

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проекту з дисципліни
"Технології проектування телекомунікаційних мереж"
для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні
програми «Комп'ютерні системи та мережі» та «Спеціалізовані
комп'ютерні системи», усіх форм навчання

Методичні вказівки до виконання курсового проекту з дисципліни "Технології проектування телекомунікаційних мереж" для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні програми «Комп'ютерні системи та мережі» та «Спеціалізовані комп'ютерні системи», усіх форм навчання / Укл. Г.Г.Киричек. – Запоріжжя: НУ «Запорізька політехніка», 2020.– 30 с.

Укладач:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 2 від 04.09.2020

Рекомендовано до видання
НМК КНТ
Протокол № 2/1 від 15.09.2020

ЗМІСТ

1 Загальні відомості	4
1.1 Календарний план та отримання завдання	4
1.2 Загальні питання проведення досліджень	6
1.3 Вимоги до змісту розділів, оформлення та обсягу пояснювальної записки	8
1.4 Теми проектів	10
1.5 Порядок захисту курсового проекту	12
2 Структура курсового проекту	13
2.1 Аналіз технічного завдання	14
2.2 Вибір технологій та обладнання телекомунікаційної мережі	16
2.3 Планування структури кожної ЛОМ об'єднаної мережі	18
2.4 Моделювання мережі. Системи моделювання	19
2.5 Технологія VPN	20
2.6 Забезпечення мережної безпеки	22
2.7 Забезпечення мережної безпеки в бездротових ЛОМ	25
3 Загальні вимоги до оформлення курсового проекту	26
3.1 Вимоги до оформлення пояснювальної записки	26
3.2 Вимоги до оформлення графічних документів	27
3.3 Вимоги до виконання схем	28
Рекомендована література	29
Додаток А	30

1 ЗАГАЛЬНІ ВІДОМОСТІ

Мета проектування – проведення досліджень та отримання науково-професійних знань і практичних навичок з питань реалізації телекомунікаційної мережевої інфраструктури, структурованої кабельної та бездротової систем, узагальнення, закріплення та поглиблення теоретичних та практичних знань зі спеціальності; використання цих знань для обґрунтованого прийняття проектних рішень та для вирішення конкретних науково-практичних задач при реалізації технологій телекомунікаційних мереж. Отримання науково-практичних знань з організації доступу та зв'язку між загальними об'єктами мережі Internet. Вміння обирати технології, методи та засоби проектування, реалізації, адміністрування та захисту, як локальних, так і глобальних телекомунікаційних мереж.

Завдання до курсового проекту передбачають: розробку телекомунікаційної мережевої інфраструктури підприємства, згідно з отриманим варіантом (загальна кількість кінцевих вузлів не менше 500, віддалених локальних мереж не менше 4); побудову моделі та планування і розробку кожної локальної мережі; монтаж телекомунікаційної мережі, згідно структурної схеми; налаштування обладнання телекомунікаційної мережі; з'єднання через маршрутизатори окремих локальних мереж підприємства; налаштування віддаленого доступу з використанням тунелів та підключення телекомунікаційної мережі до мережі Internet з забезпеченням мережної безпеки.

Примітка. Варіанти розподіляються між студентами згідно двом останнім цифрам залікової книжки з кратністю 25. Для прикладу, якщо дві останні цифри 03- варіант № 3, а якщо 87- варіант № 12 ($87-25-25-25=12$).

1.1 Календарний план та отримання завдання

Систематичне і своєчасне виконання роботи – запорука одержання якісного результату і високої оцінки.

Рекомендований графік роботи наведено в таблиці 1.1. Студент може корегувати графік в межах наведених дат, не змінюючи дати захисту.

Таблиця 1.1 - Етапи виконання курсового проекту

№ п/п	Назва етапів курсового проекту	Термін виконання
1	Аналіз технічного завдання (структури підприємства, розрахунок об'єму загального трафіку та швидкості каналів зв'язку)	до 20.09
2	Побудова моделі телекомунікаційної мережі	21.09 – 30.09
3	Аналіз, порівняння та вибір технологій організації телекомунікаційної мережі	01.10 – 8.10
4	Розробка структурної схеми телекомунікаційної мережі підприємства	09.10 – 15.10
5	Аналіз, порівняння та вибір мережного, серверного і клієнтського обладнання	16.10 – 23.10
6	Монтаж телекомунікаційної мережі	24.10 – 31.10
7	Налаштування обладнання	01.11 – 07.11
8	Організація віддаленого доступу до мережі, отримання пулу відкритих адрес	08.11 – 14.11
9	Вибір та налаштування протоколів маршрутизації телекомунікаційної мережі підприємства	15.11 – 20.11
10	Налаштування маршрутизаторів, згідно політики безпеки телекомунікаційної мережі підприємства підключення до Інтернет	21.11 – 25.11
12	Забезпечення мережевої безпеки	26.11 – 01.12
13	Оформлення графічного матеріалу (моделі, структурна схема, монтажні схеми)	02.12 – 04.12
14	Оформлення ПЗ	05.12 – 08.12
15	Захист КП	до 20.12

У відповідності до теми керівник затверджує технічне завдання на курсовий проект з вказівкою термінів виконання окремих етапів та всього проекту в цілому (в перші 2 тижня від початку семестру).

У завданні треба чітко визначити такі данні: назва проекту; вихідні данні до проектування із зазначенням кількості підключаємих об'єктів (мереж), кількості та видів обладнання, фізичного середовища каналів зв'язку та мережних (LAN та WAN) технологій; перелік загальних питань, які розглядаються (перелік основних розділів змісту) та перелік графічного матеріалу (моделі, структурна схема, монтажні схеми, алгоритми роботи). Календарний графік виконання курсового проекту, який складається студентом (за прикладом календарного плану) і затверджується керівником проекту, повинен відповідати етапам розробки, аналізу та вирішенню загальних питань стосовно до всього об'єкту проектування в цілому.

1.2 Загальні питання проведення досліджень

Проектування виконується з використанням відповідних методів і інструментальних засобів (систем моделювання) [1,2].

Методи, які використовуються: аналіз - розкладання мережі на складові частини і вивчення їх окремо; синтез - об'єднання в єдину систему отриманих результатів проведеного аналізу, що дозволяє сконструювати щось нове; аналогія - висновок про подібність двох мереж за якими-сь ознаками на підставі встановленої їх подібності; моделювання - вивчення об'єкта за допомогою моделей з перенесенням отриманих характеристик на оригінал. Предметне моделювання - створення моделей зменшених копій з певним оригінальними властивостями. Математичне моделювання - заміна реальної системи на абстрактну, в результаті чого задача перетворюється в математичну. Знакове або символічне - використання формул, креслень. Комп'ютерне моделювання – модель мережі відтворюється у комп'ютерній програмі.

Метою роботи є проведення дослідження, розробка методів і моделей, застосування засобів проектування, реалізації, функціонування, вдосконалення, адміністрування та захисту телекомунікаційних мереж різного функціонального призначення.

Відповідно до поставленої мети в роботі можливе **вирішення наступних задач**: проведення системного аналізу архітектурних та інформаційних особливостей телекомунікаційних мереж; виконання

аналізу джерел і ступеня впливу службового і широкомовного трафіку на характеристики функціонування телекомунікаційних мереж; визначення правил вибору структури мережних об'єктів; розроблення алгоритму об'єктно-орієнтованої декомпозиції телекомунікаційної мережі; розроблення інформаційної (математичної) моделі мережі із різними каналами зв'язку; моделювання, проектування, налаштування, адміністрування та захист телекомунікаційних мереж.

Об'єктом дослідження є телекомунікаційні мережі різного функціонального призначення.

Предметом дослідження є моделі і методи проектування та реалізації телекомунікаційних мереж.

Методи дослідження. Для досягнення поставленої мети, при виконанні етапів проектування, рекомендовано використовувати наступні методи дослідження: системний аналіз, для дослідження механізмів функціонування програмно-апаратних засобів телекомунікаційних мереж; об'єктно-орієнтовані методи проектування (побудова загальної моделі телекомунікаційних мереж); методи теорії обчислювальних систем і теорії масового обслуговування для побудови та розрахунку математичних моделей, що відображають імовірнісні характеристики функціонування телекомунікаційних мереж; методи натурного моделювання для верифікації розроблених моделей телекомунікаційних мереж.

Наукову новизну проектів становлять: вибір структури мереж різних рівнів ієрархії, які дозволяють синтезувати неблокуючі мережеві структури телекомунікаційних мереж, мінімальні за вартістю; декомпозиція мережі (мережа у вигляді інформаційно ізольованих мережних об'єктів); проектування мережових структур (оптимальних за критерієм "продуктивність/вартість"); врахування впливу службового та широкомовного трафіку на транзакції абонентів мережі; інформаційна та математичні моделі комутаторів, які дозволяють розраховувати характеристики функціонування як локальних, так і віддалених абонентів, підключених до комутатора.

Практичне значення отриманих результатів може включати: розробку загальної структури з урахуванням математичної моделі і розрахунку характеристик реального каналу зв'язку; розрахунок об'єму буферів комутаторів мереж на етапах проектування і модернізації; розробку процедури моделювання імовірнісно-часових характеристик функціонування телекомунікаційних мереж;

проектування оптимальної структури мережі за критерієм "продуктивність/вартість" на етапах проектування і модернізації; методи та інструментальні засоби впроваджені при проектуванні мережі за варіантом [3].

1.3 Вимоги до змісту розділів, оформлення та обсягу пояснювальної записки

До пояснювальної записки необхідно включати матеріал, який безпосередньо відноситься до розробки конкретної телекомунікаційної мережі, яка підлягає проектуванню, у відповідності до технічного завдання. Не рекомендується робити великі реферативні огляди. При необхідності можна робити посилання на відповідну літературу. Треба мати на увазі, що записку складають тоді, коли розробку проекту завершено, всі рішення прийнято, всі деталі є відомими, є кінцевий результат, і саме його необхідно привести разом з аргументацією вибору рішень, необхідними розрахунками, графіками, таблицями, рисунками, матеріалами, які обґрунтовують прийняті рішення.

Приблизний рекомендований обсяг кожного розділу наведено нижче. Назви розділів у конкретній роботі можуть відрізнятися від наведених далі, послідовність розташування розділів може бути іншою, але в цілому у пояснювальній записці рекомендовано висвітлити всі питання.

У рефераті проектант вказує мету, об'єкт та предмет дослідження; технології, вид обладнання, протоколи та стандарти, які використані у розробленому проекті. Наводить ключові слова та об'єм пояснювальної записки. Реферат рекомендовано оформити на заключному етапі (1 сторінка). Приклад реферату у додатку Д.

У вступі до проекту магістр повинен обґрунтувати актуальність проектування телекомунікаційної мережі за варіантом, навести методи та шляхи проведення досліджень, зазначити в яких розділах пояснювальної записки наведено аналіз структури організації, схема інформаційних потоків (трафіку), аналіз, порівняння та вибір технологій (локальних мереж та підключення віддалених мереж), комунікаційного обладнання, а також етапи, методи, алгоритми та

моделі проектування реальних каналів зв'язку, визначення етапів та способів налаштування, адміністрування та технології захисту мережі. Вступ має бути коротким (1-2 сторінки) і чітким. Головне, щоб було зрозуміло, чому присвячено дослідження і етапи проектування.

У першому розділі (6-10 сторінок) ПЗ необхідно провести аналіз технічного завдання, розглянути структуру підприємства в цілому та проаналізувати загальний обсяг трафіку, визначити необхідну швидкість каналів зв'язку та яке обладнання потребує заміни і яке необхідно придбати додатково для підключення віддалених об'єктів телекомунікаційної мережі. Студент повинен чітко визначити коло задач, які необхідно вирішити в курсовому проєкті, а також сформулювати технічне завдання згідно діючих стандартів та оформити його окремим підрозділом.

У другому розділі (10-12 сторінок) на підставі проведеного аналізу розробляється модель та структурна схема телекомунікаційної мережі, виконується обґрунтування вибору та опис LAN\WAN-технологій окремих сегментів телекомунікаційної мережі. Кількість підключених робочих станцій не повинна бути меншою за 500 одиниць.

Третій розділ (10-12 сторінок) повинен містити опис апаратної та кабельної частини проєкту з урахуванням попереднього вибору та можливості з'єднання через маршрутизатори окремих ЛОМ підприємства, з метою здійснення віддаленого доступу. Цей розділ містить вибір конкретних елементів реалізації функціональної та принципів електричних схем, розрахунків окремих елементів, вузлів та підсистем. Виконується налаштування загальних об'єктів.

У четвертому розділі (4-10 сторінок) розглядається підключення розробленої мережі до Internet та питання забезпечення мережевої безпеки, як у дротових так і в бездротових ЛОМ. Проектантом розкриваються питання забезпечення якості та надійності розробленої мережі, питання апаратного та програмного захисту інформації, а також захист від несанкціонованого доступу. Розглядається призначення IP-адрес та подання мережі організації (підприємства) в Інтернеті.

У висновках (1-2 сторінки) проєктанти формують основні результати, що отримані під час виконання курсового проєкту.

Оформлення записки здійснюється у відповідності до діючих стандартів ДСТУ 3008-95 “Документація. Звіти в сфері науки і техніки”, Єдиної Системи Конструкторської Документації (ЕСКД), у відповідності до ГОСТ 19.701-90 (Схемы алгоритмов, программ,

данных и систем). Бібліографічні описи в переліку посилань наводять відповідно до чинних стандартів з бібліотечної та видавничої справи відповідно ДСТУ ГОСТ 7.1:2006 "Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання". Приклад оформлення бібліографічного опису наведено у додатку А.

До записки додаються два креслення формату А4 або А3 (структурна та монтажна схеми) та 1 плакат (алгоритм роботи мережі) того ж формату. Креслення і плакати повинні відображати проходження кабелю на всіх ділянках мережі з роз'ясненням особливостей його прокладки.

Загальний обсяг ПЗ – 40 - 45 сторінок (не рекомендовано обсяг більший за 45 стор.), причому технічна її частина, має містити не менш ніж 30 сторінок тексту з рисунками.

1.4 Теми проектів

Далі наведено теми проектів (табл. 1.2) за варіантами (див. сторінку 4).

Таблиця 1.2 – Теми проектів

№	Тема	Технології LAN	Технології WAN
1	Розподілена мережа провайдера для мешканців мікрорайонів м. Запоріжжя.	Ethernet 100BaseT, WiFi	FrameRelay, 1GBaseSX
2	Оптоволоконна мережа БАТ «Дніпроспецсталь» з п'ятьма філіалами.	Ethernet 100BaseT, VLAN, WiFi	VPN (GRE)
3	Розподілена комп'ютерна мережа державного підприємства «Екологія України» (об'єкти у різних географічних частинах України).	Ethernet 10BaseT, 100BaseTX	ACL, 1GBaseSX
4	Розподілена мережа провайдера для мешканців та відпочивальників азовського побережжя.	Ethernet 100BaseTX, WiFi	Ethernet 1000BaseSX

Продовження таблиці 1.2

5	Розподілена комп'ютерна мережа концерну «Теплові мережі України» (6 віддалених об'єктів).	Ethernet 100BaseT, VLAN, WiFi	MPLS
6	Розподілена комп'ютерна мережа «Дніпровська електроенергетична система» України (об'єкти у різних географічних частинах України).	Ethernet 100BaseT, 1GBaseSX, WiFi	VPN (IPSec)
7	Корпоративна комп'ютерна мережа металургійного підприємства з трьома віддаленими філіями.	Ethernet 100BaseF, VLAN, WiFi	VPN (GRE)
8	Розподілена мережа передачі даних для головних офісів банку (об'єкти у різних містах України).	Ethernet 100BaseTX, WiFi	VPN (IPSec) VoIP
9	Мережа БАТ «Мотор-Січ» з чотирма віддаленими філіями.	Ethernet 100BaseTX, VLAN, WiFi	FrameRelay
10	Розподілена комп'ютерна мережа супермаркетів «Сільпо» м. Запоріжжя.	Ethernet 100BaseT, 1GBaseSX	VPN (IPSec) VoIP
11	Розподілена комп'ютерна мережа підприємства «Центромеблі» (об'єкти у різних містах України).	Ethernet 100BaseTX, VLAN	FrameRelay ACL
12	Розподілена комп'ютерна мережа БАТ «Укртелеком».	Ethernet 100BaseTX, VLAN	Ethernet 1000BaseSX ACL
13	Розподілена комп'ютерна мережа військових об'єктів (7 віддалених об'єктів).	Ethernet 100BaseT, WiFi	VPN (IPSec) VoIP, ACL
14	Розподілена комп'ютерна мережа комунального підприємства «Водоканал» в Запорізькій області.	Ethernet 100BaseTX, 1GBaseSX	IPv6 ACL
15	Розподілена комп'ютерна мережа ЗАТ «Запорізький залізорудний комбінат».	Ethernet 100BaseTX, WiFi	VPN (IPSec) VoIP, ACL
16	Розподілена комп'ютерна мережа підтримки проведення соціологічних досліджень.	Ethernet 100BaseTX, VLAN	Ethernet 1000BaseSX ACL
17	Розподілена комп'ютерна мережа шкіл м. Запоріжжя.	Ethernet 100BaseTX, WiFi, ACL	VPN (IPSec), VoIP

Продовження таблиці 1.2

18	Розподілена комп'ютерна мережа енергетичного комплексу БАТ «УкрЕнерго».	Ethernet 100BaseTX, WiFi	FrameRelay, 1GBaseSX,
19	Розподілена комп'ютерна мережа регіональних бібліотек (об'єкти у різних містах України).	Ethernet 100BaseTX, VLAN, WiFi	VPN (GRE)
20	Розподілена комп'ютерна мережа філіалів торговельної фірми (об'єкти у різних містах України).	Ethernet 100BaseTX, WiFi, VoIP,	VPN (IPSec) ACL
21	Розподілена мережа податкової служби України (об'єкти у різних містах України).	Ethernet 100BaseTX, WiFi	1GBaseLX, ACL
22	Корпоративна мережа регіональних лікарень України (об'єкти у різних містах України).	Ethernet 100BaseTX, VLAN, WiFi	MPLS
23	Розподілена комп'ютерна мережа банку з розвинутою системою банкоматів.	Ethernet 100BaseTX, 1GBaseSX, WiFi	VPN (IPSec)
24	Розподілена комп'ютерна мережа Укрзалізниці (об'єкти у різних містах України).	Ethernet 100BaseFX, VLAN, WiFi	VPN (GRE)
25	Корпоративна мережа агропромислового комплексу «Україна» (об'єкти у різних географічних частинах України).	Ethernet 100BaseTX, WiFi	VPN (IPSec) VoIP

1.5 Порядок захисту курсового проекту

Призначення захисту – оцінити складність розробленого проекту, кваліфікацію проектанта і ступінь самостійності його праці.

Захист відбувається за графіком у присутності комісії з двох викладачів, один з яких є керівником курсового проекту. На доповідь дається 4-5 хвилин. За цей час необхідно стисло викласти зміст поставленої задачі (одна хвилина), доповісти про власну роботу щодо розробки телекомунікаційної мережі підприємства (2-3 хвилини) і зробити висновки (одна хвилина). Необхідно розповідати про свою

власну роботу, пояснювати, чому прийнято саме такі рішення при проведенні досліджень та проектуванні мережі, а також на основі яких міркувань обрано те або інше обладнання та технології проектування і підключення ЛОМ телекомунікаційної мережі підприємства.

Після закінчення доповіді учасники комісії можуть задавати питання, призначення яких – уточнити рівень кваліфікації і ступень самостійності доповідача. На питання необхідно давати стислі прямі відповіді, при необхідності ілюструючи їх відповідними кресленнями.

2 СТРУКТУРА КУРСОВОГО ПРОЕКТУ

В процесі проектування телекомунікаційної мережі студенту рекомендовано розглянути наведені нижче питання, тримаючись загального плану проекту за варіантом.

Основні етапи проектування можуть включати.

Вступ. Аналіз технічного завдання: дослідження та аналіз структури підприємства (з описом основних підрозділів і філій, з урахуванням їх віддаленості); аналіз інформаційних потоків (обчислення загального трафіку з визначенням необхідної швидкості каналів зв'язку); аналіз (для модернізації) наявних апаратних і мережних пристроїв; побудова моделі мережі; постановку завдань, пов'язаних з проведенням досліджень, аналізом, порівнянням та вибором методів за засобів проектування. Вибір технологій, апаратних і мережних пристроїв: проведення аналізу, наявних LAN і WAN технологій, порівняння та вибір технологій (певних специфікацій) для конкретних каналів зв'язку у LAN мережах підприємства та WAN між мережами вашої організації, з урахуванням підключення філій; дослідження, аналіз технічних характеристик та вибір мережних пристроїв з визначенням кожного конкретного пристрою або групи ідентичних пристроїв, опис їх призначення та особливості застосування; аналіз технічних характеристик та вибір апаратних пристроїв (сервери, ПК, ноутбуки, термінали, планшети, IP-телефони та ін.) З описом характеристик кожного пристрою або групи пристроїв, опис призначення та особливості застосування. Монтаж та налаштування мережі: визначення основних LAN і WAN сегментів, проектування структурної схеми телекомунікаційної мережі; побудова

монтажної схеми (розміщення мережевих і апаратних пристроїв (в будівлях, на поверхах, в кімнатах)); розрахунок потужності антен; підключення (фізичне об'єднання мережних і апаратних пристроїв єдину мережу); вибір принципу адресації та маршрутизації для LAN і WAN сегментів (мереж); програмна настройка всього мережного обладнання (з урахуванням адресації і маршрутизації). Адміністрування мережі. опис настроювання віддаленого доступу до філій (технології створення тунелів між LAN підприємства (див. методичні вказівки до лабораторних робіт)); підключення до Інтернет; забезпечення мережевої безпеки (налаштування обладнання, протоколів). Висновки.

Кількість і назви розділів у проекті можуть відрізнятись від наведених але це не повинно впливати на загальну мету проектування.

2.1 Аналіз технічного завдання

У цьому розділі необхідно провести системний аналіз телекомунікаційної мережі згідно варіанту. Визначити складові частини об'єктно-орієнтованого підходу до проектування, враховуючи структуру корпорації, її функціональні особливості, віддаленість об'єктів та вид і об'єм інформаційних потоків (трафіку). Враховуючи загальний об'єм трафіку, визначити необхідну швидкість усіх реальних каналів зв'язку (як в локальних так і між віддаленими об'єктами мережі підприємства). Провести аналіз мережних структур, які використовуються на різних рівнях ієрархії телекомунікаційної мережі. Показати, що типова структура телекомунікаційної мережі підприємства містить три системи – клієнтську, серверну і комунікаційну (або рівні доступу, розподілення та ядра) [3].

На нижньому рівні ієрархії знаходяться мережі робочих груп (або сегменти локальних мереж). На середньому рівні – мережі адміністративних груп (або локальні мережі). На верхньому рівні знаходиться телекомунікаційна мережа. На рисунку 2.1 наведена приблизна ієрархічна структура мережі.

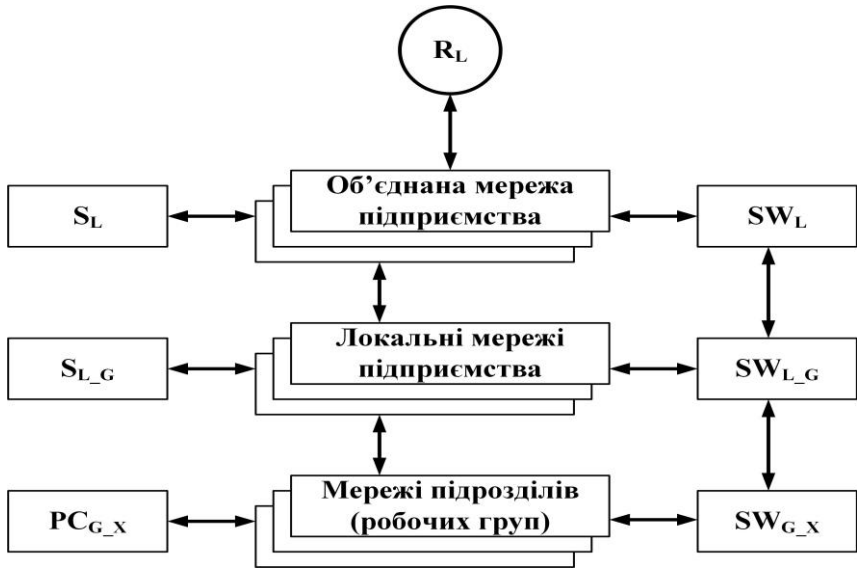


Рисунок 2.1 - Ієрархічна структура телекомунікаційної мережі підприємства.

Де маємо наступні об'єкти: PC_{G_X} , SW_{G_X} – комп'ютери та локальні комутатори підрозділів (робочих груп), S_{L_G} , SW_{L_G} – сервера та комутатори локальних мереж підприємства; S_L , SW_L , R_L – сервера, комутатори та маршрутизатори об'єднаної мережі підприємства. Де G це номер групи (підрозділу), X – номер елемента групи (підрозділу), а L – номер відповідної LAN мережі. Для аналізу мережі використовуються математичні методи і моделі масового обслуговування. Моделювання життєвого циклу комп'ютерної мережі проводиться по ітеративній моделі - це виконання робіт паралельно з безперервним аналізом отриманих результатів і коригуванням попередніх етапів роботи.

При проведенні аналізу інформаційного трафіку (обчислення загального трафіку з визначенням необхідної швидкості каналів зв'язку) можна скористатись рішенням подібних завдань. В ході вирішення поставленого завдання треба враховувати кількість клієнтів у сегменті мережі та об'єм трафіку для кожного з них. В автоматизованих проектних процедурах замість не існуючого об'єкта,

який проектується, оперують моделлю, яка відображає деякі характеристики, що цікавлять дослідника об'єкта. Математичні функціональні моделі в загальному випадку є алгоритмом обчислення вектору вихідних параметрів при заданих векторах параметрів елементів і зовнішніх параметрів [5].

2.2 Вибір технологій та обладнання телекомунікаційної мережі

Мета аналізу - отримання інформації про характер функціонування і значення вихідних параметрів при заданій структурі об'єкта, відомості про зовнішні параметри і параметри об'єктів. У мережі завжди використовується 3-4 технології, як канального рівня так і накладені поверх канального рівня, з використанням різних пристроїв. Важливо орієнтуватися у цьому обладнанні. Моделі комутаторів, маршрутизаторів та серверів, які були популярні торік, уже давно не є такими - на їх місце прийшли нові моделі, з кращими функціями та технічними показниками, які дозволяють ефективніше використовувати всю систему в цілому.

Корпоративна мережа повинна мати надлишкові маршрути та відповідати вимогам надійності для підтримки поетапної реалізації її плану. Тоді додаткові сегменти можуть додаватися в різних місцях при підключенні до маршрутизатора при розширенні мережі.

Поняття характеристики функціонування мережі включає вторинні властивості комп'ютерної мережі, які визначаються в процесі вирішення завдань аналізу, як функція параметрів. Параметри комп'ютерної мережі описують первинні властивості мережі і є вихідними даними при вирішенні задач аналізу. Характеристики комп'ютерних мереж – сукупність показників ефективності (якості) мережі. Характеристики комп'ютерних мереж можна розділити на якісні і кількісні [5].

Кількісні характеристики комп'ютерних мереж можна розділити на дві групи: глобальні, що визначають найбільш важливі властивості мережі як цілісного об'єкта; локальні, які визначають властивості окремих пристроїв або частин мережі і дозволяють отримати більш детальне уявлення про ефективність мережі.

Для оцінки продуктивності комп'ютерної мережі в цілому використовується наступна сукупність показників: продуктивність мережі передачі даних, яка вимірюється числом повідомлень (пакетів, кадрів, біт) по мережі за одиницю часу; продуктивність засобів обробки даних (представляє собою сумарну продуктивність усього обладнання мережі).

Продуктивність (комунікаційна потужність) може бути задана наступними показниками: максимальна або гранична продуктивність (пропускна спроможність) мережі, яка вимірюється кількістю пакетів (кадрів), переданих в мережі за одиницю часу; реальна або фактична продуктивність мережі передачі даних, яка може бути задана як середнє значення на деякому інтервалі часу або як миттєве значення в конкретний момент часу.

Продуктивність в цілому складається з продуктивності обчислювальних систем (ОС), які виконують обробку даних в мережі.

При виконанні проекту рекомендовано проаналізувати вище наведені характеристики продуктивності та надійності при використанні (виборі) одного (або декілька) видів технології Ethernet для використання в локальних мережах головних офісів та філій. При плануванні глобальних сегментів рекомендовано проаналізувати та порівняти характеристики продуктивності наступних технологій:

- **frame relay** – протокол канального рівня мережної моделі OSI. Технологія виникла з метою об'єднання локальних мереж каналами глобальних мереж, поєднання територіально розрізнених локальних мереж корпорації в єдину швидкісну корпоративну мережу, а також впровадженням новітніх досягнень в технології передачі глобальних мереж. Стандарти Frame Relay визначають два типи віртуальних каналів: PVC, (Permanent Virtual Circuit) постійний віртуальний канал та SVC (Switched Virtual Circuit) - віртуальний канал, що комутує. FR допускає змінну довжину кадру – від кількох байтів до 2000 байт. Гнучка зміна довжини кадру дає змогу налаштовуватися до зміни навантаження. Перед початком з'єднання користувачу забезпечують: гарантовану швидкість передавання інформації (Committed Information Rate, CIR) – швидкість з якою мережа буде передавати дані користувача; гарантовану величину пульсації (Committed Burst Size, Bc) – максимальна кількість байтів, яку мережа передає від даного користувача за інтервал часу T, який називаємо часом пульсації, дотримуючись гарантованої швидкості

передавання CIR; допоміжна величина пульсації (Excess Burst Size, Be) – максимальна кількість байтів, які мережа буде пробувати передавати зі зверх встановленого значення Bc за інтервал часу T. Якщо приведені вище величини відомі, то час T визначається наступною формулою:

$$T=Bc/CIR \quad (2.1)$$

Основним параметром за яким абонент і мережа заключає згоду при з'єднанні віртуального каналу, являється гарантована швидкість передачі даних. Для постійних віртуальних каналів ця згода являється частиною контракту на користування послугами мережі [6];

– **технологія асинхронного режиму передачі даних (Asynchronous Transfer Mode, ATM)** - комунікаційна технологія, яка об'єднує принципи комутації пакетів і каналів при передачі інформації різного типу. Розрахована на високі швидкості передачі і різні види навантаження. Передає всі види різнорідного трафіку (цифрові, голосові і мультимедійні дані) по одним і тим же системам і лініях зв'язку. Швидкість передачі в магістралях ATM - 155Мбіт / с (STM1) - 2,5 Гбіт / с (STM16). Орієнтована на з'єднання з пакетним способом комутації із забезпеченням заданої якості обслуговування (Quality of Service). Перетворює всі види навантаження в потік комірок (cell). Еталонна модель протоколів ATM (BISDN) містить три площини: користувача (U-plane) - передача і прийом всіх видів даних, забезпечення управління потоком і захист від помилок, має рівневу структуру; управління (C-plane) - протоколи, які використовуються для сигналізації при встановленні, контролі і роз'єднанні з'єднання, має рівневу структуру; менеджменту (адміністративного управління) (M-plane) – має дві площини: адміністративне управління рівнями площин і управління площинами. ATM підтримує 2 типи з'єднань: "точка-точка" і "точка - три крапки" [6].

2.3 Планування структури кожної ЛОМ об'єднаної мережі

Створення плану мережної інфраструктури - найважливіша частина проектування мережі. Як правило, не всі елементи

інфраструктури мережі доводиться проектувати "з нуля", деякі з них успадковуються від інших елементів.

Планування інфраструктури набагато складніше інших етапів побудови мережі, оскільки припускає створення плану, який буде використаний для монтажу мережі і підтримки її надалі. На плані треба зазначити розміщення основних компонентів мережі: кабельних ліній, комутаторів, серверів, маршрутизаторів і інших комунікаційних пристроїв, а також комп'ютерів і периферії. Знаючи, які протоколи каналного рівня обрані для мережі, можна приступати до планування розміщення мережних ресурсів, тому що від протоколу залежить максимальна довжина кабелю і число комутаторів у мережі. Вибір протоколу каналного рівня в основному зводиться до вибору типу фізичного середовища: витой пари, оптоволоконного кабелю і частоти для бездротових каналів. Кожний тип має свої переваги та недоліки, які потрібно врахувати при виборі середовища передачі. Швидкість передачі - важливий критерій вибору протоколу каналного рівня.

Розміщення серверів повинне бути зручним для тих, хто їх підтримує та обслуговує. У кожному разі захист серверів повинен бути надійним. Їх необхідно захищати не тільки від фізичного доступу, але також від стрибків напруги та перебоїв струму. Розміщення сервера повинне враховувати розташування робочих місць користувачів, характер трафіку і бути зручним для обслуговуючого персоналу. При проектуванні рекомендовано визначитись з розміщенням обладнання з застосуванням загальних стандартів СКС, враховуючи організацію основних підсистем СКС структурних елементів корпорації [7].

2.4 Моделювання мережі. Системи моделювання

Комп'ютерні мережі стають більш складними, тому і їх проектування суттєво ускладнюється. Студенти проектують комп'ютерну мережу під конкретне підприємство у відповідності до поставлених завдань, тому їх рішення повинні бути достатньо оптимальними. Тому при проектуванні корпоративних мереж підприємств доцільно застосовувати засоби імітаційного моделювання комп'ютерних мереж. При цьому існує достатньо велика кількість

програмних засобів моделювання комп'ютерних мереж будь-якої складності та типу. Найбільш поширені для використання в навчальному процесі засоби моделювання мереж, які є вільним програмним забезпеченням і не поступаються функціональністю своїм комерційним аналогам, це GNS3, NS3 та доступний учасникам СНА засіб Packet Tracer. Вони підтримують локальні та глобальні мережі і дозволяють моделювати мережі будь-якої топології і складності.

Packet Tracer - автономне, засноване на моделюванні навчальне середовище для проектування і дослідження обчислювальних мереж CCNA-рівня складності. Packet Tracer передбачає моделювання, візуалізацію і анімацію подій в мережі. Packet Tracer містить спрощені моделі мережних пристроїв та протоколів. Програмне забезпечення Cisco Packet Tracer дозволяє імітувати роботу різних мережних пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, комп'ютерів, мережних принтерів, IP-телефонів і т.д. Робота з симулятором дає досвід налаштування реальної мережі, яка може включати в себе десятки чи сотні пристроїв. Завдяки такій функції Cisco Packet Tracer, як режим візуалізації, користувач може відстежити переміщення даних по мережі, появу і зміну параметрів IP-пакетів при проходженні даних через мережеві пристрої, швидкість і шляхи переміщення IP-пакетів. Аналіз подій, які відбуваються в мережі, дозволяє зрозуміти механізм її роботи і виявити несправності.

Виходячи з того, що в курсі проектування комп'ютерних мереж при виконанні лабораторних робіт використовується програмний продукт Cisco Packet Tracer, студентам рекомендовано його використання і в процесі моделювання корпоративної мережі. Але це не є обов'язковим, можливе застосування іншого з засобів імітаційного моделювання комп'ютерних мереж [6].

2.5 Технологія VPN

Технологія VPN використовує передові технології шифрування і тунелювання для створення безпечного з'єднання через Інтернет. Основою для безпеки VPN є конфіденційність даних, цілісність даних та автентифікація. VPN забезпечує конфіденційність за рахунок використання механізмів інкапсуляції та шифрування. Для

забезпечення цілісності даних VPN, як правило, використовують хешування. Для автентифікації VPN може використовувати паролі, цифрові сертифікати, смарт-карти і біометрію для ідентифікації на кінці мережі. Використання можливостей конфіденційності даних в VPN гарантує, що тільки визначені відправники та отримувачі здатні інтерпретувати оригінальний зміст повідомлення.

Тунелювання дозволяє використовувати публічні мережі для передачі даних для користувачів так, ніби користувачі мали доступ до приватної мережі. Тунелювання інкапсулює весь пакет в інший пакет і посилає новий, композитний пакет по мережі. Використовуються три класи протоколів тунелювання: протоколи передачі (Carrier protocol: FRRelay, ATM, MPLS); протоколи інкапсуляції (Encapsulating protocol: GRE, IPSec, L2F, PPTP, L2TP); пасажир – інкапсульований протокол (passenger protocol: IPX, AppleTalk, IPv4, IPv6).

Тунелі - створюються на різних протоколах інкапсуляції: універсальна інкапсуляція маршрутизації (Generic Route Encapsulation, GRE); протокол безпеки IP (IPSec); протокол переадресації 2 рівня 2 (Layer 2 Forwarding, L2F); протокол тунелювання точка-точка (Point-to-Point Tunneling Protocol, PPTP); протокол тунелювання 2 рівня (Layer 2 TP, L2TP).

Мережа VPN імітує канал точка-точка та інкапсулює дані, у заголовку яких міститься інформація про маршрутизацію. Даний формат дозволяє даним проходити через публічну мережу, щоб досягнути призначення. Сам по собі тунель не може забезпечити безпеку, а лише створює розширення локальної мережі в рамках WAN чи публічної мережі. Тунелі можуть передавати як зашифровані, так і незашифровані дані. Організації використовують site-to-site VPN мережі, щоб зв'язати розкидані підрозділи. Оскільки більшість організацій зараз мають доступ до Інтернет, є сенс скористатися перевагами site-to-site VPN. Загалом, site-to-site VPN є продовженням класичних WAN мереж, які підключають всі мережі одну з одною. Наприклад, вони можуть зв'язати мережі філії до мережі штаб-квартири компанії. В site-to-site VPN, хости відправляють та приймають TCP/IP-трафік через VPN шлюз, яким може бути маршрутизатор або Adaptive Security Appliance (ASA).

Мобільні користувачі та віддалені працівники інтенсивно використовують технологію VPN віддаленого доступу (remote access VPN). Більшість віддалених працівників тепер мають доступ до

Інтернет з дому і можуть встановити віддалений VPN з використанням широкосмугового з'єднання.

Сьогодні існують чотири види архітектури організації захисту інформації на базі застосування технології VPN: **локальна** мережа (Local Area Network - LAN). Забезпечує захист потоків даних всередині мережі компанії, інформаційну безпеку на рівні розмежування доступу, системних і персональних паролів, безпеки функціонування ОС, а також ведення журналу колізій і шифрування конфіденційної інформації; **внутрішньокорпоративна мережа VPN** (Intranet-VPN). Підтримує безпечні з'єднання між внутрішніми підрозділами розподіленої компанії; **мережі VPN з віддаленим доступом** (Internet-VPN). Забезпечує захищений дистанційний доступ віддалених підрозділів розподіленої компанії і мобільних співробітників і відділів через відкритий простір Internet; **міжкорпоративні мережі VPN** (Extranet-VPN). Гарантує ефективний захищений обмін інформацією з постачальниками, партнерами, філіями корпорації в інших країнах.

VPN-тунель має всі властивості захищеної виділеній лінії, що проходить через відкритий простір Інтернету. Засоби побудови захищеної VPN досить різноманітні. Вони можуть включати маршрутизатори з механізмом фільтрації пакетів (Filtering Router), багатофункціональні міжмережні екрани (Multifunction Firewall), проміжні пристрої доступу в мережу (Proxy Server), програмно-апаратні шифратори (Firmware Cryptograph) і т.д [6-7].

2.6 Забезпечення мережної безпеки

Інформаційна система перебуває в стані захищеності, якщо забезпечені її конфіденційність, доступність і цілісність. Безпека забезпечується технічними засобами - системами шифрування, автентифікації, авторизації, аудита, антивірусного захисту, мережевими екранами, а також юридичними, морально-етичними нормами та адміністративними мірами.

Автентифікація користувача - процедура доказу, що він той, за кого себе видає. Це багаторазові та одноразові паролі, володіння

якимось унікальним предметом (фізичним ключем, документом, сертифікатом), біохарактеристики (рисунок райдужної оболонки ока).

Авторизація - процедура контролю доступу легальних користувачів до ресурсів системи та надання кожному з них саме тих прав, які визначені йому адміністратором.

Антивірусний захист служить для профілактики та діагностики вірусного зараження, а також для відновлення працездатності уражених вірусами інформаційних систем.

Мережевий екран здійснює інформаційний захист однієї частини комп'ютерної мережі від інших шляхом аналізу трафіку.

Проксі- сервер - виконує функції посередника між клієнтськими та серверними частинами розподілених мережевих частин, причому клієнти належать внутрішній мережі, а сервери – зовнішній (потенційно небезпечній) мережі.

Технологія захищеного каналу – захист трафіку між двома підключеннями у відкритій транспортній мережі (Інтернет). Захищений канал виконує три основних функції: автентифікація абонентів при встановленні з'єднання; шифрування переданих повідомлень; підтвердження цілісності повідомлень. До популярних протоколів захищеного каналу відносять IPSec і SSL.

IPSec - архітектура або набір концепцій, які використовуються для захисту мереж IP (скорочена версія найменування в RFC (RFC +4301; архітектура безпеки Інтернет-протоколу - Security Architecture for the Internet Protocol), для якої вживається назва "IPSecurity" або скорочена версія - "IPSec "). Протоколи IPSec можна розділити на два класи: протоколи, які відповідають за захист потоку пакетів та протоколи обміну криптографічними ключами. На даний момент визначений тільки один протокол обміну криптографічними ключами – IKE (Internet Key Exchange) – та два протоколи, які забезпечують захист потоку інформації, що передається:

– Authentication Header (AH) - використовується коли конфіденційність не потрібна, або не вимагається. AH забезпечує перевірку достовірності і цілісності даних для IP пакетів, переданих між двома системами. Даний алгоритм перевіряє відсутність змін під час передачі повідомлення та підтверджує, що дані належать визначеним відправнику та отримувачу. AH не забезпечує конфіденційність даних шляхом шифрування пакетів. При використанні лише AH протоколу забезпечується слабкий захист.

Тому він використовується з протоколом ESP, щоб забезпечити шифрування даних і захист від підробок;

- Encapsulating Security Payload (ESP) - забезпечує цілісність та конфіденційність шляхом шифрування IP-пакетів. Шифрування IP-пакетів забезпечує приховування даних та відомостей про відправника та отримувача. Хоча шифрування та автентифікація є обов'язковими для ESP, як мінімум, одна з цих функцій має бути вибрана.

IPsec реалізований на основі існуючих алгоритмів шифрування, автентифікації та обміну ключами. Деякі з стандартних алгоритмів, що використовує IPsec: DES – шифрує та розшифровує пакети даних; 3DES – забезпечує кращу ефективність шифрування ніж 56-бітний DES; AES – забезпечує кращий рівень шифрування, в залежності від довжини ключа, і більшу пропускну здатність; MD5 – автентифікація пакетної передачі даних з використанням 128-бітного спільного секретного ключа; SHA-1 – автентифікує дані, використовуючи 160-бітний спільний секретний ключ; DH – дозволяє двом сторонам створити спільний секретний ключ, що використовується для шифрування та хеш-алгоритмів, наприклад, DES та MD5, при передачі даних по незахищеному каналі.

GRE (англ. *Generic Routing Encapsulation* - загальна інкапсуляція маршрутів) - протокол тунелювання мережевих пакетів, розроблений компанією Cisco Systems. Його основне призначення - інкапсуляція пакетів мережевого рівня моделі OSI в IP пакети. Сам по собі GRE не забезпечує ніякої безпеки переданих даних - це site-to-site VPN тунель у чистому вигляді. Використовується зазвичай такий тунель, коли є специфічні завдання, пов'язані з маршрутизацією і немає вимог до безпеки. Не варто забувати, що чистий GRE тунель - не навантажує обладнання, а навантаження при шифруванні великого обсягу даних досить істотне.

Протокол GRE інкапсулюється безпосередньо в IP, минаючи TCP або UDP, в IP пакеті є спеціальне поле «Protocol type», в якому міститься число, що позначає протокол, інкапсульований в даний IP пакет, для GRE код protocol type дорівнює 47. У зв'язку з цим, якщо в мережі є GRE тунелі, то варто уважно ставитися до написання розширених списків контролю доступу (ACL), так як `permit tcp any any` і `permit udp any any` приведуть до заборони на GRE через те, що він інкапсулюється безпосередньо в пакет, тому треба писати або `permit ip any any` або `permit gre any any` [8].

2.7 Забезпечення мережної безпеки в бездротових ЛОМ

Бездротовий сегмент мережі завжди має додаткову небезпеку, вимагаючи більшої уваги при установці і налаштування. При налаштування захисту бездротової мережі зазвичай розглядаються декілька методів: зміна пароля адміністратора; відключення трансляції SSID мережі; фільтрація за MAC-адресами; шифрування даних; зниження потужності передавача. Паролі адміністратора та ідентифікатори SSID у більшості випадків вільно доступні в Інтернеті для більшості моделей бездротового устаткування. Потрібно обов'язково змінити стандартні пароль адміністратора та ідентифікатор SSID, що задає ім'я мережі. А це означає, що злоумисникові досить з'ясувати модель вашої бездротової точки доступу, щоб одержати до неї доступ, попередньо довідавшись стандартні SSID і пароль адміністратора.

Також треба змінити IP-адрес. Багато точок доступу за замовчуванням транслюють усім свій SSID. Тому до вашої може підключитися будь-який небажаний гість, навіть ненавмисно, - людина просто запустить пошук мережі і знайде вашу точку доступу. Якщо настроюється невелика бездротова мережа вдома або в офісі, то виникає необхідність підключати додаткові комп'ютери. В цьому випадку можна використовувати фільтрацію за MAC-адресами. Цей режим дозволить підключатися до мережі тільки заданим пристроєм з їх унікальними MAC-адресами. Фільтрація за MAC-адресами не може забезпечити стовідсотковий захист. Вона розглядається як один з заходів по забезпеченню безпечної роботи.

Щоб захистити дані під час передачі від одного мережевого пристрою до другого, використовується шифрування даних. При шифруванні даних необхідно на кожному з цих пристроїв налагодити **протокол шифрування і ключі**.

Основні типи шифрування. **WEP**-шифрування. Перший та найбільш простий спосіб шифрування - використання протоколу **WEP** (Wired Equivalence Privacy). **WPA**-шифрування з двома режимами: **WPA-EAP** (Extensible Authentication Protocol); **WPA-PSK** (Pre-Shared Key). Режим **WPA-EAP** використовується в корпоративних мережах, оскільки вимагає наявності сервера автентифікації (RADIUS-сервера). З цієї причини він не може використовуватися в домашніх умовах.

Для персонального використання призначений режим **WPA-PSK**. Він передбачає застосування заздалегідь заданих ключів шифрування (пароль доступу), однакових для всіх мережевих пристроїв, а первинна автентифікація користувачів здійснюється з використанням даного ключа. В якості алгоритмів шифрування при використанні стандарту **WPA** можна вибрати **TKIP** або **AES**. Алгоритм **WPA2** є наступною версією протоколу WPA. Якщо всі пристрої бездротової мережі підтримують даний режим, то можна їм скористатися. Налаштування в даному випадку здійснюються такі самі, як і у разі WPA-шифрування [6-8].

3 ЗАГАЛЬНІ ВИМОГИ ДО ОФОРМЛЕННЯ КУРСОВОГО ПРОЕКТУ

3.1 Вимоги до оформлення пояснювальної записки

Пояснювальна записка курсового проекту оформлюється відповідно до діючих стандартів на оформлення програмної, текстової та графічної документації: ДСТУ 3008-95 «Документація. Звіти в сфері науки та техніки».

Кожна сторінка тексту пояснювальної записки оформлюється в основній рамці (відступ зліва на 20 мм, з інших сторін на 5 мм) та з надписом (рис. 3.1), в якому визначається децимальний номер курсового проекту та номер листа (сторінки) пояснювальної записки, написаний арабськими цифрами.

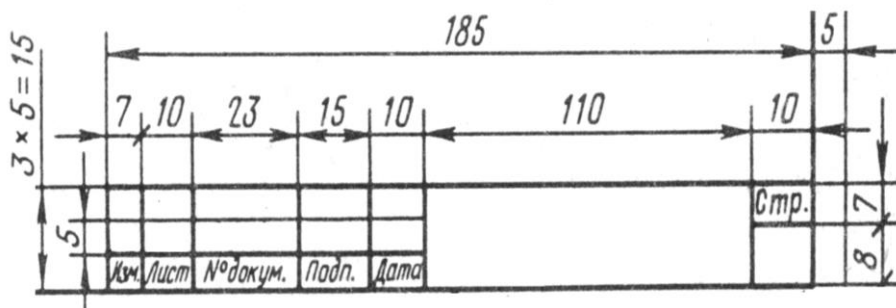


Рисунок 3.1 – Форма надпису в пояснювальній записці

Децимальний номер курсового проекту має структуру:

XX.XXXXXXXX.XXXXX XX, де:

- 1 – шифр держави (для України – 13);
- 2 – шифр вищого навчального закладу (для ЗНТУ – 02070849);
- 3 – номер групи + номер теми проекту (номер варіанту);
- 4 – літерно-цифровий шифр документа.

Наприклад, для пояснювальної записки курсового проекту студента групи КНТ620 з номером варіанту – 12, децимальний номер – 13.02070849.62012 ПЗ.

Перша сторінка пояснювальної записки (титульний лист) не нумерується.

Зразок оформлення титульного листа наведено в додатку Б.

Друга та третя сторінки пояснювальної записки – технічне завдання, виконується з обох сторін аркуша. Зразок оформлення технічного завдання наведено в додатку В.

3.2 Вимоги до оформлення графічних документів

Графічні документи курсового проекту пропонується виконувати на папері для креслення з нанесенням зовнішньої рамки зліва на 20 мм, з інших сторін на 5 мм. В правому нижньому куті виконують основний надпис (рис. 3.2). Графічні матеріали виконуються на папері формату А4 або А3 (210х290) та розміщуються в додатках. Кількість листів та вигляд графічних документів узгоджується студентом з керівником курсового проекту з урахуванням особливостей теми проекту. Рекомендована кількість графічних документів – 3-5 листів.

Графічні документи складаються з плакатів, що мають ілюстраційний характер, та креслень, які виконуються згідно стандартів. Графічна частина курсового проекту обов'язково повинна містити в собі два або одне креслення.

3.3 Вимоги до виконання схем

В графічній частині курсового проекту пропонується виконувати креслення або плакати на 3-5 листах формату А4 або А3. В склад графічної частини включають: модель мережі; структурні схеми мережі, яка проектується; специфікації компонентів мережі; алгоритми роботи мережі; схеми зв'язків; монтажні схеми розташування апаратних засобів.

З урахуванням особливостей конкретної теми курсового проекту склад графічних документів може бути змінено.

Схеми в залежності від елементів й зв'язків між ними розділяються на такі види: структурна схема Е1 (додаток А) визначає основні функціональні частини виробів, їх значення та взаємозв'язки; функціональна схема Е2 (служить для роз'яснення процесів, які протікають в окремих функціональних колах виробу або у виробі в цілому); принципова (повна) схема Е3 (визначає повний склад елементів та зв'язків між ними та дає детальне уявлення про принципи роботи виробу); схема з'єднань (монтажна) Е4 (показує з'єднання складових частин виробів та визначає проводи, джгути, кабелі або трубопроводи, за допомогою яких виконуються ці з'єднання, а також місця їх з'єднань та виведення); схема підключення Е5 (показує зовнішні підключення виробів).

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101 / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 912 с. – ISBN 978-5-8459-1906-9.
2. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 736 с. – ISBN 978-5-8459-1907-6.
3. Шапорін Р.О. Моделі та методи проектування комунікаційних систем комп'ютерних мереж масштабу підприємства [Текст]: автореф. дис... канд. техн. наук: 05.13.12 / Р.О.Шапорін ; Одеський національний політехнічний ун-т. - О., 2007. - 22 с.
4. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.
5. Бакланов И.Г. NGN: принципы построения и организации. – М. : Эко-Трендз, 2008. – 400 с.
6. Гольдштейн А.Б. Технология и протоколы MPLS / А.Б.Гольдштейн, Б.С.Гольдштейн. – СПб.: БХВ, 2005. – 304 с.
7. Глотиков К. IMS (IP multimedia Subsystem). М.: Эко-трендз. 2009. – 100 с.
8. Гольдштейн Б.С. Сети связи. Учебник для вузов / Б.С. Гольдштейн, Н.А.Соколов, Г.Г.Яновский. – СПб. : БХВ, 2009. – 400 с.
9. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide / D. Hucaby. – 2nd Edition. – USA: Cisco Press, 2015. – 578 p.
10. Платунова С.М. Методы проектирования фрагментов компьютерной сети – СПб: НИУ ИТМО, 2012. – 51 с.
11. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.

Додаток А

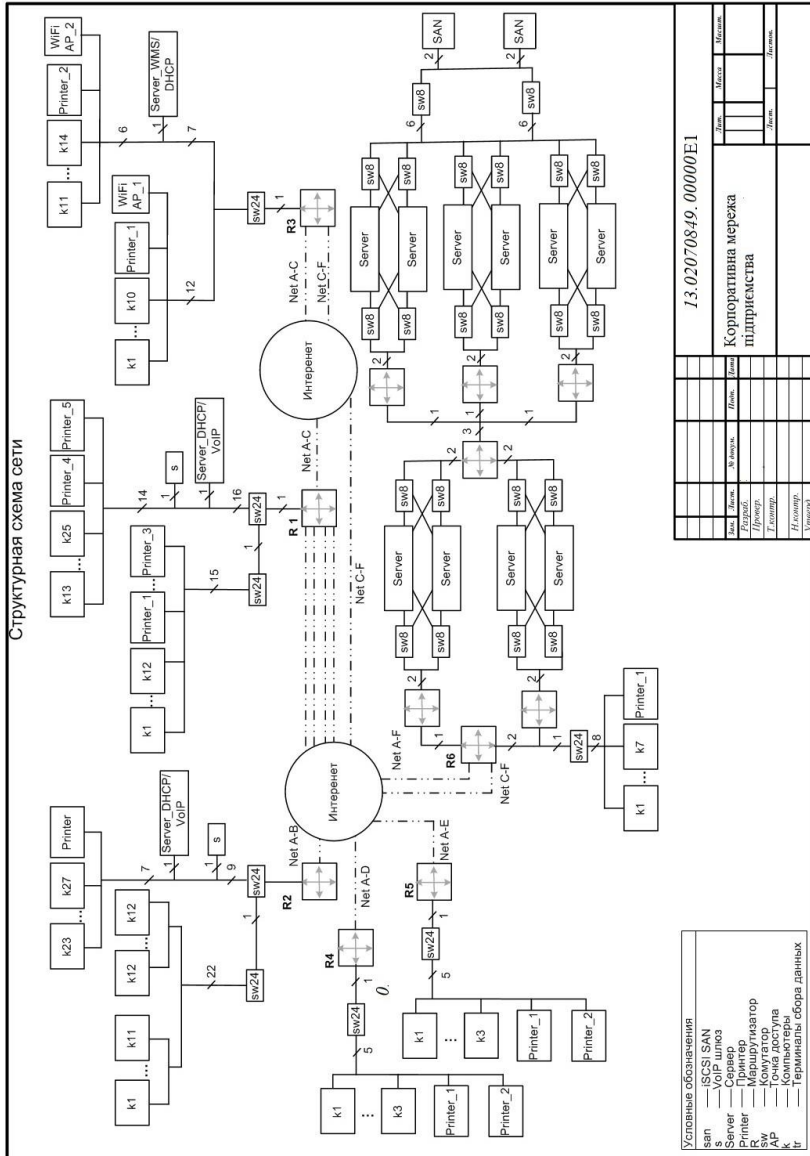


Рисунок А.1 – Структурна схема мережі