

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проекту з дисципліни

"Проектування комп'ютерних мереж"

для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні
програми "Спеціалізовані комп'ютерні системи" та "Комп'ютерні
системи та мережі", усіх форм навчання

Методичні вказівки до виконання курсового проекту з дисципліни "Проектування комп'ютерних мереж" для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні програми "Спеціалізовані комп'ютерні системи" та "Комп'ютерні системи та мережі", усіх форм навчання // Укл. Г.Г. Киричек. – Запоріжжя: ЗНТУ, 2017. – 54 с.

Укладач:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

Р.К. Кудерметов, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 2 від 13.09.2017

Затверджено
на засіданні НМК КНТ
Протокол № 2 від 28.09.2017

ЗМІСТ

1 Загальні відомості	4
1.1 Календарний план та отримання завдання	5
1.2 Загальні питання проведення досліджень	6
1.3 Вимоги до змісту розділів, оформлення та обсягу пояснювальної записки	9
1.4 Теми проектів	11
1.5 Порядок захисту курсового проекту	12
2 Структура курсового проекту	13
2.1 Аналіз технічного завдання	14
2.2 Вибір технологій LAN\WAN сегментів та обладнання об'єднаної мережі підприємства	18
2.3 Планування структури кожної ЛОМ об'єднаної мережі	24
2.4 Моделювання мережі. Системи моделювання	25
2.5 Віддалений доступ до мережі. З'єднання ЛОМ підприємства.	26
2.6 Технологія VPN	28
2.7 Забезпечення мережної безпеки	30
2.8 Забезпечення мережної безпеки в бездротових ЛОМ	33
2.9 Налаштування доступу в Інтернет через cisco vpn client	35
3 Загальні вимоги до оформлення курсового проекту	40
3.1 Вимоги до оформлення пояснювальної записки	40
3.2 Вимоги до оформлення графічних документів	41
3.3 Схеми алгоритмів, програм, даних та систем	42
3.4 Вимоги до виконання електричних схем	44
Рекомендована література	46
Додаток А	47
Додаток Б	48
Додаток В	49
Додаток Г	51
Додаток Е	53

1 ЗАГАЛЬНІ ВІДОМОСТІ

Мета проектування – проведення досліджень та одержання практичних навичок аналізу, порівняння, вибору методів розрахунку, моделювання, проектування і розробки об'єднаних, корпоративних та комп'ютерних мереж рівня підприємства, проведення аналізу їх функціонування у сучасному середовищі. Вміння аналізувати, порівнювати, моделювати та впроваджувати мережні технології при проектуванні як локальних так і глобальних сегментів мереж об'єднаної мережі підприємства. Отримання практичних знань з організації доступу до мережі Internet та між локальними мережами підприємства. А також: узагальнення, закріплення та поглиблення теоретичних та практичних знань зі спеціальності; використання цих знань для проведення дослідження, обґрунтованого прийняття проектних рішень та вирішення конкретних задач; практичне закріплення навичок моделювання та розробки комп'ютерних мереж рівня масштабу підприємства.

Завдання до курсового проекту передбачають розробку об'єднаної (корпоративної) мережі підприємства згідно з варіантом (загальна кількість кінцевих вузлів не менше 1000, віддалених локальних мереж не менше 3), побудову моделі та планування і розробку кожної локальної обчислювальної мережі (ЛОМ) з яких складається об'єднана мережа, монтаж мережі, згідно структурної схеми мережі, налаштування мережного обладнання, з'єднання через маршрутизатори окремих ЛОМ підприємства, налаштування віддаленого доступу між ЛОМ (використання тунелів) та до мережі Internet з забезпеченням мережної безпеки.

На всіх етапах проектування необхідно проводити оцінку альтернативних варіантів побудови об'єднаної мережі та її окремих частин.

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 об'єднаної мережі	21.09 – 30.09
3	Аналіз, порівняння та вибір технологій організації LAN та WAN мереж	01.10 – 8.10
4	Розробка структурної схеми об'єднаної мережі підприємства	09.10 – 15.10
5	Аналіз, порівняння та вибір мережного, серверного і клієнтського обладнання	16.10 – 23.10
6	Монтаж мережі	24.10 – 31.10
7	Налаштування обладнання LAN та WAN мереж підприємства	01.11 – 07.11
8	Організація віддаленого доступу до мережі, отримання пулу відкритих адрес	08.11 – 14.11
9	Вибір та налаштування протоколів маршрутизації об'єднаної мережі підприємства	15.11 – 20.11
10	Налаштування маршрутизаторів, згідно політики безпеки об'єднаної 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 15.12

У відповідності до теми **керівник видає** технічне завдання на курсовий проект з вказівкою термінів виконання окремих етапів та всього проекту в цілому (**до 20.09 можливе узгодження та затвердження за вибором студента**).

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

Одним із перспективних напрямків розвитку сучасних підприємств є створення об'єднаних, корпоративних та комп'ютерних мереж масштабу підприємства різного функціонального призначення. Важливим елементом створення таких мереж є проектування систем, які містять сотні одиниць різного комунікаційного обладнання. 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, моделей і засобів проектування комп'ютерних мереж масштабу підприємства, що забезпечують зменшення часу та ефективність передачі даних і дозволяють отримати оптимальні за критерієм "продуктивність/ вартість" проектні рішення.

Відповідно до поставленої мети в роботі можливе **вирішення наступних задач**:

- проведення системного аналізу архітектурних та інформаційних особливостей мереж;
- виконання аналізу джерел і ступеня впливу службового і ширококомовного трафіку на характеристики функціонування комп'ютерних мереж;
- визначення правил вибору структури мережних об'єктів;
- розроблення алгоритму об'єктно-орієнтованої декомпозиції комп'ютерної мережі;
- розроблення інформаційної (математичної) моделі мережі із різними каналами зв'язку;
- моделювання комп'ютерних мереж масштабу підприємства;
- проектування комп'ютерних мереж масштабу підприємства;
- налаштування комп'ютерних мереж масштабу підприємства;
- адміністрування та захист комп'ютерних мереж масштабу підприємства.

Об'єктом дослідження є комп'ютерні мережі масштабу підприємства.

Предметом дослідження є моделі і методи проектування комп'ютерних мереж масштабу підприємства.

Методи дослідження. Для досягнення поставленої мети, при виконанні етапів проектування, рекомендовано використовувати наступні методи дослідження:

- системний аналіз, для дослідження механізмів функціонування програмно-апаратних засобів комп'ютерних мереж масштабу підприємства;

- об'єктно-орієнтовані методи проектування (побудова загальної моделі комп'ютерної мережі масштабу підприємства);
- методи теорії обчислювальних систем і теорії масового обслуговування для побудови та розрахунку математичних моделей, що відображають імовірісно-часові характеристики функціонування комп'ютерних мереж масштабу підприємства;
- методи натурального моделювання для верифікації розроблених моделей комп'ютерних мереж масштабу підприємства.

Наукову новизну проектів становлять:

- вибір структури мереж різних рівнів ієрархії, які дозволяють синтезувати неблокуючі мережеві структури комп'ютерних мереж масштабу підприємства, мінімальні за вартістю;
- декомпозиція мережі (мережа у вигляді інформаційно ізольованих мережних об'єктів);
- проектування мережевих 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 імовірісно-часових характеристик функціонування комп'ютерних 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 мережі, яка підлягає проектуванню, у відповідності до технічного завдання. Не рекомендується робити великі реферативні огляди. При необхідності можна робити посилання на відповідну літературу. Основний зміст записки – це аналіз, порівняння, вибір та обґрунтування прийнятих рішень та проект об'єднаної мережі, згідно затвердженої назви. 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 проєктант вказує мету, об'єкт та предмет дослідження; технології, вид обладнання, протоколи та стандарти, які використані у розробленому проєкті. Наводить ключові слова та об'єм пояснювальної записки. Реферат рекомендовано оформити на заключному етапі (1 сторінка). Приклад реферату у додатку Д.

У вступі до проєкту магістр повинен обґрунтувати актуальність проектування об'єднаної (корпоративної) 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. Його не слід перевантажувати загальними фразами. 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 об'єднаної мережі. Студент повинен чітко визначити коло задач, які необхідно вирішити в курсовому проекті, 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 об'єднаної мережі підприємства, виконується обґрунтування вибору та опис LAN\WAN-технологій окремих сегментів об'єднаної мережі. Кількість підключених робочих станцій не повинна бути меншою за 1000 одиниць.

Третій розділ (10-12 сторінок) повинен містити опис апаратної та кабельної частини проекту 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, розрахунок окремих елементів, вузлів та підсистем. Виконується налаштування загальних об'єктів.

У четвертому розділі (4-10 сторінок) розглядається підключення розробленої мережі підприємства 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 головного офісу організації (підприємства) в Інтернеті.

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

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 – 45 - 50 сторінок (не рекомендовано обсяг більший за 50 стор.), причому технічна її частина, має містити не менш ніж 30 сторінок тексту з рисунками.

1.4 Теми проектів

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

1. Корпоративна мережа металургійного підприємства.
2. Мережа ВАТ «Мотор-Січ» з віддаленими філіями.
3. Комп'ютерна мережа супермаркетів «Сільпо» м. Київ.
4. Об'єднана мережа «Дніпровська електроенергетична система» України.
5. Мережа державного підприємства «Екологія України».
6. Комп'ютерна мережа «Радіоком» азовського побережжя.
7. Кампусна комп'ютерна мережа мешканців мікрорайонів м.Запоріжжя.
8. Комп'ютерна мережа головних офісів банку.
9. Оптиволоконна мережа ВАТ «Дніпроспецсталь» з трьома філіалами.
10. Корпоративна мережа агропромислового комплексу «Україна» (об'єкти у різних географічних частинах України).
11. Комп'ютерна мережа концерну «Теплові мережі України».
12. Об'єднана мережа підприємства «Центромеблі».
13. Комп'ютерна мережа Запорізької філії ВАТ «Укртелеком».
14. Розподілена мережа підприємства на базі ADSL та VPN-технологій.
15. Комп'ютерна мережа комунального підприємства «Водоканал» м. Запоріжжя.

16. Комп'ютерна мережа ЗАТ «Запорізький залізорудний комбінат».
17. Розподілена комп'ютерна мережа підтримки проведення соціологічних досліджень.
18. Комп'ютерна мережа пенсійного фонду України.
19. Об'єднуюча магістраль енергетичного комплексу ВАТ «УкрЕнерго».
20. Комп'ютерна мережа підприємства з використанням технологій Wi-Fi у ЛОМ філіалів.
21. Комп'ютерна мережа філіалів торгівельної фірми з підвищеною надійністю Internet з'єднання.
22. Комп'ютерна мережа податкової служби області.
23. Корпоративна мережа регіональних лікарень України.
24. Комп'ютерна мережа банку з розвиненою системою банкоматів міста.
25. Об'єднана мережа Укрзалізниці.

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 комп'ютерної 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 об'єднаної 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 мережі рівня підприємства студенту рекомендовано розглянути наведені нижче питання, тримаючись загального плану проекту за варіантом.

Основні етапи проектування можуть включати.

Вступ.

1. 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.

2. 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.

3. Монтаж та налаштування мережі:

- визначення основних LAN і WAN сегментів, проектування структурної схеми мережі;
- побудова монтажної схеми (розміщення мережових і апаратних пристроїв (в будівлях, на поверххах, 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).

4. 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 комп'ютерної мережі масштабу підприємства, 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 комп'ютерних мереж масштабу підприємства. Показати, що типова структура комп'ютерних мереж масштабу підприємства містить три системи – клієнтську, серверну і комунікаційну (або рівні доступу, розподілення та ядра). Визначити, що основою комунікаційної системи є комутатори і кожен рівень ієрархії можна побудувати на основі однієї з типових структур, які використовуються на даному рівні [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 об'єднана (корпоративна) мережа масштабу підприємства. На рисунку 2.1 наведена приблизна ієрархічна структура мережі.

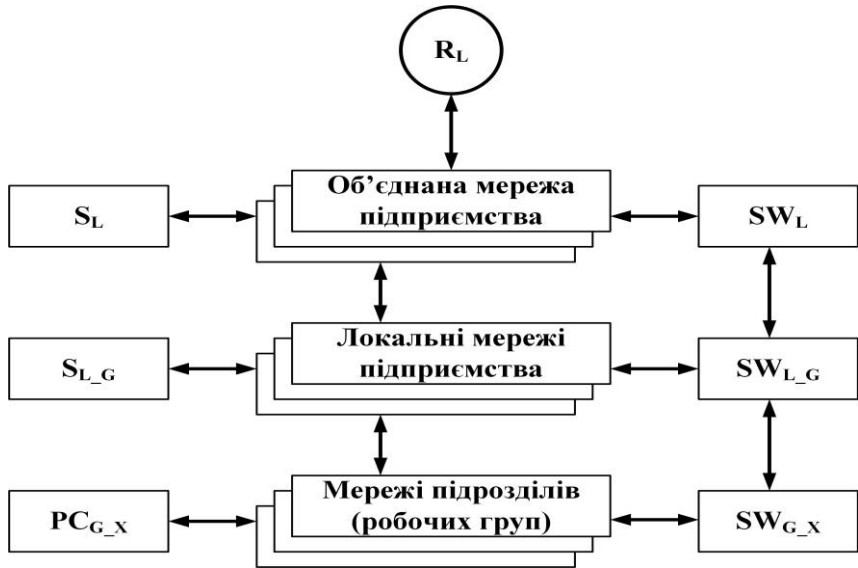


Рисунок 2.1 - Ієрархічна структура комп'ютерної мережі масштабу підприємства.

Де маємо наступні об'єкти: PC_{G_X} , SW_{G_X} – комп'ютери та локальні комутатори підрозділів (робочих груп), SL_G , SW_{L_G} – сервера та комутатори локальних мереж підприємства; SL , SW_L , R_L – сервера, комутатори та маршрутизатори об'єднаної мережі підприємства. Де G це номер групи (підрозділу), X – номер елементу 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. Комп'ютерна мережа при цьому підходить в кожній стадії проходить цикл, який може повторюватися: планування - реалізація - перевірка - оцінка.

При проектуванні, замість оригінального об'єкта, оперують моделлю, яка відображає властивості, що цікавлять дослідника.

Математична функціональна модель, у загальному випадку, являє собою алгоритм обчислення вектору вихідних параметрів при заданих векторах параметрів елементів і зовнішніх параметрів. Вам, як проектувальнику, важливо продумати всі нюанси, пов'язані з побудовою мережі.

Корпоративна мережа – складна система, яка складається з тисяч різних компонентів, основними характеристиками яких є: пропускна здатність P , продуктивність G та вартість C [3].

Нижче наведено приклад визначення формальних правил розрахунку характеристик мережних структур на прикладі комутаторів.

Пропускна здатність комутатора P_S може бути представлена у вигляді $P_S = \min\{\sum_{i=1}^N P_{ВПi}, P_{ВМ}, \sum_{j=1}^M P_{СПj}\}$, де N – кількість вхідних портів; M – кількість серверних портів; $P_{ВПi}$ – пропускна здатність i -го вхідного порту; $P_{ВМ}$ – пропускна здатність внутрішньої магістралі; $P_{СПj}$ – пропускна здатність j -го серверного порту.

Продуктивність комутатора $G_S = 1/T_{ТР}$, де $T_{ТР}$ – середній час транзакції через комутатор.

Вартість комутатора $C_S = \sum_{i=1}^K C_{БП} + \sum_{j=1}^L C_{ФП}$, де K – кількість базових портів; L – кількість факультативних портів; $C_{БП}$ – вартість базового порту; $C_{ФП}$ – вартість факультативного порту.

Аналіз відомих методів проектування мережі масштабу підприємства показує, що вони містять два етапи. На першому етапі вибираються базові структури для кожного з рівнів ієрархії. На другому етапі виконується їхня структурна оптимізація. Найбільш трудомістким є другий етап, що виконується ітераційно і пов'язаний з моделюванням частини або всієї мережі масштабу підприємства. Для зменшення числа ітерацій на першому етапі проводиться вибір надлишкових мережних структур.

При проведенні аналізу інформаційного трафіку (обчислення загального трафіку з визначенням необхідної швидкості каналів зв'язку) можна скористатись рішенням подібних завдань.

Вирішимо задачу на встановлення максимального розміру бази даних, яку можна передати за встановлений час, при використанні різних протоколів транспортного рівня.

Приклад. Нехай через зовнішній сегмент комп'ютерної мережі необхідно копіювати базу даних. Середня швидкість передачі 1 біта = 0,5 мкс, MTU=274 В. Який максимальний розмір (точно) БД можливо передати за 2 хвилини? Яка при цьому буде технічна (R_t) та інформаційна швидкості (R_i)? Маємо заголовки каналного рівня = 26В, заголовок IP, UDP, TCP дорівнюють відповідно 24, 8, 24 В. Для спрощення вважаємо, що 1GB=1000MB, 1MB=1000KB.

Вирішення. Переводимо час в секунди $T = 120\text{с}$.

Швидкість R_t в біт/с дорівнює $1\text{ біт/с} / 0,5\text{ мкс} = 2\text{Мб/с}$.

Об'єм даних $V_t = T * R_t = 120\text{с} * 2\text{Мб/с} = 240\text{Мбіт} = 30\text{ Мбайт}$.

$MSS_{UDP} = 274 - 24 - 8 = 242\text{ байти}$. $MSS_{TCP} = 274 - 24 - 24 = 226\text{ байт}$.

Знаходимо обсяг переданих даних з урахуванням тільки інформаційної складової:

- за UDP – 30 МБ - 300Б (MTU+26 В – загол.канал.рівня);
X МБ - 242 Б (MSS_{UDP}); $V_{UDP} = 24,2\text{ МБ}$;
- за TCP – 30 МБ - 300Б (MTU+26В – загол.канал.рівня);
X МБ - 226 Б (MSS_{TCP}); $V_{TCP} = 22,6\text{ МБ}$;
- максимальний розмір БД - $V = 24,2\text{ МБ}$;
- затримка на 1 кадр $300 * 8 / 2\text{Мб/с} = 0,0012\text{ с}$;
- $R_i = MSS_{UDP} / 0,0012 = 242 * 8 / 0,0012 = 1,61\text{ Мб/с}$;
- $R_i = MSS_{TCP} / 0,0012 = 226 * 8 / 0,0012 = 1,51\text{ Мб/с}$;
- кількість кадрів - $T / 0,0012 = 120 / 0,0012 = 100000\text{ кадрів}$.

Перевірка. $UDP = 24,2\text{ МБ} / 242\text{Б} = 100000\text{ кадрів}$. $TCP = 22,6\text{ МБ} / 226\text{Б} = 100000\text{ к} [4]$.

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.

Закон функціонування мережі можна представити в наступному вигляді: $H(t) = f_c(S, F, Y, X, t)$, де f_c - функція, функціонал, логічні умови, алгоритм, методика, таблиця або опис, який визначає правило (закон) перетворення вхідних величин (параметрів) у вихідні величини (характеристики). $H(t)$ - вектор характеристик, що залежить від поточного моменту часу t ($t \geq 0$): $H = \{V, T, N, C, Z\}$.

Параметри - первинні дані мережі: S - структурні, F - функціональні, Y - навантажувальні, X - зовнішнього середовища.

Характеристики - вторинні дані мережі: V - потужності, T - тимчасові, N - надійність, C - економічні, Z - інші [5].

2.2 Вибір технологій LAN\WAN сегментів та обладнання об'єднаної мережі підприємства

Створити проект мережі означає вибрати структуру мережі, визначити значення всіх її параметрів і представити результати у встановленій формі. Результати (проектна документація) потрібно представляти у вигляді схем, пояснювальних записок, програм. Розробка (вибір) структури мережі є проектна процедура структурного синтезу, а розрахунок значень параметрів елементів процедура параметричного синтезу. Завдання структурного синтезу полягає у визначенні мети, безлічі можливих рішень і обмежуючих умов, полягає в синтезі структури, визначенні типів серверів (програмно-апаратних засобів), розподілі функцій по серверам так, щоб досягався екстремум цільової функції при виконанні завдань.

Наступна після синтезу група проектних процедур - процедура аналізу. 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 корпоративній (об'єднаній) 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.

Серверне приміщення – найважливіше приміщення корпоративної мережі. Хости та сервери можна розташовувати в мережі централізовано або в різних точках мережі. Групу серверів звичайно розташовують в машинній залі (апаратній) з контрольованим середовищем. Вона має спеціальне обладнання для фільтрації коливань силової напруги та підтримки температури в заданому діапазоні. Також там встановлюють системи архівації.

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.

Завдання ІТ-співробітників і сфери їхньої відповідальності повинні чітко розподіляється. Ієрархія підрозділів зображується у вигляді організаційної або пірамідальної діаграми.

Магістраль (ядро) – один із самих головних і найдорожчих компонентів мережі. Через магістраль проходить більша частина трафіку мережі, тому вона впливає на роботу всієї мережі в цілому. Рішення про вибір технологій магістралі є одним з найважливіших при плануванні мережі. Тому виникає необхідність у підвищенні пропускної здатності каналів між клієнтами мережі, серверами та об'єктами віддалених підрозділів.

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.

До глобальних належать показники оперативності, надійності, вартості і т.п. Продуктивність комп'ютерної мережі – міра потужності

мережі. Вона визначає кількість роботи, яку виконує мережа за одиницю часу та включає показники ефективності комп'ютерної мережі, які визначають якість функціонування як мережі в цілому, так і окремих її підсистем і елементів – технічних і програмних засобів: швидкість передачі даних по каналах зв'язку, яка вимірюється обсягом даних, які передаються за одиницю часу, швидкодії ПК, точніше, процесора (вимірюється числом команд, виконуваних в одиницю часу) і т.п. 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. Найбільш важливим показником продуктивності ОС, як сукупності технічних і програмних засобів є системна продуктивність, яка вимірюється числом завдань, що виконуються системою за одиницю часу. Характеристики оперативності описують затримки, що виникають при передачі і обробці даних в мережі. Для оцінки оперативності мережі використовуються такі показники: час доставки пакетів (повідомлень), час відгуку (відповіді).

Час доставки (час затримки) пакетів характеризує ефективність передачі даних в мережі і являє собою інтервал часу, який вимірюється від моменту надходження пакету (кадру, повідомлення) в мережу до моменту отримання його адресатом. У комп'ютерних мережах зазвичай час доставки задається середнім його значенням. При передачі мультимедійних даних крім середнього часу доставки

пакетів важливою характеристикою є джиттер затримки, який є середньоквадратичним відхиленням часу затримки різних пакетів.

Час відгуку (відповіді) - інтервал часу від моменту надходження запиту (повідомлення, транзакції) в мережу до моменту завершення його обслуговування, пов'язаного з виконанням деякої прикладної або обслуговуючої програми, зі зверненням до бази даних і т.п. Час відповіді є час перебування запиту в мережі і характеризує ефективність як телекомунікаційних, так і обчислювальних засобів комп'ютерної мережі [5].

У якості характеристик надійності використовуються наступні показники: ймовірність безвідмовної роботи мережі - ймовірність того, що протягом часу t не станеться відмови; інтенсивність відмов - середнє число відмов за одиницю часу; час напрацювання на відмову - проміжок часу між двома суміжними відмовами; час відновлення - інтервал часу від моменту настання відмови до моменту відновлення; коефіцієнт готовності – проміжок часу, протягом якого мережа працездатна.

У якості вартісних (економічних) характеристик комп'ютерної мережі можуть використовуватися такі показники: повна вартість володіння (Total cost of ownership, TCO) – витрати, які розраховуються на всіх етапах життєвого циклу мережі і включають вартість технічних, інформаційних і програмних засобів (прямі витрати) і витрати на експлуатацію мережі (непрямі витрати); вартість (ціна) передачі даних і обробки даних в мережі, яка визначається обсягом і вартістю ресурсів мережі відповідно при передачі і обробці даних.

У якості локальних характеристик комп'ютерних мереж можуть використовуватися різні показники ефективності. Локальні характеристики описують ефективність функціонування: вузлів і каналів зв'язку; окремих сегментів мережі; вузлів обробки даних: обчислювальної системи і її підсистем. Локальні характеристики можуть бути розбиті на дві групи: тимчасові та безрозмірні.

До тимчасових характеристик відносяться: час доставки (затримки) пакетів при передачі між сусідніми вузлами мережі; час очікування передачі даних на вузлах мережі; час перебування даних на різних вузлах, пристроях або підсистемах.

До безрозмірних відносяться [5]: число пакетів, що знаходяться в буферній пам'яті вузлів (маршрутизаторів, комутаторів); коефіцієнти завантажень вузлів, каналів зв'язку і пристроїв.

За час, з появи перших локальних мереж, розроблено декілька сотень різних мережевих технологій, проте помітне поширення отримали лише мережі, які пов'язані з їх підтримкою відомими фірмами та з високим рівнем стандартизації принципів їх організації. Мережа **Ethernet** зараз найбільш популярна в світі, і немає сумніву, що такою вона і залишиться в найближчі роки. Структурні елементи технології використовують як в LAN так і в WAN сегментах корпоративних мереж.

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. При встановленні з'єднання комутуючого віртуального каналу (Switching Virtual Chennel, SVC) згода про якість обслуговування встановлюється автоматично. Потрібні параметри передаються в пакеті запиту на встановлення з'єднання. Швидкість передачі даних вимірюється на контрольному інтервалі часу T , на якому перевіряються умови згоди. Тобто користувач не повинен в цьому інтервалі передавати в мережу дані з середньою швидкістю більшою за CIR. Якщо ж користувач порушує умови згоди, то мережа не гарантує доставки кадра і помічає цей кадр ознакою готовності до видалення – $DE=1$ [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". Точка-точка - односпрямоване або двунправленне (для кожного напрямку своє QoS). Точка - три крапки завжди односпрямоване - від 1 користувача до багатьох. За часом утримання з'єднання ATM забезпечує - Типи з'єднань: постійне віртуальне з'єднання (Permanent Virtual Connection - PVC); комутуюче віртуальне з'єднання (Switch Virtual Connection - SVC); інтелектуальні

постійні віртуальні канали (smart permanent virtual circuit - SPVC) - гібрид PVC і SVC. Подібно PVC - встановлюється вручну на етапі конфігурації мережі [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 канального 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 канального рівня в основному зводиться до вибору типу фізичного середовища: витої 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 канального 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, з використанням апаратних та кросових, 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 CNA 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.

2.5 Віддалений доступ до мережі. З'єднання ЛОМ підприємства.

Організація віддаленого доступу - одна з проблем комп'ютерних мереж, яка отримала назву «проблеми останньої милі» - під останньою милю мається на увазі відстань від точки присутності (POP - Point of presence) оператора зв'язку до приміщень клієнтів.

Вибір постачальника послуг Інтернету (ISP) - важливий аспект планування стратегії доступу в Інтернет для великої та середньої мережі. Основна функція ISP - надання доступу в Інтернет. ISP підтримує власну мережу, з'єднану з Інтернетом, до якої абоненти підключаються за допомогою самих різних ГОМ- технологій. Різні ISP займають різні рівні володіння мережами. Одні підключені безпосередньо до магістралей Інтернету, а інші є лише посередниками. Одні ISP орієнтовані на домашніх користувачів, а інші - на корпоративних.

Клієнти різних типів відрізняються обладнанням і вимогами до параметрів доступу. Приміщення клієнтів можуть з'єднуватись з найближчою точкою доступу оператора зв'язку різними способами: за допомогою аналогової або цифрової телефонної мережі; провідного зв'язку; телевізійного кабелю; бездротового зв'язку.

Оператор зв'язку може мати різну спеціалізацію: постачальник телефонних послуг; постачальник послуг Інтернету; оператор кабельного телебачення; універсальний оператор, який надає весь спектр послуг і володіє власними мережами всіх типів.

Технологія асиметричного цифрового абонентського закінчення (Assymetric Digital Subscriber Line, **ADSL**) розроблена для забезпечення швидкісного доступу в Інтернет масових індивідуальних користувачів, квартири яких оснащені звичайними телефонними закінченнями. Для доступу через ADSL потрібні телефонні абонентські закінчення «модеми». Принциповою відмінністю доступу через ADSL від комутованого доступу є те, що ADSL-модеми працюють лише в межах абонентського закінчення. ADSL-модеми отримують в своє розпорядження смугу близько 1 МГц - ця величина залежить від довжини кабелю, прокладеного між приміщенням користувача і POP, і перетину проводів цього кабелю. Схема доступу через ADSL близька до загальної схеми використання універсального

абонентського закінчення за виключення того, що при доступі через ADSL факт наявності телевізорів у користувачів ігнорується, а доступ для телефонів і комп'ютерів є спільним. ADSL-модеми, які підключаються до обох кінців короткої лінії між абонентом і POP, утворюють три канали: високошвидкісний спадний канал передачі даних з мережі в комп'ютер, менш швидкісний вихідний канал передачі даних з комп'ютера в мережу і канал телефонного зв'язку, по якому передаються звичайні телефонні розмови.

Кабельне телебачення - телекомунікаційна послуга з власною інфраструктурою абонентських закінчень. Кабельне телебачення використовує коаксіальні абонентські закінчення, які з'єднують будинки і квартири з POP. Коаксіальний кабель має широку смугу пропускання (700-800 МГц), тому абонентське закінчення CATV може впоратися одночасно з передачею телефонного, комп'ютерного та телевізійного трафіку. Відмінністю абонентського закінчення CATV є те, що до коаксіального кабелю підключаються одночасно декілька абонентів. Це може бути декілька десятків будинків або ж сотень квартир багатоквартирного будинку. Абонентське закінчення CATV є класичним розподільним середовищем, яке використовується в мережах Ethernet на коаксіальному кабелі.

Бездротова передача даних широко використовується для організації доступу у випадках, коли постачальник послуг з якоїсь причини не може забезпечити своїм клієнтам доступ через провідну мережу, через відсутність високошвидкісного доступу для певної будівлі, наприклад при проведенні конференції в приміщенні готелю, не оснащеному засобами провідного доступу необхідної пропускну здатності. Бездротовий доступ може бути як фіксованим, так і мобільним. Фіксований бездротовий доступ організовується для абонентів, комп'ютери яких знаходяться в межах обмеженої території - в межах будівлі. Постачальник послуг використовує спрямовану антену і передавач зазначеної потужності. Якщо у постачальника послуг є велика кількість абонентів фіксованого бездротового доступу, то він використовує декілька спрямованих антен, щоб покрити всі сектори, в яких знаходяться його абоненти.

Ethernet операторського класу (Carrier Ethernet) - послуги Ethernet, які оператори зв'язку надають в глобальному масштабі і технології, на основі яких послуги організовуються - вдосконалена версія Ethernet, MPLS та технології первинних мереж, такі як SDH,

OTN і DWDM. Внутрішня організація послуги Ethernet в межах мережі провайдера може значно відрізнятись. Виділяють **три основні варіанти** організації в залежності від внутрішньої транспортної технології, яка використовується: **Ethernet поверх MPLS** (EoMPLS) - MPLS-тунелі; **Ethernet поверх Ethernet** (Ethernet over Ethernet), транспортні засоби Ethernet операторського класу (Carrier Ethernet Transport, CET); **Ethernet поверх транспорту** (Ethernet over Transport, EOT) - транспорт, заснований на техніці комутації каналів - використовується для створення первинних мереж операторів (SDH, DWDM або OTN) [6,7].

2.6 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 вміст 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.

2.7 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 мережових 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 "). IPSec - набір протоколів для забезпечення IP комунікацій, який забезпечує шифрування, цілісність та автентифікацію. Протокол IPSec включає криптографічні методи, які задовольняють потреби керування ключами на мережевому рівні безпеки. IPSec також містить в собі протоколи для захищеного обміну ключами в мережі Інтернет. 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.

Для виконання шифрування та дешифрування за допомогою алгоритмів, які використовують симетричний секретний ключ колективного використання, необхідно його створити та роздати. Налаштування ключів може здійснюватися вручну мережевим адміністратором, або за допомогою методу обміну ключами. Погодження ключа Діффі-Хеллмана (DH) – це публічний метод обміну ключами, який дозволяє двом сторонам встановлювати секретний ключ, що використовується при передачі даних по незахищеному каналі. В групах Діффі-Хеллмана має бути вказаний тип криптографії:

- DH GROUP 1 – використовується 768-бітна криптографія;
- DH GROUP 2 – тільки для пристроїв Cisco IOS, PIX Firewall та пристрою адаптивного захисту Cisco (ASA), використовується 1024-бітне шифрування;
- DH GROUP 5 – підтримується при умові виконання вимог програмної системи, використовується 1536-бітне шифрування.

GRE (англ. *Generic Routing Encapsulation* - загальна інкапсуляція маршрутів) - протокол тунелювання мережеских 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 навантажувє 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`.

У зв'язку зі службовим заголовком розмір переданих даних усередині IP пакета через GRE-тунель зменшується при збереженні загального розміру пакета. У IP-пакеті передбачено наявність біта DF (do not fragment), який забороняє поділ пакета на декілька частин при передачі через середовище з меншим розміром MTU. У цьому випадку пакет з розміром корисної області даних, яка перевищує MTU IP пакету в GRE-тунелі, відкидається, що призводить до втрат пакетів при істотному навантаженні (проходять пакети малого розміру, такі як SYN пакети TCP, ICMP повідомлення (ping), але губляться пакети з даними в TCP потоці (тобто з'єднання рветься)). Для вирішення цієї проблеми рекомендується використовувати path-mtu-discovery (визначення TCP MSS, тобто максимального розміру IP-пакетів на всьому шляху) при передачі даних через GRE-тунель, щоб уникнути надмірної фрагментації або втрати великих пакетів [8].

2.8 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 зломисникові 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 настраюється 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 пристроям 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].

2.9 Налаштування доступу в Інтернет через cisco vpn client

Виконаємо налаштування доступу в інтернет через cisco VPN client і корпоративний cisco router, підключений до провайдера по PPPoE. Необхідно організувати IPsec VPN між корпоративним мережним пристроєм і в інтернет виходити через нього. З'явиться реальна можливість безпечно використовувати внутрішні ресурси корпоративної мережі. Для цього досить мати router з підтримкою VPN. Схема наступна (рис.2.2):

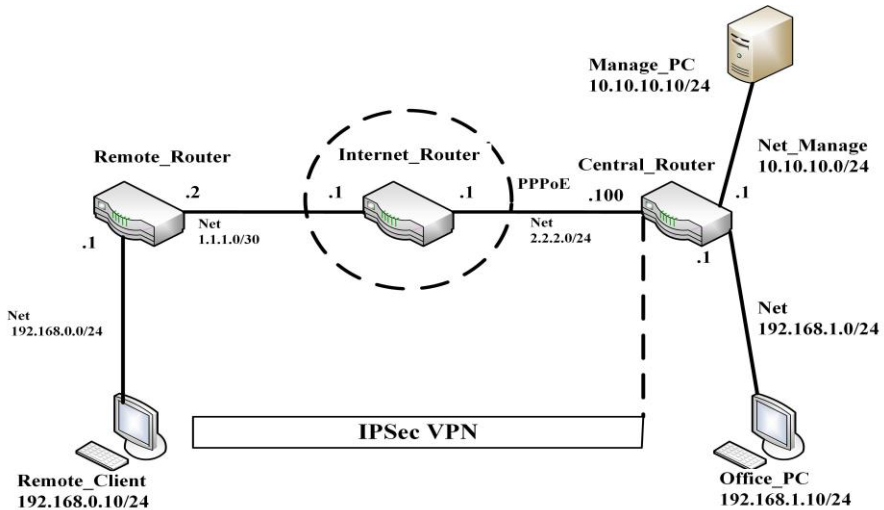


Рисунок 2.2 – Схема мережі

Пояснення до схеми. Є центральний офіс, де розташований Central_Router. Через даний пристрій співробітники отримують доступ в інтернет. На ньому є 3 інтерфейси:

- FEthernet 0/0 - підключений до інтернет. 2.2.2.100/24 - адресу він отримує від провайдера по протоколу PPPoE. Також інтерфейс використовується як outside при налаштуванні NAT, і на нього приходять запити від клієнтів на встановлення VPN тунелю;

- FEthernet 1/0 - підключений до локальної мережі з IP-адресом 192.168.1.1/24. Цей інтерфейс є inside для NAT. В даній мережі розташовані внутрішні ресурси і користувачі;

- FEthernet 2/0 - підключений до мережі управління (Manage). IP-адреса 10.10.10.1/24. У цій мережі розташована консоль (Manage_PC 10.10.10.10/24) для налаштування роутера.

Далі є Internet_Router. За допомогою нього емулюється мережа Internet і він налаштовується як PPPoE Server, для обслуговування підключення центрального офісу (Central_Router). Будемо вважати що Internet_Router має публічні адреси на інтерфейсах і видає їх клієнту (2.2.2.100/24 - публічна IP-адреса).

Далі Remote_Router, використовуємо в якості доступу до Internet віддалених клієнтів. На ньому є два інтерфейси:

- FEthernet0/0 - підключений до ЛОМ з адресою 192.168.0.1/24, де знаходиться віддалений клієнт. Адреса є inside для NAT;

- FEthernet1/0 - підключений до мережі Internet. IP-адреса 1.1.1.2/24 Цей інтерфейс є outside для NAT;

Для перевірки є два комп'ютера:

- перший (Office_PC) в ЛОМ офісу (192.168.1.10/24);
- другий (Remote_Client) розташовується у віддаленій мережі (192.168.0.10/24) з cisco VPN client для побудови VPN тунелю.

Почнемо з віддаленого роутера. Заходимо на Remote_Router:

```
R1#conf t
R1(config)#hostname Remote_Router - задаємо ім'я;
Remote_Router(config)#int fa 0/0
Remote_Router(config-if)#ip address 192.168.0.1 255.255.255.0
- встановлюємо IP-адресу;
Remote_Router(config-if)#no cdp enable - вимикаємо CDP;
Remote_Router(config-if)#ip nat inside - вказуємо, що
інтерфейс буде inside для NAT;
Remote_Router(config-if)#no shutdown - вмикаємо інтерфейс;
Remote_Router(config-if)#exit
Remote_Router(config)#int fa 1/0
Remote_Router(config-if)#ip address 1.1.1.2 255.255.255.252
Remote_Router(config-if)#ip nat outside - вказуємо, що
інтерфейс буде outside для NAT;
Remote_Router(config-if)#no shutdown
Remote_Router(config-if)#exit
Remote_Router(config)#ip access-list extended FOR_NAT -
створюємо список доступу для NAT;
Remote_Router(config-ext-nacl)#permit ip 192.168.0.0
```

```
0.0.0.255 any
Remote_Router(config-ext-nacl)#deny ip any any
Remote_Router(config-ext-nacl)#exit
Remote_Router(config)#ip nat inside source list FOR_NAT
interface fa 1/0 overload - вмикаємо NAT на роутері;
Remote_Router(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.1 -
прописуємо маршрут за замовченням;
Remote_Router(config)#exit
Remote_Router#wr - зберегаємо конфігурацію.
```

Переходимо на роутер Internet_Router:

```
R2#conf t
R2(config)#hostname Internet_Router
Internet_Router(config)#int fa 0/0
Internet_Router(config-if)#ip address 1.1.1.1 255.255.255.252
Internet_Router(config-if)#no shutdown
Internet_Router(config-if)#exit
Internet_Router(config)#interface virtual-template 1 -
заходимо в налаштування шаблону інтерфейсу користувача для
PPPoE клієнтів;
Internet_Router(config-if)#ip address 2.2.2.1 255.255.255.0 -
вказуємо IP-адресу, яка буде gateway для PPPoE клієнтів;
Internet_Router(config-if)#ip virtual-reassembly
Internet_Router(config-if)#ip unnumbered fastEthernet 1/0 -
визначаємо інтерфейс, на який будуть приходити запити на
встановлення PPPoE з'єднань;
Internet_Router(config-if)#ppp authentication chap ms-chap -
визначаємо вид аутентифікації для PPPoE клієнтів;
Internet_Router(config-if)#exit
Internet_Router(config)#bba-group pppoe global - вмикаємо
підтримку PPPoE на роутері;
*Mar 1 00:24:45.303: %LINK-3-UPDOWN: Interface Virtual-
Access2, changed state to up
*Mar 1 00:24:46.303: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access2, changed state to up
Internet_Router(config-bba-group)#virtual-template 1 -
прив'язуємо до цієї групи раніше створений шаблон;
Internet_Router(config-bba-group)#sessions max limit 100 -
обмежуємо кількість сесій;
Internet_Router(config-bba-group)#sessions per-mac limit 1 -
одна мас-адреса на сесію;
Internet_Router(config-bba-group)#sessions auto cleanup -
вмикаємо автоматичне очищення сесій;
Internet_Router(config-bba-group)#exit
Internet_Router(config)#int fa 1/0
Internet_Router(config-if)#pppoe enable group global -
вмикаємо PPPoE на потрібному інтерфейсі;
Internet_Router(config-if)#no shutdown
```

```

Internet_Router(config-if)#exit
Internet_Router(config)#aaa new-model - вмикаємо функцію aaa на роутері;
Internet_Router(config)#aaa authentication ppp default local
- вказуємо, що процес аутентифікації PPPoE клієнтів буде використовувати локальну базу користувачів;
Internet_Router(config)#aaa authorization network default local
- процес авторизації PPPoE клієнтів також буде використовувати локальну базу;
Internet_Router(config)#aaa attribute list PPPOE - створюємо перелік атрибутів (далі прив'яжемо його до конкретного клієнта, щоб отримувати конкретну IP-адресу);
Internet_Router(config-attr-list)#attribute type addr 2.2.2.100 service ppp protocol ip - прописуємо конкретний IP-адрес, який нам потрібен;
Internet_Router(config-attr-list)#exit
Internet_Router(config)#username PPPOE_User privilege 0 password cisco - створюємо PPPoE користувача;
Internet_Router(config)#username PPPOE_User aaa attribute list PPPOE - прив'язуємо до нього перелік атрибутів (тепер цей клієнт отримає конкретну IP-адресу, вказану в атрибутах);
Internet_Router(config)#exit
Internet_Router#wr

```

3 Internet_Router закінчили. Тут ми налаштували видачу конкретної IP-адреси конкретному клієнту. Можна зробити видачу IP-адрес PPPoE клієнтам більш розширено, налаштувавши або пул адрес, або DHCP.

Тепер переходимо до Center_Router.

```

R3#conf t
R3(config)#hostname Center_Router
Center_Router(config)#int fa 1/0
Center_Router(config-if)#ip address 192.168.1.1 255.255.255.0
Center_Router(config-if)#ip nat inside
Center_Router(config-if)#no cdp enable
Center_Router(config-if)#no shutdown
Center_Router(config-if)#exit
Center_Router(config)#int fa 2/0
Center_Router(config-if)#ip address 10.10.10.1 255.255.255.0
Center_Router(config-if)#no cdp enable
Center_Router(config-if)#no shutdown
Center_Router(config-if)#exit
Center_Router(config)#interface dialer 1 - створюємо спеціальний інтерфейс Dialer, який і підніме PPPoE;
Center_Router(config-if)#ip address negotiated - вказуємо, що IP-адреса буде прийматися від провайдера;
Center_Router(config-if)#ip mtu 1492 -вказуємо mtu для PPPoE;

```

```

Center_Router(config-if)#ip nat outside - цей інтерфейс буде outside і через нього користувачі будуть виходити в інтернет;
Center_Router(config-if)#encapsulation ppp - інкапсуляція;
Center_Router(config-if)#dialer pool 1 - задаємо № пулу для прив'язки на фізичному інтерфейсі;
Center_Router(config-if)#ppp chap hostname PPPOE_User - вказуємо ім'я користувача на Internet_Router (дає провайдер);
Center_Router(config-if)#ppp chap password cisco - вказуємо пароль користувача;
Center_Router(config-if)#exit
Center_Router(config)#int fa 0/0
Center_Router(config-if)#pppoe-client dial-pool-number 1 - прив'язуємо фізичний і Dialer через раніш заданий пул;
Center_Router(config-if)#no shutdown
Center_Router(config-if)#exit
Center_Router(config)#
*Mar 1 00:07:45.407: %DIALER-6-BIND: Interface V11 bound to profile D11
*Mar 1 00:07:45.463: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 1 00:07:46.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up - це означає, що інтерфейс піднявся;
Center_Router(config)#ip access-list extended FOR_NAT - створюємо список доступу для NAT;
Center_Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 any
Center_Router(config-ext-nacl)#deny ip any any
Center_Router(config-ext-nacl)#exit
Center_Router(config)#ip nat inside source list FOR_NAT interface dialer 1 overload - включаємо NAT на роутері;
Center_Router(config)#ip route 0.0.0.0 0.0.0.0 dialer 1 - прописуємо маршрут за замовчуванням через інтерфейс Dialer 1;
Center_Router(config)#exit
Center_Router#wr

```

Приклад повного налаштування мережі наведено у статті електронного ресурсу [9].

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.

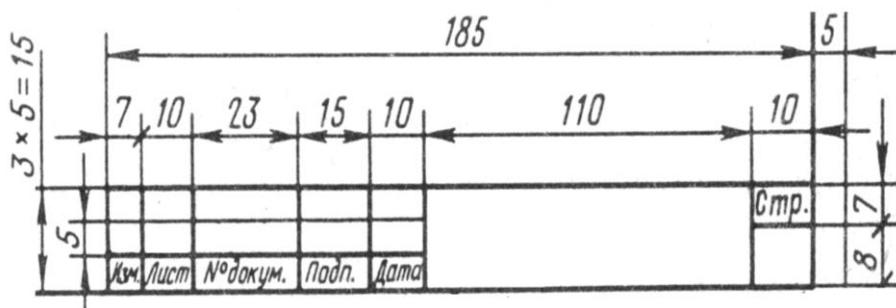


Рисунок 3.1 – Форма надпису в пояснювальній записці

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.

Четверта сторінка – реферат, який оформлюється в основній рамці з повним надписом (рис. 3.2), в якому наводиться визначання десятичного номеру пояснювальної записки, підписи студента, керівника, назва курсового проекту, номер листа (4) та кількість листів в пояснювальній записці. Зразок оформлення реферату наводиться в додатку Д.

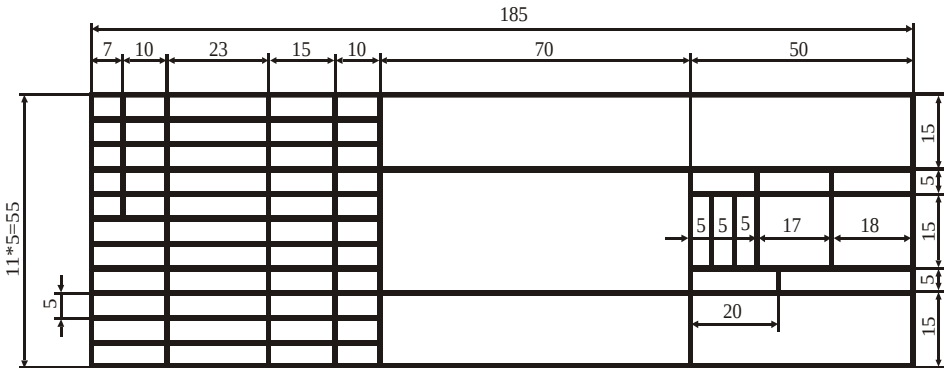


Рисунок 3.2 – Форма рамки для реферату курсового проекту

3.2 Вимоги до оформлення графічних документів

Графічні документи курсового проекту пропонуються 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 (210x290) 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.

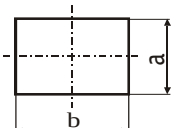
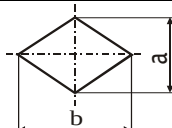
Графічна частина курсового проекту обов'язково повинна містити в собі два або одне креслення.

3.3 Схеми алгоритмів, програм, даних та систем

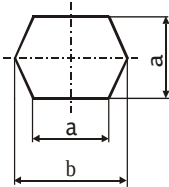
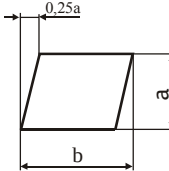
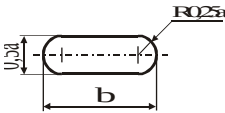
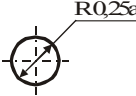
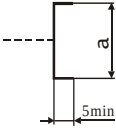
Схеми алгоритмів, програм, даних та систем (далі схеми) складаються з наявних значень символів, стислого пояснювального тексту та з'єднувальних ліній.

Нижче надані символи для використання в документації даних і наведені їх умовні зазначення (табл. 3.1) для використання їх в схемах алгоритмів.

Таблиця 3.1 - Символи

Найменування	Позначення й розміри, мм	Функція
Процес		Виконання операції або групи операцій, в результаті яких змінюється значення, форма подання або розташування даних
Рішення		Вибір напрямлення виконання алгоритму або програми в залежності від деяких змінних умов

Продовження таблиці 3.1

Назва	Позначення та розміри, мм	Функція
Модифікація		Виконання операцій, які мають команди або групу команд, що змінюють програму
Введення – виведення		Перетворення даних в схему, яку можна використовувати для обробки (введення) або відображення результатів обробки (виведення)
Лінія потоку		Визначення послідовності зв'язків між символами
Паралельні дії		Початок або кінець двох або більше одночасно виконаних операцій
Пуск, зупинка		Початок, переривання, кінець обробки даних або виконання програм
З'єднувач		Визначення зв'язку між перериваннями ліній потоку, які зв'язують символи
Коментар		Зв'язок між елементом схеми та поясненням

Розмір **a** повинен вибиратись з ряду 10, 15, 20 мм. Розмір **a** дозволяється збільшувати на число кратне 5. Розмір **b** дорівнює $1,5a$.

Усі символи в схемі повинні бути пронумеровані. Порядковий номер проставляють зліва в верхній частині символу у розриві контуру (рис. 3.3).

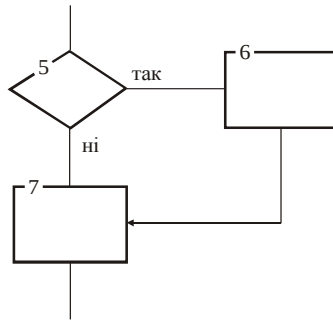


Рисунок 3.3 – Приклад частини алгоритму програми

В схемах, якщо направлення лінії потоку зліва направо або зверху вниз то стрілка не ставиться, в інших випадках стрілка ставиться. В випадках, коли відображаються варіанти рішення (наприклад, так, ні), вони ставляться над лінією потоку або справа від неї.

3.4 Вимоги до виконання електричних 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.

Схема – це графічний конструкторський документ, на якому відображені у вигляді умовних зображень або позначень складові частини виробу та зв'язки між ними. Схеми використовуються під час вивчення принципу дії механізмів, машин, пристроїв, апаратів, при їх налагодженні та ремонті, монтажі трубопроводів та електричних мереж, для пояснення зв'язку між окремими складових частин виробів без уточнення особливостей їх конструкцій.

Схеми в залежності від елементів й зв'язків між ними розділяються на такі види:

- структурна схема Е1 (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);

- загальна схема Е6 (визначає складові частини комплексу й з'єднання їх між собою на місці експлуатації);

- схема розміщення (визначає розміщення складових частин виробу, при необхідності також джгутів, проводів, кабелю, трубопроводів);

- об'єднана схема (схема, коли на одному конструктивному документі виконуються схеми двох або кількох типів, випущених на один виріб).

Зразки схем наведено в додатках Г та Е.

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. Методичні вказівки до виконання самостійних робіт з дисципліни "Комп'ютерні мережі" для студентів напряму підготовки 6.050102 "Комп'ютерна інженерія", усіх форм навчання / Укл. Г.Г Киричек. – Запоріжжя: ЗНТУ, 2015. – 46 с.
5. Платунова С.М. Методы проектирования фрагментов компьютерной сети – СПб: НИУ ИТМО, 2012. – 51 с.
6. 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.
7. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.
8. Палмер М. Проектирование и внедрение компьютерных сетей / М.Палмер, Р. Синклер. – СПб.: БХВ-Петербург, 2004. – 752с.
9. Настройка доступа в интернет через cisco VPN client и корпоративный cisco router, подключенный к провайдеру по PPPoE – [Электронный ресурс] Режим доступа: http://www.go-to-easyit.com/2012/08/cisco-vpn-client-cisco-router-pppoe_8449.html.

Додаток А

Приклади оформлення бібліографічного опису

1. Биков В. Ю. Моделі організаційних систем відкритої освіти = Models of the Education Organizational Systems: [монографія] / В. Ю. Биков. – Київ : Атіка, 2009. – 682 с.
2. Вершина А.И. Модель отримання знань [Текст] / А.И. Вершина, Г.Г. Киричек // Тиждень науки: наук.-техн. конф., 19-23 квіт. 2010 р.: тези доп. – Запоріжжя: ЗНТУ, 2010. – Т. 2. – С.115–116.
3. Нортроп Т. Проектирование сетевой инфраструктуры Windows Server 2008. Учебный курс Microsoft [Текст] / Т. Нортроп, Дж. К. Макин // Пер. с англ. – М. : Издательство «Русская Редакция», 2009. – 592с.
4. Мосіяшенко В.А. Мережі [Текст] : навч. посіб. / В. А. Мосіяшенко. – Суми : Унів. кн., 2005. – 174 с. – ISBN 966-680-198-1.
5. Лепа Є.В. Системи підтримки прийняття рішень. Частина 1 [Текст] / Є.В. Лепа, Є.К. Міхеєв, В.В. Крініцин. // Навчальний посібник. – Херсон, 2006. – 324 с.
6. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання [Текст] : (ГОСТ 7.1-2003, ІДТ) : ДСТУ ГОСТ 7.1:2006. – К. : Держспоживстандарт України, 2007. – 47 с. ; 29 см. – (Система стандартів з інформації, бібліотечної та видавничої справи) (Національний стандарт України).
7. Perez K. Radiation therapy for cancer of the cervix / K. Perez // Oncology. – 1993. – Vol. 7, №2. – P. 89–96.
8. Камишин В. В. Система оцінки науково-технічних програм та напрямків за допомогою експертного опитування методом “ДЕЛЬФІ” / В. В. Камишин, А. М. Рибак, І. М. Петрінко [та ін.] // VIII Междунар. науч.-практ. конфер. ”Система научно-технической информации: проблемы развития и функционирования” : тезисы док. и сообщ., 30–31 мая 2001 г. – К. : УкрИНТЭИ, 2001. – С. 71–76.
9. Життєвий цикл програмного засобу – [Електронний ресурс] Режим доступу: <http://mu.od.ua/zhittieviy-tsikl-programnogozasobu.html>.

Додаток Б

Форма № 17

Комп'ютерні системи та мережі

(повна назва кафедри)

**КУРСОВИЙ ПРОЕКТ
(РОБОТА)**з Проектування комп'ютерних мереж
(назва дисципліни)на тему: _____
_____Студента (ки) _____ курсу _____ групи
напряму підготовки _____
спеціальності _____

(прізвище та ініціали)

Керівник _____

(посада, вчене звання, наук. ступінь, прізвище та
ініціали)

Національна шкала _____

Кількість балів: _____ Оцінка: ECTS _____

Члени комісії _____
(підпис) (прізвище та ініціали)_____
(підпис) (прізвище та ініціали)_____
(підпис) (прізвище та ініціали)

м. Запоріжжя

20__ рік

Додаток В**Форма №24****Запорізький національний технічний університет**

(повне найменування вищого навчального закладу)

Інститут, факультет _____

Кафедра _____

Рівень вищої освіти (освітньо-кваліфікаційний рівень) _____

Напрямок підготовки _____

(код і назва)

Спеціальність _____

(код і назва)

ЗАВДАННЯ

на курсовий проект студенту

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) _____

керівник проекту (роботи) _____

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від

“ ____ ” _____ 20__ року № ____

2. Строк подання студентом проекту (роботи) _____

3. Вихідні дані до проекту (роботи) _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) _____

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів курсового проекту (роботи)	Срок виконання етапів проекту (роботи)	Примітка

Студент

(підпис) (прізвище та ініціали)

Керівник проекту

(підпис) (прізвище та ініціали)

Структурная схема сети

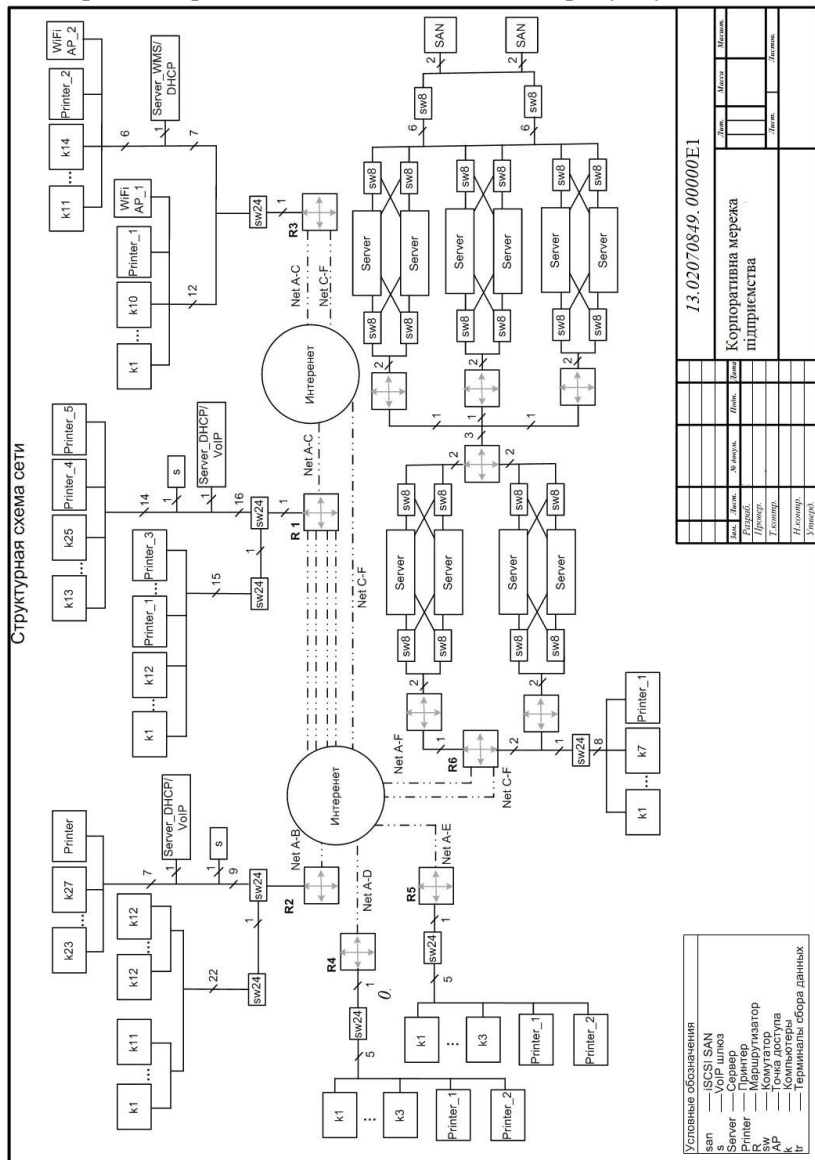


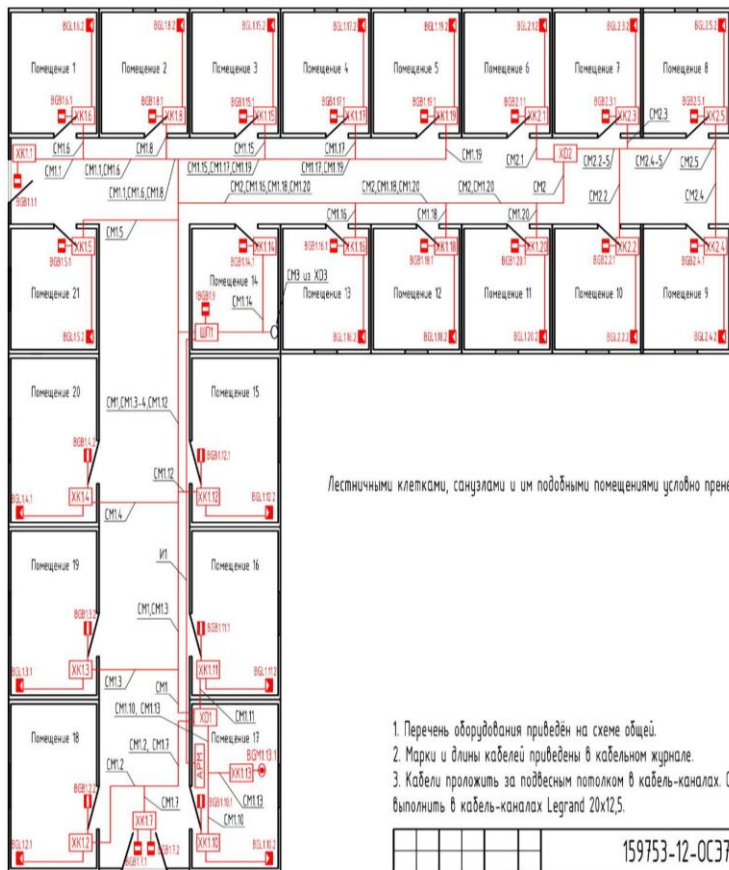
Рисунок Г.1 – Структурна схема мережі.

WI-FI, IEEE 802.11G, GIGABIT ETHERNET, 1000BASE-T,
CEPBEP, VPN, IPSEC, VOIP, VLAN

[illegible]

Додаток Е

Схема расположения ТСО и кабельных трасс на первом этаже.



Лестничными клетками, санузлами и им подобными помещениями условно пренебрегаем.

1. Перечень оборудования приведен на схеме общей.
2. Марки и длины кабелей приведены в кабельном журнале.
3. Кабели проложить за подвесным потолком в кабель-каналах. Спуски к ТСО выполнить в кабель-каналах Legrand 20x12,5.

159753-12-ОС37					
Гатчинский нефтеперерабатывающий завод					
Изм.	Желуд	Лист	ИВЖ	Подп	Дата
Административно-бытовой корпус. Система охранной сигнализации.				Листов	Листов
Начальник				P	1
Инженер				3АО	
Прораб				Интернет-проект	
Инженер					

Схема общая

