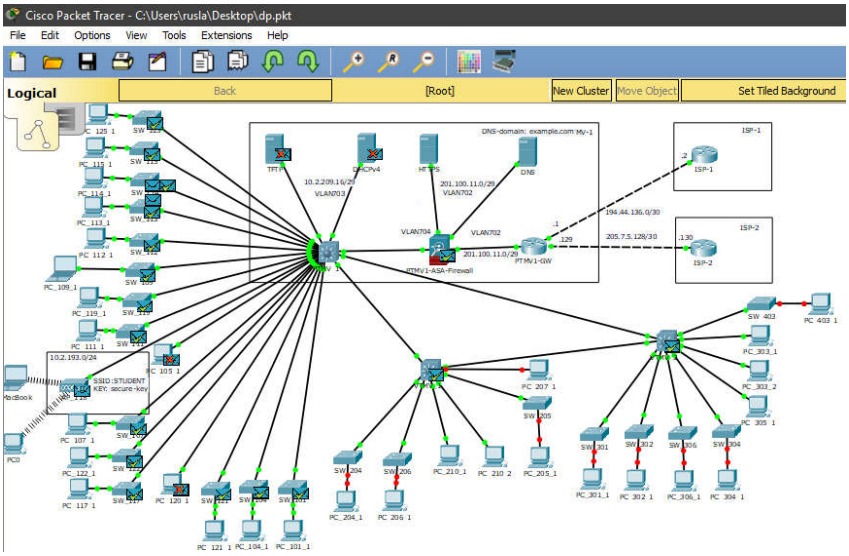

Рисунок 3.4 — Режим симуляції в Cisco Packet Tracer

Отже, за даними перевірки працездатності мережі засобами програми Cisco Packet Tracer можна сказати, що планування і проектування мережі є успішними.

4 ТЕХНІКО-ЕКОНОМІЧНИЙ РОЗДІЛ

Метою техніко-економічного розділу є проведення економічних розрахунків, які спрямовані на роз'яснення економічної ефективності розробки проекту мережі для підприємства і прийняття рішення про його подальший розвиток і впровадження або ж недоцільність проведення даної розробки.

Для визначення загальної тривалості проведення НДР дані витрат часу з окремих операцій доцільно звести у таблицю 4.1.

4.1 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Витрати на оплату праці включають в себе заробітну плату (ЗП) всіх категорій працівників, що брали участь на всіх етапах проектування. Розмір ЗП вираховується на основі трудоємності відповідних робіт та середньої ЗП відповідних категорій працівників.

У розробці проектного рішення були задіяні наступні спеціалісти – розробники, а саме: керівник проекту, студент-дипломник та консультант техніко– економічного розділу (таблиця 4.1).

Таблиця 4.1 – Вихідні дані для розрахунку витрат на оплату праці

Посада виконавців	Місячний оклад (стипендія), грн.
Керівник ДП, викладач	5950,00
Консультант техніко– економічного розділу, доцент	7293,00
Студент	1400,00

Витрати на оплату праці розробників проекту визначаються за формулою:

$$B_{ОП} = \sum_{i=1}^{N} \sum_{j=1}^{M} n_{ij} \cdot t_{ij} \cdot C_{ij} \ , \qquad (4.1)$$

де n_{ij} – чисельність розробників i–ої спеціальності j– го тарифного розряду, осіб;

t_{ij} – затрачений час на розробку проекту співробітником i–ої спеціальності j– го тарифного розряду, год;

C_{ij} – годинна ставка працівника i–ої спеціальності j– го тарифного розряду, грн.,

Середньо годинна ставка працівника може бути розрахована за формулою:

$$C_{ij} = \frac{C_{ij}^{0}(1+h)}{РЧ_i}, \qquad (4.2)$$

де C_{ij} – основна місячна заробітна плата розробника i-ої спеціальності j-го тарифного розряду, грн.;

h – коефіцієнт, що визначає розмір додаткової заробітної плати (при умові наявності доплат);

$РЧ_i$ – місячний фонд робочого часу працівника i-ої спеціальності j-го тарифного розряду, год. (приймаємо 168 год.).

Коефіцієнт h, який визначає розмір додаткової заробітної плати, для керівника та консультанта техніко-економічного розділу дорівнює 1,47.

Середня годинна ставка керівника ДП дорівнює:

$$C_{ij} = \frac{5950 \cdot (1+1{,}47)}{168} = 87{,}48 \text{ грн/год.}$$

Середня годинна ставка консультанта техніко-економічного розділу ДП дорівнює:

$$C_{ij} = \frac{7293 \cdot (1 + 1{,}47)}{168} = 107{,}22 \text{ грн/год.}$$

Середня годинна оплата студента дорівнює:

$$C_{ij} = \frac{1400}{168} = 8{,}33 \text{ грн/год.}$$

Звідси, загальні витрати на оплату праці ($B_{ОП}$) дорівнюють:

$$B_{ОП}=16*87{,}48+144*8{,}33+2{,}107{,}22=2813{,}64 \text{ грн}$$

Дані для розрахунку витрат на оплату праці наведено в таблиці 4.2

Таблиця 4.2 – Середній час виконання НДР та стадії технологічного процесу

Назва операції (стадії)	Середній час виконання операції, год.	Погодинна заробітна плата, грн/год.	Витрати на розробку, грн
Керівник ДП, викладач	16	87,48	1399,68
Консультант ТЕР, доцент	2	214,44	241,44
Розробка проекту мережі, студент	144	8,33	1199,52
Разом			2813,64

Крім того, слід визначити відрахування на соціальні заходи. Величну відрахувань у спеціальні державні фонди визначають у відсотковому співвідношенні від суми основної та додаткової заробітних плат. Згідно діючого нормативного законодавства сума відрахувань у спеціальні державні фонди складає 20,5% від суми заробітної плати:

$$B_{Ф} = 0{,}205 \cdot B_{\text{ОП}},$$

$$B_{Ф} = \frac{20{,}5}{100} \cdot 2813{,}64 = 576{,}80 \text{ грн.}$$

Загальна сума витрат на матеріальні ресурси ($B_{M)}$ визначається за формулою:

$$B_M = \sum_{i=1}^{n} K_i \cdot Ц_i, \qquad (4.3)$$

де K_i – витрата i-го типу матеріалу, натуральні одиниці вимірювання;

$Ц_i$ – ціна за одиницю i-го типу матеріалу, грн.;

i – тип матеріального ресурсу;

n – кількість типів матеріальних ресурсів

Звідси, витрати на матеріальні ресурси дорівнюватимуть:

B_M =32000,00+36000,00+2000,00+30240,00+800,00=85920,00 грн.

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна за одиницю, грн.	Загальна сума, грн.
Маршрутизатор Cisco 2811	шт.	2	16000,00	32000,00
Комутатор 2960x-24	шт.	3	12000,00	36000,00
Ліцензія Data Encryption Standard (3DES) Image	шт.	1	2000,00	2000,00
Міжмережевий екран ASA - 5510	шт.	1	15120,00	15120,00
Ліцензія Cisco ASA 5510 Security Plus	шт.	1	800,00	800,00
Разом	-	9	-	85920,00

Загальна сума витрат на електроенергію розраховується за формулою:

$$B_E = \sum_{i=1}^{n} P_i \cdot k_i \cdot T_i \cdot Ц \,, \qquad (4.4)$$

де P_i – паспортна потужність i-го електрообладнання, кВт;

k_i – коефіцієнт використання потужності i-го електрообладнання (приймається 0.7 , 0.9);

T_i – час роботи i-го обладнання за весь період розробки, год;

$Ц$ – ціна електроенергії, грн / кВт·год;

i – тип електрообладнання;

n – кількість електрообладнання.

Для розробки проекту даної комп'ютерної мережі використовується один ПК потужністю P = 0,22 кВт з монітором потужністю P = 0,013 кВт, який за весь

період розробки працює 21 годину, та друкуючий пристрій потужністю P = 0,37 кВт, який працює 2 години.

$$B_E=0,9*(0,22+0,013)*21*0,9+0,9*0,37*2*0,9=5,16 \text{ грн}$$

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Для визначення амортизаційних відрахувань застосуємо метод прямолінійного списання. Загальна сума амортизаційних відрахувань (B_{AM}) визначається за формулою:

$$B_{AM} = \sum_{i=1}^{n} \frac{B_i \cdot H_i}{100}, \qquad (4.5)$$

де B_i – вартість i-го обладнання на початок звітного періоду, грн.;

H_i – річна норма амортизації i-го обладнання, %;

i – тип обладнання;

n – кількість обладнання.

Для проектування даної комп'ютерної мережі використовуються один ноутбук вартістю 17800 грн., та принтер вартістю 7350 грн.

Тоді:

$$B_{AM} = \frac{17800 \cdot 10}{100} + \frac{7350 \cdot 20}{100} = 3250,00 \text{ грн.}$$

Транспортні витрати слід прогнозувати у розмірі 8-12 % від загальної суми матеріальних витрат.

$$B_T = 0.08 \cdot B_M , \quad (4.6)$$

де B_T – транспортні витрати.

$$B_T = 0{,}08*85920{,}00=6873{,}6 \text{ грн.}$$

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 60-100 % від суми основної та додаткової заробітної плати працівників.

$$H_B = 0{,}7 \cdot B_{ОП} , \quad (4.7)$$

де H_B – накладні витрати.

$$H_B=0{,}7\cdot 2813{,}64=1969{,}55 \text{ грн.}$$

Загальні витрати ($B_{КС}$) розрахуємо за формулою:

$$B_{КС}= B_{ОП} +B_Ф+B_М+B_Е+ B_{АМ}+ B_Т+H_B \quad (4.8)$$

Результати проведених розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 – Кошторис витрат

Зміст витрат	Сума, грн.
1	2
Витрати на оплату праці (осн. і дод. ЗП)	2813,64
Відрахування на соціальні заходи	576,80

Продовження таблиці 4.4

1	2
Матеріальні витрати	85920,00
Витрати на електроенергію	5,16
Амортизаційні відрахування	3250,00
Транспортні витрати	6873,6
Накладні витрати	1969,55
Разом по кошторису	101408,75

4.2 Розрахунок ціни проекту

Договірна ціна ($Ц_Д$) для проектних рішень розраховується за формулою:

$$Ц_Д = B_{КС} \cdot \left(1 + \frac{p}{100}\right), \quad (4.9)$$

де $B_{КС}$ – кошторисна вартість, грн.;

p – середній рівень рентабельності, % (приймаємо 26% за погодженням з керівником).

$$Ц_Д = 101408,75 \cdot (1+0,26) = 127775,02 \text{ грн.}$$

4.3 Визначення економічної ефективності і терміну окупності капітальних вкладень

Економічна ефективність (E_P) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = \frac{Цд - B_{КС}}{B_{КС}}, \quad (4.10)$$

де $Цд$ – договірна ціна, грн.;

$B_{КС}$ – кошторисна вартість, грн..

$$E_p = 26366,27 \text{ грн.} / 101408,75 \text{ грн.} = 0,26.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_p = \frac{1}{E_p}. \quad (4.11)$$

Тобто:

$$T_P = 1/0,26 = 3,8 \text{ р.}$$

Прийнятним вважається термін окупності близький до 7 років.

Розраховані економічні показники проекту занесемо до таблиці 4.5.

Таблиця 4.5 Економічні показники розробки

Показник	Значення
Собівартість, грн.	101408,76
Плановий прибуток, грн.	26366,27
Ціна, грн.	127775,02
Економічна ефективність	0,26
Термін окупності, рік	3,8

Враховуючи основі економічні показники з таблиці 4.5, можна зробити висновок, що при економічній ефективності 0,26 та терміні окупності – 3,8 роки, і проектування, і розробка цієї корпоративної мережі є економічно доцільними. Як можна побачити із розрахунків, основними є матеріальні витрати. Тому, для зменшення грошових затрат на розробку даної мережі, має сенс здійснення закупівлі обладнання у офіційних дилерів вказаних марок обладнання.

ВИСНОВКИ

В ході виконання дипломного проекту були вирішені основні завдання побудови корпоративної мережі малого підприємства із застосуванням технології VLAN.

1. Виконано аналіз існуючої мережі, в ході якого було вирішено вибрати технологію VLAN.

2. Проведено теоретичне ознайомлення з технологією VLAN, можливості реалізації, тенденції розвитку, його переваги та недоліки.

3. Була побудована функціональна модель корпоративної мережі програмі Cisco Packet Tracer, де були використані образи справжнього обладнання.

4. Проведено конфігурацію клієнтських маршрутизаторів, а саме налаштовано протокол маршрутизації з клієнтом.

5. Налаштовано EIGRP всередині мережі провайдера, в якості протоколу маршрутизації для VLAN; налаштовано Рег- VLAN Spanning Tree (PVST), що призначений для роботи з декількома VLAN.

Результати бакалаврської роботи апробовані на інтернет-конференції "Інтелектуальні комп’ютерні системи та мережі" (додаток В).

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вито А. Основы организации сетей Cisco, том 1. М.: Издательский дом "Вильяме", 2004. 512с.
2. Вито А. Основы организации сетей Cisco, том 2. М.: Издательский дом "Вильяме", 2004. 464с.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М.: Информатика. Компьютеры, 2003. 1106с.
4. Таненбаум Э. Компьютерные сети. СПБ.: Информатика. Компьютеры, 2003. 992с.
5. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство, 3-е изд., с испр. [Текст]: Пер. с англ. М.: ООО «И. Д. Вильямс», 2007. 994.
6. Кульгин М. Технологии корпоративных сетей. Изд. «Питер», 1999. 402с.
7. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М.: Радио и связь, 2000. 512с.
8. Соколов Н.А. Эволюция местных телефонных сетей. Издательство ТОО "Типография "Книга", Пермь, 1994. 448с.
9. Соколов Н.А. Сети абонентского доступа. Принципы построения. Пермь, "Энтер-профи", 1999. 250с.
10. Филимонов А. Построение мультисервисных сетей Ethernet [Текст] СпБ. 2007. «БХВ-Петербург».
11. Бахтеяров П. Основы построения Metro Ethernet сетей [Текст]. // Вестник связи. 2004. Вып. №10. С. 45-51.
12. Руководство по Cisco IOS [Текст]. СПб.: Питер, М.: Издательство «Русская Редакция». 2008. 784 с

13. Росляков А.В., Самсонов А.В. IP-телефония. М.: Эко-Трендз, 2003. 252 с.

14. Официальный сайт произвоизводителя оборудования Cisco Systems [Електронний ресурс]. Режим доступу: http://www.cisco.com.

15. Optix OSN 3500 Интеллектуальная система оптической передачи Техническое руководство. Описание системы.

16. Транспортные сети и системы электросвязи. Системы мультиплексирования: Учебник для студентов ВУЗов по специальности «Телекоммуникации» [Текст] / Под ред. В.К. Стеклова. К.; 2003. 352 с.

17. Официальный сайт компании D-Link. Техническое описание медиаконвертора DMC-920 [Електронний ресурс]. Режим доступу: http://ftp.dlink.ru/pub/transciever_mediaconverter/DMC-920/Data_sh.

18. Дональд Дж. Стерлинг. Техническое руководство по волоконной оптике [Текст] / пер. Московченко А. Издательство «ЛОРИ».1998.

19. Основы организации сетей Cisco, том 1 [Текст] / Пер. с англ. М.: Издательский дом «Вильямс», 2002. 512 с.

20. Портнов, Э.Л. Оптические кабели связи [Текст]. М. «Информсвязь», 2000 – 112 с.

21. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство, 3-е изд., с испр. [Текст] / Пер. с англ. М.: ООО «И. Д. Вильямс», 2007. 994.

22. Слепов Н.Н. Оптоволоконные системы дальней связи. Перспективы развития [Текст]. Электроника: НТБ. 2005. Вып.6.

23. Величко В.В., Субботин Е.А., Величко В.В., Шувалов В.П., Ярославцев А.Ф. Телекоммуникационные системы и сети: Учебное пособие в 3-х томах. Том 3. Мультисервисные сети [Текст] / под ред. профессора В.П. Шувалова. М.: Горячая линия. Телеком, 2005. 592 с.

24. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102 «Комп’ютерна інженерія» фахового спрямування «Комп’ютерні системи та мережі» / О.М. Березький, Л.О.Дубчак, Р.Б. Трембач, Г.М. Мельник, Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. Тернопіль: ТНЕУ, 2016. 60 с.

25. Гураль І.В., Дубчак Л.О. Методичні вказівки до оформлення курсових проектів, звітів про проходження практики, випускних кваліфікаційних робіт для студентів спеціальності «Комп’ютерна інженерія» / Під ред. О.М. Березького. Тернопіль: ТНЕУ, 2019. 33 с.

26. Методичні вказівки до написання техніко-економічного розділу дипломних проектів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050102 комп’ютерна інженерія/ І.Р. Паздрій. Тернопіль: ТНЕУ, 2014. 37 с.