МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та математичного моделювання

КОМП'ЮТЕРНІ МЕРЕЖІ

МЕТОДИЧНІ ВКАЗІВКИ
до курсового проектування
для здобувачів
першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми «Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано
на засіданні кафедри
Кібербезпеки та математичного
моделювання
Протокол №2
від 13 лютого 2024 р.

Чернігів 2024

Комп’ютерні мережі. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с.

Укладачі: СЕМЕНДЯЙ СЕРГІЙ МАТВІЙОВИЧ, старший викладач кафедри кібербезпеки та математичного моделювання;
ПЕТРЕНКО ТАРАС АНАТОЛІЙОВИЧ, доцент кафедри кібербезпеки та математичного моделювання, кандидат технічних наук;
ШЕЛЕСТ МИХАЙЛО ЄВГЕНОВИЧ, професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор
ГРЕБЕННИК АЛЛА ГРИГОРІВНА, старший викладач кафедри кібербезпеки та математичного моделювання;

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,
завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Рецензент – МЕХЕД ДМИТРО БОРИСОВИЧ,
доцент кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук, доцент

ЗМІСТ

ВСТУП

Вивчення комп'ютерних мереж є невід'ємною частиною навчання для студентів, які обрали спеціальність "Кібербезпека". Ця область знань важлива з багатьох причин, починаючи з того, що майже будь-який аспект сучасного життя пов'язаний з використанням комп'ютерів і мереж. Кіберзлочинці і загрози кібербезпеці використовують комп'ютерні мережі для атак та злому систем, тому розуміння їх функціонування є важливим для розробки і впровадження ефективних заходів захисту.

По-перше, комп'ютерні мережи становлять основу інтернету і міжнародних комунікацій, тож знання їх структури та принципів роботи є критичним для аналізу загроз та знаходження слабких місць в існуючих системах.

По-друге, студенти, які вивчають комп'ютерні мережі, розвивають навички, які допомагають їм розуміти як загрози проникають в системи через мережі, так і як їх можна запобігти.

По-третє, розуміння комп'ютерних мереж сприяє ефективному використанню інструментів і технологій для моніторингу та аналізу мережевого трафіку з метою виявлення аномалій і потенційних загроз. Крім того, це допомагає створювати більш безпечні системи та вдосконалювати заходи кібербезпеки.

1. МЕТА ТА ЗАВДАННЯ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт – важливий етап навчального процесу та науково-дослідної роботи студента, її виконання сприяє поглибленому ознайомленню з додатковою науково-технічною літературою, документами, форумами, науковими працями вітчизняних та закордонних вчених. Також студенти набувають практичних навичок самостійно вирішувати задачі, критично мислити, шукати необхідну літературу, чітко і лаконічно формулювати запитання та формувати запити.

Мета роботи – одержання практичних навичок розробки об’єднаних комп’ютерних мереж (КМ) та аналіз їх функціонування у сучасному середовищі. Вміння проєктувати та адмініструвати, як локальні так і об’єднані мережі масштабу підприємства. Отримання практичних знань з організації доступу до мережі Internet. А також: узагальнення, закріплення та поглиблення теоретичних та практичних знань зі спеціальності; використання цих знань для обґрунтованого прийняття проєктних рішень та для вирішення конкретних задач; практичне закріплення навичок розробки комп’ютерних мереж масштабу підприємства.

Завдання до курсового проєкту передбачають розробку структурної схеми об'єднаної мережі підприємства (загальна кількість кінцевих вузлів не менше 50), планування топології кожної локальної обчислювальної мережі (ЛОМ, англ. local area network, LAN) з яких складається об’єднана мережа, призначення IP-адрес, планування визначення імен, з’єднання через маршрутизатори окремих ЛОМ підприємства, здійснення віддаленого доступу до мережі та забезпечення мережевої безпеки, як у дротових так і в бездротових ЛОМ.

На всіх етапах проєктування необхідно проводити оцінку альтернативних варіантів побудови КМ та її окремих частин.

2. ТЕМАТИКА КУРСОВИХ РОБІТ

Тема курсового проєкту вибирається студентом самостійно із рекомендованого списку:

1) Комп’ютерна мережа ПАТ «Чернігівський хлібокомбінат» Україна, 14037, м. Чернігів, вул. Громадська, 41.

2) Комп’ютерна мережа ПАТ "Чернігівський молокозавод" Україна, 14021, м. Чернігів, вул. Любецька, 76.

3) Комп’ютерна мережа Чернігівського відділення ПАТ «САН ІнБев Україна» Україна, 14037, м. Чернігів, вул. Інструментальна, 20.

4) Комп’ютерна мережа ПАТ «Млибор» Україна, 14026, м. Чернігів, вул. Елеваторна, 1.

5) Комп’ютерна мережа ПрАТ «Чернігівська швейна фабрика «Елегант» Україна, 14017, м. Чернігів, пр. Перемоги, 41.

6) Комп’ютерна мережа ПрАТ «Чернігівська взуттєва фабрика «Берегиня» Україна, 14000, м. Чернігів, вул. Родимцева, 16.

7) Комп’ютерна мережа ТОВ "Чернігіввовна-плюс” Україна, 14001, м. Чернігів , вул. Текстильників, 1.

8) Комп’ютерна мережа ПАТ «Поліграфічно-видавничий комплекс «Десна» 14000, м. Чернігів, проспект Перемоги, 62.

9) Комп’ютерна мережа ПрАТ “Чернігівський цегельний завод №3” Україна, 14010, м. Чернігів, вул. Попова, 6.

10) Комп’ютерна мережа ПрАТ "Чернігівський Інструментальний завод" Україна, 14037, м. Чернігів, вул. Інструментальна, 18.

11) Комп’ютерна мережа ПАТ «Продовольча компанія «Ясен» Україна, 14007, м. Чернігів, вул. Громадська, 41-а.

12) Комп’ютерна мережа ПАТ "Чернігівська кондитерська фабрика "Стріла" Україна, 14005, г. Чернігів, вул. Комунальна, 2.

13) Комп’ютерна мережа ТОВ «Торговий дім «Чернігівській» 14021, м. Чернігів, вул. Старобілоуська, 71.

14) Комп’ютерна мережа Чернігівської філії ПАТ «Укртелеком», 14000, Чернигов, проспект Миру, 28.

15) Комп’ютерна мережа Управління Північного офісу Держаудитслужби в Чернігівській області, 14000, м. Чернігів, вул. Єлецька, 11.

16) Комп’ютерна мережа Головного управління ДСНС України в Чернігівській області, 14037, м. Чернігів, проспект Миру, 190-А.

17) Комп’ютерна мережа Головного управління Держгеокадастру у Чернігівській області, 14000, м.Чернігів, вул. П’ятницька,11 А.

18) Комп’ютерна мережа Управління ДМС у Чернігівській області, 14039 Чернігів, вулиця Шевченка, 51А.

19) Комп’ютерна мережа Чернігівського обласного центру зайнятості, 14000, м. Чернігів, вул. Коцюбинського, 40

20) Комп’ютерна мережа Головного управління ДПС у Чернігівській області, 14000, м. Чернігів, вул. Ремісничa, 11.

21) Комп’ютерна мережа Головного управління статистики у Чернігівській області, 14000, м.Чернігів, вул. Гонча, 37.

22) Комп’ютерна мережа Державної екологічної інспекції у Чернігівській області, 14017, м.Чернігів, вул. Пантелеймонівська, 12.

23) Комп’ютерна мережа Чернігівської міської ради, 14000, м.Чернігів, вул.Магістратська,7.

24) Комп’ютерна мережа Управління освіти і науки Чернігівської ОДА, 14013, м. Чернігів, вул. Шевченка, 34.

25) Комп’ютерна мережа Комунального підприємства «АТП-2528» Чернігівської міської ради, 14034, м. Чернігів, проспект Михайла Грушевського, 173.

26) Комп’ютерна мережа Комунального підприємства «Зеленбуд» Чернігівської міської ради, 14034, м. Чернігів, вул. 1-го Травня, 168-А.

27) Комп’ютерна мережа Комунального підприємства «Чернігівводоканал» Чернігівської міської ради, 14017, м.Чернігів, вул.Жабинського, 15.

28) Комп’ютерна мережа Комунального підприємства «ЖЕК-13» Чернігівської міської ради, 14026, м. Чернігів, вул. Авіаторів, 22а.

29) Комп’ютерна мережа Комунального підприємства «Міськсвітло» Чернігівської міської ради, 14001, м. Чернігів, вул. Робітнича, 6.

30) Комп’ютерна мережа корпусу № 1 Національного університету "Чернігівська політехніка", 14035, м. Чернігів, вул. Шевченка, 95.

Можливий індивідуальний вибір студентом теми курсового проєкту за узгодженням з викладачем.

Дві однакових теми в межах однієї академічної групи допускається лише за узгодженням з викладачем. В такому випадку результати виконання курсового проєкту не можуть збігатись більше ніж на 20%.

В окремих випадках, при виборі складної теми, допускається виконання курсового проєкту групою студентів (2-3 студенти).

3. СТРУКТУРА КУРСОВОГО ПРОЄКТУ, ОСНОВНІ ЕТАПИ ЙОГО ВИКОНАННЯ

3.1. Календарний план та отримання завдання

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

Рекомендований графік роботи наведено в таблиці 3.1 Студент може корегувати графік в межах наведених дат, не змінюючи дати захисту.

У відповідності до теми керівник видає технічне завдання на курсовий проєкт з вказівкою термінів виконання окремих етапів та всього проєкту в цілому.

У завданні повинно бути чітко визначено такі данні: назва проєкту, призначення комп'ютерної мережі, що розробляється, вихідні данні до проєктування та умови експлуатації, перелік загальних питань, які розглядаються та відображаються в проєкті.

Таблиця 3.1– Етапи виконання курсового проєкту

№ п/п	Назва етапів курсового проєкту	Термін виконання
1	Отримання технічного завдання	
2	Аналіз технічного завдання	
3	Робота з літературою	
4	Розробка функціональної схеми мережі	
5	Вибір технологій локальних і глобальних сегментів об'єднаної мережі	
6	Розробка структурної схеми об'єднаної мережі підприємства	
7	Вибір і налаштування маршрутизаторів, згідно політики безпеки об'єднаної мережі підприємства і ISP (постачальника послуг Інтернет), отримання пулу відкритих адрес	
8	Організація віддаленого доступу до мережі	
9	Вибір та налаштування роботи протоколів маршрутизації	
10	Вибір та розміщення мережевого і клієнтського обладнання	
11	Вибір та налаштування ОС	
12	Забезпечення мережевої безпеки	
13	Призначення IP-адрес та DNS-імен	
14	Монтаж мережі. Об'єднання віддалених сегментів	
15	Оформлення ПЗ та захист КП	

Календарний графік виконання курсового проєкту, який складається студентом (за прикладом календарного плану) і затверджується керівником проєкту, повинен відповідати етапам розробки, вивченню та аналізу загальних

питань стосовно до всього об’єкту проєктування в цілому.

3.2. Структура курсового проєкту

В процесі проєктування мережі рівня підприємства студенту рекомендовано розглянути наведені нижче питання, тримаючись загального плану проєкту.

Основні етапи проєктування можуть включати.

1) Аналіз технічного завдання:

– аналіз структури підприємства (з описом основних підрозділів і філій, з урахуванням їх віддаленості один від одного);

– аналіз інформаційних потоків (типи переданих даних);

– аналіз (для модернізації) наявних апаратних і мережевих пристроїв;

– постановку завдань, пов'язаних з проєктуванням та шляхи їх вирішення.

2) Вибір технологій, апаратних і мережевих пристроїв:

– короткий аналіз, наявних LAN і WAN технологій і вибір технологій (певних специфікацій) для конкретних ліній зв'язку між сегментами та мережами вашої організації, з урахуванням підключення філій;

– вибір мережевих пристроїв з визначенням технічних характеристик для кожного конкретного пристрою або групи ідентичних пристроїв, опис їх призначення та особливості застосування;

– вибір апаратних пристроїв (сервери, ПК, ноутбуки, термінали, планшети, IP-телефони та ін.) З описом технічних характеристик для кожного пристрою або групи пристроїв, опис призначення та особливості застосування.

3) Монтаж мережі:

– визначення основних LAN і WAN сегментів;

– проєктування структурної схеми мережі;

– побудова монтажної схеми (розміщення мережевих і апаратних пристроїв (в будівлях, на поверхах, в кімнатах));

– розрахунок кабелю і потужності антен;

– підключення (об'єднання мережевих і апаратних пристроїв єдину мережу).

4) Адміністрування мережі:

– вибір і опис операційних систем серверів та ПК;

– вибір принципу адресації для LAN і WAN сегментів (мереж);

– вибір принципів маршрутизації (опис особливостей роботи обраних протоколів маршрутизації);

– програмна настройка всього мережевого обладнання (з урахуванням адресації і маршрутизації);

– опис настроювання віддаленого доступу до філіям;

– підключення до Інтернет;

– забезпечення мережевої безпеки (налаштування обладнання, протоколів).

Кількість і назви розділів у проєкті можуть відрізнятись від наведених далі, послідовність розташування розділів може бути іншою але це не повинно впливати на загальну мету проєктування.

3.2.1. Аналіз технічного завдання

У цьому розділі пропонується провести детальний аналіз та огляд предметної області, визначити мету роботи та провести аналіз технічного завдання (ТЗ), окреслити задачі, які вирішуються при розробці об’єднаної комп’ютерної мережі, а також вказати, які особливості ТЗ визначили вибір тих чи інших рішень. Студент повинен проаналізувати структуру підприємства, визначити типи даних, що передаються та наявність апаратних і мережевих пристроїв. Визначитись із шляхами вирішення завдань, які поставленні в процесі формування технічного завдання на проєктування об’єднаної мережі підприємства.

3.2.2. Вибір технологій LAN/WAN сегментів та обладнання об’єднаної мережі підприємства

Зараз ви плануєте мережу, ви – головний, і вам ніхто не заважає. Дуже важливо продумати всі нюанси, пов'язані з побудовою мережі. Адже корпоративна мережа – це дуже складна система, яка складається з тисяч різних компонентів.

У корпоративній (об'єднаній) мережі завжди використовується 3-4 технології, як канального рівня так і ті, які накладені поверх канального рівня,

тому можуть використовуватись і найрізноманітніші пристрої. Дуже важливо орієнтуватися у цьому устаткуванні. Модель маршрутизатора, яка була популярна торік, уже давно не є такою – на її місце прийшла більш нова, з кращими функціями та 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 з контрольованим середовищем. Вона має спеціальне устаткування для фільтрації коливань напруги електромережі та підтримки температури в заданому діапазоні. Крім того, у ньому встановлюють системи архівації.

Поки мережа не стане настільки ж важливою, як робочі станції користувачів, вона повинна мати надлишкові маршрути та відповідати вимогам надійності для підтримки поетапної реалізації її плану. Тоді додаткові сегменти можуть додаватися в різних місцях, їх можна підключати до маршрутизатора при розширенні мережі в різних випадках.

Завдання IT-співробітників і сфери їхньої відповідальності повинні бути чітко розподілені. Звичайно ієрархія того або іншого підрозділу зображується у вигляді організаційної або піраміdальної діаграми.

Магістраль – один із самих головних і, отже, найдорожчих компонентів мережі. Через магістраль проходить більша частина трафіку мережі, тому вона впливає на роботу всієї мережі в цілому. Рішення про вибір магістралі є одним з найважливіших при плануванні мережі. Все частіше виникає необхідність у підвищенні пропускної здатності каналів між клієнтами мережі та серверами. Потужні комп'ютери дозволяють ефективно працювати з мультимедіа та передавати мультимедійну інформацію локальною мережею та через Інтернет.

Вибір технології магістралі – це завжди компроміс між швидкістю та вартістю. Можна вибрати все швидкодіюче і дороге, але в деяких випадках застосування такого устаткування не виправдає себе. Канали, що зв'язують сервери та мережеве устаткування, повинні бути високошвидкісними, і їх варто ізолювати від тих сегментів, у яких розташовуються робочі станції.

Мережеве керування тісно пов'язане з моделлю, технологіями і топологією мережі, оскільки одними топологіями простіше управляти, чим іншими. У багатьох випадках зіркоподібна топологія забезпечує більш швидке виявлення проблем. Крім того, мережева структура, у якій використані комутатори та маршрутизатори, простіше для моніторингу та діагностики.

В Інтернеті можна скачати різні програми для планування вашої мережі. З їхньою допомогою ви накидаєте схему мережі, що допоможе потім при розгортанні мережі. Одна з таких програм: LanFlow (рис. 3.1). Скачати ознайомлювальну версію програми можна на сайті www.pacestar.com/lanflow.

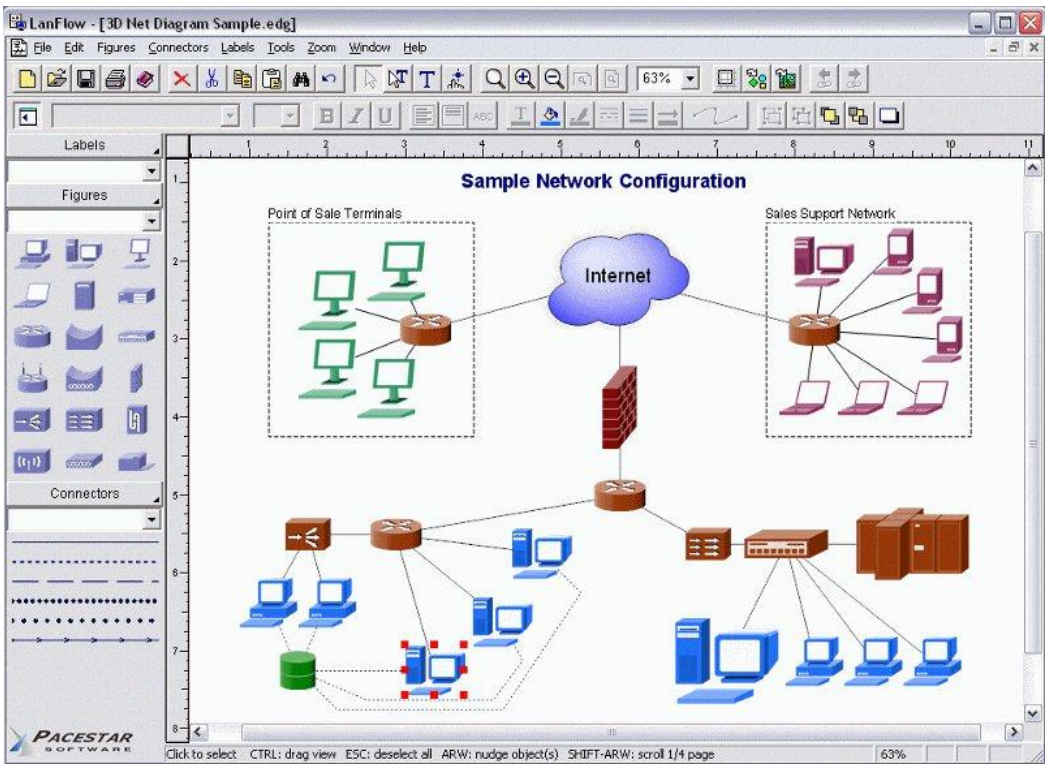

Рисунок 3.1 – Програма LanFlow

Також ви можете скористатися програмою Visio, що є в пакеті офісних програм Microsoft або вже відомим з лабораторних робіт програмним забезпеченням Cisco Packet Tracer, яке дозволяє імітувати роботу різних мережевих пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів, IP-телефонів тощо.

Загальні питання для розгляду.

1. Визначення кількості ЛОМ (як дротових так і бездротових), з яких складатиметься об'єднана мережа та вибір їх технологій.

2. Складання плану об’єднаної мережі з розбивкою на внутрішню (локальну) і зовнішню (демілітаризовану зону, периметр) частини.

3.2.3. Планування структури кожної ЛОМ об’єднаної мережі

Створення плану мережевої інфраструктури – найважливіша частина проєктування мережі. Як правило, не всі елементи інфраструктури мережі доводиться проєктувати "з нуля", деякі з них успадковуються від інших елементів.

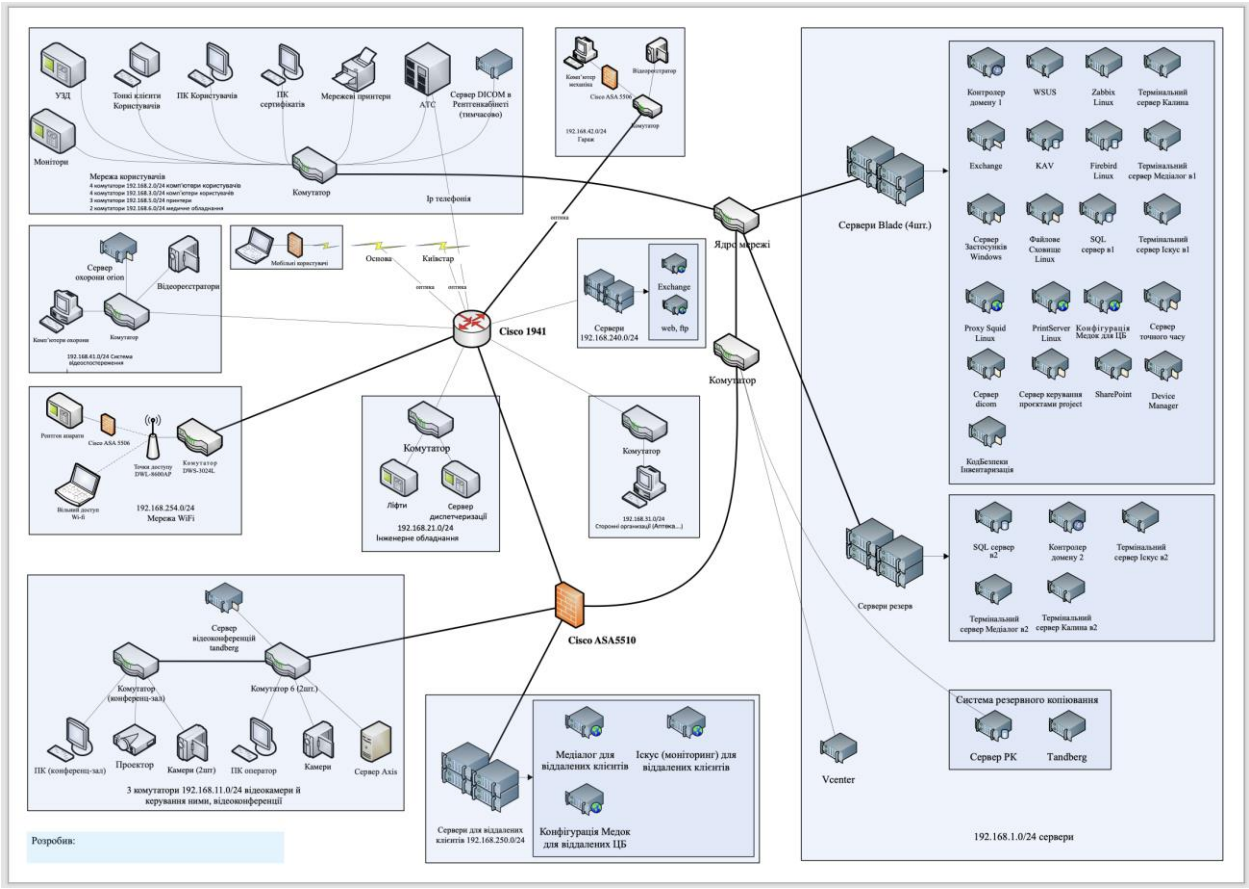

Рисунок 3.2 – Приклад структурної схеми мережі

Планування інфраструктури набагато складніше інших етапів побудови мережі, оскільки припускає створення плану, що буде використаний для монтажу мережі і підтримки її надалі. На плані повинно бути зазначене розміщення основних компонентів мережі: кабельних ліній, комутаторів і інших комунікаційних пристроїв, а також комп'ютерів і периферії.

Знаючи, які протоколи обрані для мережі, можна приступати до планування розміщення мережевих ресурсів, тому що від протоколу залежить максимальна довжина кабелю і число комутаторів у мережі.

Вибір протоколу канального рівня в основному зводиться до вибору типу несучого середовища: неекранованої 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.

Кабель UTP відносно дешевий і простий в установці, але чутливий до електромагнітних завад і має обмежену максимальну довжину. Оптоволоконні

кабелі менш чутливі до електромагнітних завад і ослаблення сигналу в порівнянні з мідними кабелями, але дорожче і складніше в установці та обслуговуванні. Перш ніж включати бездротову технологію в інфраструктуру мережі, настійно рекомендується її ретельно протестувати на ділянці, де передбачається її використання. Самі різні фактори навколишнього середовища, товщина і матеріал стін будівлі, близькість електроустаткування, і навіть погодні умови створюють перешкоди для передачі даних у бездротовій мережі. Залежно від цих умов ефективний радіус дії бездротового пристрою може змінюватися ледве не щохвилинно.

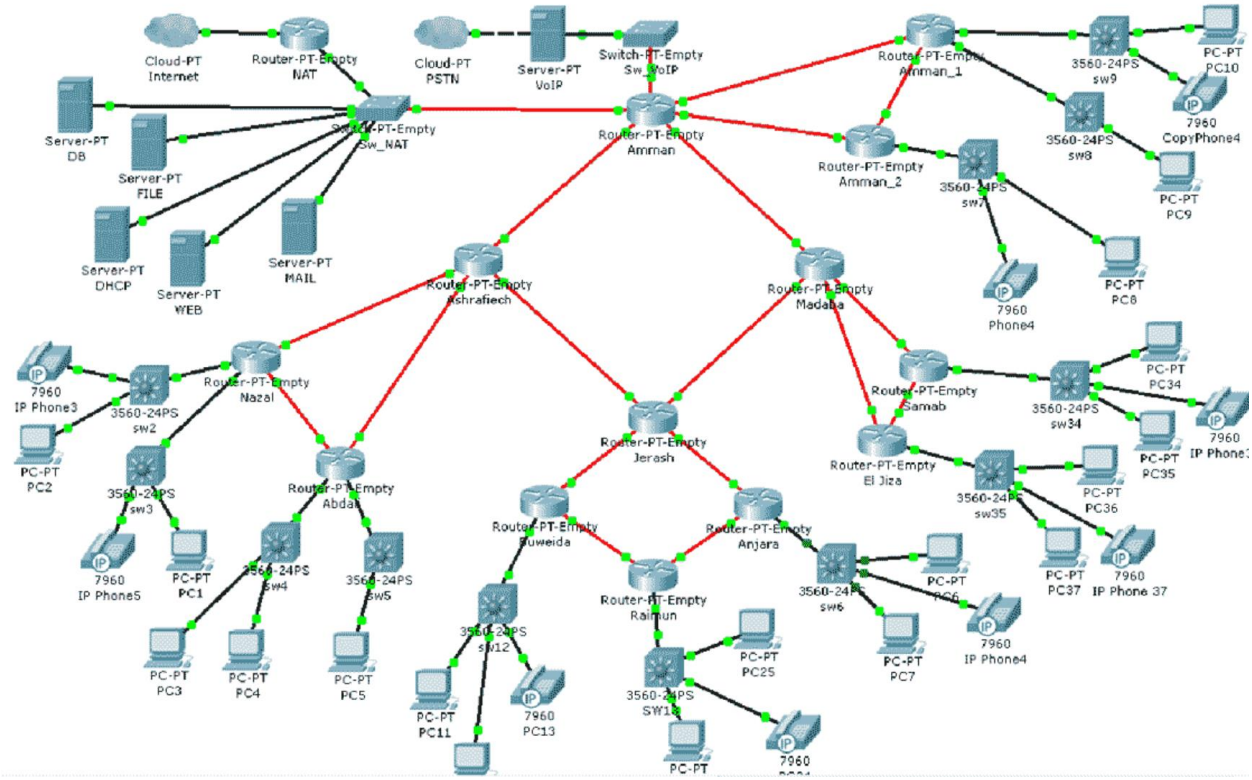

Рисунок 3.3 – Приклад функціональної схеми мережі

Схема кабельних з'єднань – важлива частина плану мережі, оскільки після монтажу мережі всі кабелі, швидше за все, будуть заховані. Крім самого кабелю, на плані необхідно вказати перешкоди, які кабель огинає, а також розташування розеток і розподільчих панелей.

TCP/IP – це пакет протоколів мережевого й транспортного рівнів, що став промисловим стандартом, підходить для більшості мереж.

При плануванні розміщення мережевих компонентів необхідно врахувати кілька критеріїв. Перший і головний – можливість доступу до устаткування, яке необхідне для виконання посадових обов'язків персоналу, тобто доступу до робочих станцій і периферійних пристроїв, таким як принтери та сканери.

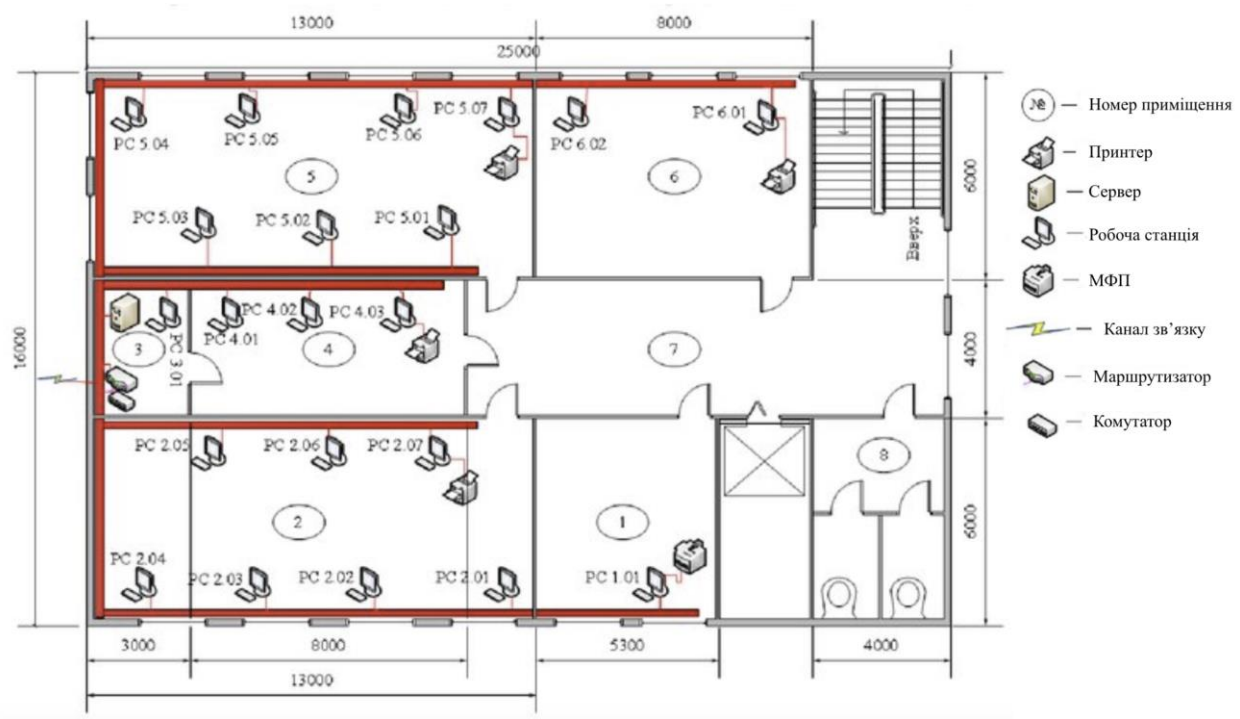

Рисунок 3.4 – Приклад монтажної схеми мережі

Не у всіх офісах у кожного є свій стіл з комп'ютером. Іноді робочі станції перебувають у загальному доступі для різних співробітників. Для таких комп'ютерів необхідно вибрати та вказати на плані зручне розміщення.

Розміщення серверів повинно бути зручним для тих, хто буде їх підтримувати та обслуговувати. У кожному разі захист серверів повинен бути надійним. Їх необхідно захищати не тільки від фізичного доступу, але також від стрибків напруги та перебоїв електроживлення. Розміщення сервера повинно враховувати розташування робочих місць користувачів, характер трафіку й бути зручним для обслуговуючого персоналу.

Загальні питання для розгляду.

1. Вибір протоколу канального рівня.

2. Вибір типу несучого середовища: неекранована вита пара, екранована вита пара, оптоволоконний кабель, бездротові канали.

3. Вибір швидкості передачі.

4. Вибір протоколів мережевого і транспортного рівнів. Складання структурних і монтажних схем для всіх ЛОМ об’єднаної мережі: критерії розміщення компонентів мережі, розміщення робочих станцій, розміщення периферійних пристроїв, прокладання кабелів, розміщення комунікаційних пристроїв, розміщення серверів.

3.2.4. Підключення до Інтернету

Плануючи стратегію підключення доступу в Інтернет, вибираючи розміщення маршрутизаторів та устаткування, треба оцінити не тільки пропускну здатність каналу зв'язку, але й розташування комп'ютерів, яким

потрібен доступ до Інтернету. Якщо доступ до Інтернету потрібен усім користувачам корпоративної мережі, то маршрутизатор найкраще підключити до магістральної мережі або до іншого центрального каналу. Якщо всі комп'ютери, яким потрібен доступ до Інтернету, наприклад група Web-серверів, розміщені окремо, то для уникнення перевантаження інших ділянок мережі Інтернет-канал варто підключати тут же.

Мінімальний набір устаткування для підключення до мережі Інтернету складається з маршрутизатора та каналу глобальної обчислювальної мережі (wide area network, WAN).

Два десятки років тому, актуальним було модемне підключення до мереж. Підключення через модем можна настроїти так, що воно буде доступним всім користувачам мережі. Однак одне модемне з'єднання через телефонну лінію забезпечує швидкість не більше 56 кбіт/с. Цього вистачить лише для декількох користувачів, та й то за умови, що вони не працюють із додатками, що вимагають високої пропускної здатності та продуктивності. На даний час практично не використовується.

Цифрова мережа комплексних послуг (Integrated Services Digital Network, ISDN) – працює через телефонні лінії. Вона вимагає підтримки з боку телефонної компанії та спеціального устаткування. Забезпечувала швидкість до 1,544 Мбіт/с. На даний час не використовується.

Рішення для доступу в Інтернет на основі мережі кабельного телебачення (КТБ) і абонентських цифрових ліній Digital subscriber line (DSL) орієнтовані, у першу чергу, на домашнього користувача, але можуть застосовуватися й у корпоративних мережах. Багато постачальників послуг КТБ мають мережі на оптоволоконному кабелі з досить щільним покриттям території. DSL – це служба високошвидкісної передачі цифрових даних по стандартних телефонних лініях. DSL являє собою виділений канал з постійною швидкістю передачі. Існує кілька типів DSL-технологій з різними назвами, включаючи ADSL і HDSL, тому DSL часто називають узагальненим ім'ям - xDSL. Говорити про xDSL потрібно переважно в історичному розрізі, оскільки свого часу ця технологія була проривною, але сьогодні мало актуальна для жителів великих міст. Максимум швидкості, доступний користувачеві виділеної лінії, – 24 Мбіт в секунду. У порівнянні з комутованим доступом, використовуваним до XDSL, прогрес очевидний. Поява технології зумовила перехід від лімітних тарифів на безлімітні.

Волокно до х (FTTX) – це загальний термін для будь-якої архітектури широкосмугової мережі, що використовує оптичне волокно. Оскільки волоконно-оптичні кабелі здатні переносити набагато більше даних, ніж мідні кабелі, особливо на великі відстані, мідні телефонні мережі, побудовані в 20 столітті, замінюються волокном. FTTB (fiber-to-the-building, -business, or -basement) – наступна після xDSL технологія, на даний момент користується найбільшим поширенням у цивілізованому світі. Принцип роботи нехитрий: в під'їзді розміщується комутатор, який з'єднують зі станцією постачальника

інтернет-послуг. У квартиру проводять виту пару, яка підключається до ПК або спеціального роутера. Головна перевага – вигідне співвідношення між швидкістю інтернету і вартістю. Гранична з можливих швидкостей – 1 Гбіт в секунду.

xPON (оптоволоконний канал). Найбільш прогресивний і сучасний спосіб з існуючих, передбачає організацію гігабітного каналу з послугами Tripple Play. Для забезпечення з'єднання проводиться спеціальний оптичний кабель, який підключають до відповідного обладнання; використовуються конвертери, sfp-модуль, оптичні термінали. Фактично технологія xPON поступово витісняє FTTB, а бізнес-інтернет часто використовують компанії, робота яких пов'язана з необхідністю передачі великих кількостей інформації.

GPRS, 3G, LTE. Оскільки у практично кожної людини сьогодні є сучасний смартфон, мобільний інтернет користується великим попитом. Переваги очевидні – можливість мати з'єднання з інтернетом буквально «під рукою», основний недолік – обмежені ліміти. За останні роки швидкість істотно зросла: якщо раніше в ходу були GPRS і 3G, то сьогодні їм на зміну прийшла технологія 4G. Гранична швидкість останньої LTE – 300 Мбіт (теоретично); в дійсності вона зазвичай істотно нижче. Для організації підключення встановлюють USB-модеми та роутери.

Супутниковий інтернет – ще одне прогресивне відгалуження, що підрозділяється на два підтипи: односторонній і двосторонній. Перший – його також називають асиметричним – припускає використання зв'язку із супутником виключно для прийому інформації, в той час як для передачі використовується звичайний зв'язок. Другий – симетричний, більш прогресивний, оскільки дозволяє здійснювати також і передачу інформації, однак для реалізації такого підключення потрібно дороге обладнання; тарифи теж досить високі. Єдина, нехай і вкрай вагома перевага – можливість отримання доступу в будь-якій точці світу.

WiFi і WiMax. Переважна більшість сучасних пристроїв – телевізори, телефони, смартфони – мають вбудований модуль Wi-Fi, що забезпечує стабільний зв'язок з інтернетом в межах певної області. Великі бездротові мережі проводять переважно у великих містах і в місцях скупчення великої кількості людей. WiMAX може забезпечити домашній або мобільний доступ до Інтернету в цілих містах або країнах. У багатьох випадках це призвело до конкуренції на ринках, які, як правило, мали доступ лише через існуючого діючого оператора DSL (або подібного). Крім того, враховуючи відносно низькі витрати, пов'язані з розгортанням мережі WiMAX (у порівнянні з 3G, xDSL, або FTTx), зараз економічно доцільно забезпечити широкосмуговий доступ до Інтернету останньої милі у віддалених місцях.

Загальні питання для розгляду.

1. Визначення вимог до каналу зв'язку з Інтернетом для вашої мережі:

   – оцінка необхідної пропускної здатності каналу зв'язку;

– призначення часу доступу в Інтернет;
– розміщення користувачів.

2. Вибір каналу для підключення до Інтернету:

– модемне з'єднання через телефонну лінію;
– PPPoE; DSL;
– VPN;
– мережі кабельного телебачення;
– xPON (оптоволоконний канал);
– FTTB;
– супутниковий інтернет;
– Wi-Fi;
– 3 G-UMTS/CDMA;
– 4G-WiMAX/LTE.

3.2.5. Вибір маршрутизатора та постачальника послуг Інтернету

Модуль служби маршрутизації та віддаленого доступу (RRAS) можна настроїти для маршрутизації трафіку між LAN і будь-яким WAN-каналом, підключеним до комп'ютера, на якому працює RRAS. Крім того, RRAS підтримує NAT і здатна забезпечити доступ в Інтернет комп'ютерам LAN із незареєстрованними IP-адресами. Перетворення мережевих адрес (Network address translation, NAT) реалізовано програмою, вбудованою в маршрутизатор.

Маршрутизатор може бути виконаний у вигляді окремого пристрою. Більшість маршрутизаторів з нижнього сегмента цінового діапазону – це комбіновані пристрої, які на додаток до стандартних функцій маршрутизації підтримують NAT і DHCP. Такі маршрутизатори, підключені безпосередньо до WAN, забезпечують загальний доступ в Інтернет через стандартний модем, ISDN, мереже КТБ або DSL. Оскільки загальний доступ надається з використанням NAT, мережа пов’язана з ISP через єдиний канал, отже, такі пристрої не підходять для великих мереж, а також мереж, де зареєстровані IP-адреси, які потрібні декільком комп’ютерам. Більшість WAN-технологій, вимагають також спеціального устаткування: для з'єднання через телефонну лінію – модему, для виділеної лінії – пристроїв CSU/DSU.

Вибір постачальника послуг Інтернету (Internet Service Provider, 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 WAN-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.

Загальні питання для розгляду.

1. Вибір типу маршрутизатора.

2. Вибір постачальника послуг Інтернету та визначення, які служби (Web, DNS, електронна пошта) будуть підтримуватися в мережі, а які буде отримано у постачальника послуг Інтернету.

3. Захист і керування доступом в Інтернет:

- визначення вимог до захисту доступу в Інтернет;
- вибір методу доступу до Інтернет (за допомогою маршрутизатора NAT або проксі-сервера).

3.2.6. З'єднання через маршрутизатори окремих віддалених ЛОМ підприємства

WAN-топологія – структура з'єднань між віддаленими сегментами або LAN підприємства. Вибирати WAN-топологію треба з урахуванням особливостей наміченої для використання WAN-технології. Обрану WAN-топологію можна реалізувати на основі постійних підключень або підключень за запитом.

Постійні підключення забезпечують постійну швидкість передачі даних, звичайно за фіксовану щомісячну плату. Підключення за запитом дозволяють оплачувати тільки ресурси каналу зв'язку, які реально використані.

Служби доступу через лінії, що підключенні з ретрансляцією кадрів і VPN дозволяють реалізувати мережі з топологією без попарного з'єднання вузлів виділеними WAN-каналами.

Статична маршрутизація вимагає створювати маршрути вручну, тому вона не підходить для великих мереж із інфраструктурою, яка часто змінюється.

Динамічна маршрутизація використовує протокол, що дозволяє маршрутизаторам автоматично адаптуватися до змін у мережі та обмінюватися повідомленнями з даними про мережі, у яких вони розміщені.

RIP – протокол маршрутизації оптимальний для мереж, всі ділянки яких працюють на однаковій швидкості. OSPF – протокол маршрутизації на основі стану каналу. Завдяки масштабованості він придатний для мереж практично будь-якого розміру, але вимагає більше ретельного планування, настроювання та підтримки, ніж RIP.

Загальні питання для розгляду.

1. Вибір WAN-топології (на основі постійних підключень і/або на основі підключень за запитом).

2. Вибір WAN-технології:

- виділені лінії;
- підключення за запитом;

– з'єднання з ретрансляцією кадрів;
– віртуальна приватна мережа.

3. Вибір маршрутизаторів.

4. Вибір протоколу маршрутизації.

3.2.7. Віддалений доступ до мережі

Для того, щоб сформулювати вимоги безпеки до сервера віддаленого доступу, визначите, які користувачі мають потребу у віддаленому доступі до мережі, який тип доступу їм потрібний, а також чи необхідно вводити різні рівні доступу. RRAS підтримує кілька протоколів перевірки дійсності: EAP, MS-CHAP (версій 1 і 2), CHAP, SPAP і PAP.

Політики віддаленого доступу є наборами умов, яким повинні задовольняти клієнти, які намагаються підключитися до сервера віддаленого доступу. Політики управляють віддаленим доступом залежно від членства користувачів у групах.

RRAS звіряє параметри всіх вхідних підключень зі списком політик віддаленого доступу, які створені на сервері, і дозволяє доступ тільки підключенням, що задовольняють всім умовам хоча б однієї з політик.

Профілі віддаленого доступу являють собою набори атрибутів, які RRAS застосовує до підключень, що пройшли аутентифікацію та авторизацію. Профілі дозволяють задавати час, коли підключення дозволене, установлювати типи дозволеного IP-трафику, а також обов'язкові до використання протоколи перевірки та алгоритми шифрування.

Невірне настроювання протоколу маршрутизації порушує обмін повідомленнями між маршрутизаторами мережі та веде до передачі пакетів невірними маршрутами.

Загальні питання для розгляду.

1. Визначення вимог до безпеки:

– визначення користувачів, яким потрібен віддалений доступ до мережі;
– визначення типу доступу для кожного користувача, якому він потрібен.

2. Керування доступом через властивості облікових записів.

3. Планування перевірки дійсності (аутентифікації).

4. Застосування політик віддаленого доступу.

3.2.8. Вибір операційної системи та обладнання

Сервери здатні виконувати в мережі організації безліч ролей: контролер домену, Web-сервер, сервер БД, поштовий сервер, сервер інфраструктури,

сервери файлів та друку, сервер резервного копіювання.

Конфігурація серверів зазвичай створюється розраховуючи на вимоги конкретного програмного середовища, а робочі станції проєктуються для вирішення широкого кола завдань.

Створюючи специфікацію устаткування сервера, варто передбачити можливість нарощування числа процесорів і пам'яті, а також об’єму дискової підсистеми.

Сімейство ОС Windows для робочих станцій включає дві лінії, засновані, відповідно, на технологіях DOS і Windows NT, для використання в мережах віддають перевагу останній.

У якості серверної ОС варто вибирати платформу, що максимально підходить для даної серверної ролі, пріоритетом при виборі ОС для робочих станцій є стандартизація. Для робочих станцій варто вибрати ОС, що підійде для максимально можливого числа користувачів.

Вибір ОС для серверів ширше, для кожного сервера він здійснюється відповідно до вимог програмного середовища, яке буде працювати на цьому сервері. Але більш бажаним для використання у WAN вважають сімейство Unix-подібних ОС.

Установка ОС у базовій конфігурації забезпечує мінімальний рівень безпеки, необхідний організації. Для комп'ютерів з особливими вимогами до захисту базову конфігурацію можна змінити шляхом настроювання її параметрів і установки додаткового захисного ПЗ і устаткування.

Загальні питання для розгляду.

1. Установка сервера (серверів) з необхідною роллю:
   - сервер резервного копіювання;
   - сервер баз даних;
   - контролер домену;
   - поштовий сервер;
   - сервер файлів та друку;
   - сервер інфраструктури;
   - Web-сервер.
2. Визначення вимог до обладнання серверів.
3. Визначення вимог до обладнання робочих станцій.
4. Вибір операційної системи:
   - для робочих станцій;
   - для серверів.

3.2.9. Забезпечення мережевої безпеки

Інформаційна система перебуває в стані захищеності, якщо забезпечені

її конфіденційність, доступність і цілісність. Безпека забезпечується технічними засобами – системами шифрування, аутентифікації, авторизації, аудиту, антивірусного захисту, мережевими екранами тощо, а також юридичними і морально-етичними нормами, просвітньою роботою та адміністративними заходами.

Існує два класи алгоритмів шифрування – симетричні (наприклад, DES) і асиметричні (наприклад, RSA). Дайджест – результат однобічної функції шифрування. Знання дайджесту не дозволяє й навіть не припускає відновлення вихідних даних. Дайджест використається для контролю цілісності й автентичності документа (цифровий підпис).

Аутентифікація користувача – процедура доказу того, що він є той, за кого себе видає. Це багаторазові та одноразові паролі, володіння якимось унікальним предметом (фізичним ключем, документом, сертифікатом), біохарактеристики (малюнок райдужної оболонки ока).

Авторизація – це 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.

Мережеві екрани діляться на: екрани з фільтрацією пакетів на основі IP-адрес; екрани сеансового рівня, здатні фільтрувати пакети з урахуванням контексту; найбільш інтелектуальні мережеві екрани прикладного рівня.

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 забезпечує захист трафіку між двома підключеннями у відкритій транспортній мережі, наприклад в Інтернеті. Захищений канал має на увазі виконання трьох основних функцій: взаємна аутентифікація абонентів при встановленні з'єднання; шифрування переданих повідомлень; підтвердження цілісності повідомлень. До числа найбільш популярних протоколів захищеного каналу відносять IPSec і SSL.

Більш масштабним засобом захисту трафіку, в порівнянні із захищеними каналами, є віртуальні приватні мережі (VPN). VPN на основі шифрування гарантують конфіденційність корпоративних даних при передачі через відкриту мережу, аутентифікацію взаємодіючих систем на обох кінцях VPN і тунелювання, що дозволяє передавати зашифровані пакети по відкритій публічній мережі.

VPN забезпечують той же рівень безпеки, що і виділені канали.

Конфіденційність (Privacy) – відсутність у третьої особи можливості скопіювати або переглянути дані, які передаються по мережі Інтернет. Аутентифікація (Authentication) – перевірка, чи дійсно відправник пакетів VPN – легітимний пристрій, а не той, що використовується зловмисником. Цілісність даних (Data integrity) – перевірка, чи не піддавався змінам пакет при передачі через Інтернет. Пересилання недостовірної інформації (Antireplay) – відсутність у третьої особи можливості копіювати пакети даних, відіслані легітимним відправником, а потім пересилати ці пакети, видаючи себе за легітимного відправника.

Для вирішення цих завдань двома пристроями створюється VPN (тунель VPN). Вони додають ще один заголовок до оригінального пакету. У заголовок включаються поля, які дозволяють VPN-пристроям виконувати функції безпеки. Пристрої відповідають за шифрування оригінальних пакетів IP. Інформація передається в зашифрованому вигляді. Прочитати дані, можна лише володіючи ключем до шифру. Управління доступом, автентифікація і шифрування – важливі елементи захищеного з'єднання.

IPSec VPN – класичний приклад VPN, побудованої за так званою накладеною моделлю (Overlay) – обладнання сервіс-провайдера не задіюється в процесі маршрутизації клієнтського трафіку, а його мережа надає лише «прозоре» з'єднання між майданчиками підприємства – модель дозволяє забезпечити високу безпеку мережі без додаткових засобів і витрат з боку оператора. IPSec – архітектура або набір концепцій, які використовуються для захисту мереж IP. Визначає методи ідентифікації при ініціалізації тунелю, методи шифрування для кінцевих точок тунелю і механізми обміну та управління ключами шифрування між ними. Недолік – протокол орієнтований на IP. При шифруванні в IPSec використовується декілька алгоритмів, фактично – математичні формули, які вибираються так, щоб одна використовувалася для шифрування даних, а інша – для розшифрування і щоб неавторизована особа не змогла дешифрувати пакет даних або текст. Є важлива вимога: навіть якщо вдалося дешифрувати пакет, це ніяк не повинно сприяти дешифруванню подальших пакетів даних.

Загальні питання для розгляду.

1. Вибір «технічного» методу (методів) забезпечення інформаційної безпеки (забезпечення конфіденційності, доступності, цілісності при передачі інформації):

- аутентифікація;
- авторизація;
- шифрування (симетричне, асиметричне, шифрування за допомогою однобічної функції);
- антивірусні засоби, мережевий екран (мережевий екран мережевого рівня, мережевий екран сеансового рівня, мережевий екран

прикладного рівня);

– проксі-сервер (проксі-сервер прикладного рівня, проксі- сервер рівня з'єднань);

– фільтруючий маршрутизатор;

– захищений канал, (захищений канал на базі протоколу S/MIME, захищений канал на базі протоколу SSL, захищений канал на базі протоколу PPTP, захищений канал на базі протоколу IPSec (у транспортному режимі, в тунельному режимі));

– віртуальна приватна мережа (віртуальна приватна мережа на основі розмежування трафіку, віртуальна приватна мережа на основі шифрування).

2. Вибір «нетехнічних» засобів захисту:

– у сфері законодавства;
– морально-етичні норми, просвітня робота;
– адміністративні заходи.

3. Вибір фізичних засобів захисту:

– замки;
– камери спостереження;
– охоронні системи.

4. Резервне копіювання даних:

– вибір устаткування для архівації;
– вибір програми для архівації;
– складання плану резервного копіювання:
  a) вибір даних, що архівуємо;
  b) типи архівації:
    – повна;
    – додаткова;
    – різницева (диференціальна);
    – планування архівації;
    – повна (щотижня) + додаткова або різницева (щодня).

3.2.10. Забезпечення мережевої безпеки в бездротових LAN

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 зловмисникові досить з'ясувати модель вашої бездротової точки доступу, щоб одержати до неї доступ, попередньо довідавшись стандартні SSID і пароль адміністратора.

Також треба змінити IP-адресу. 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.

Протоколи WPA (Wi-Fi Protected Access), WPA2 і WEP (Wired Equivalent Privacy) забезпечують захист і шифрування даних, переданих бездротовою точкою доступу та бездротовим клієнтом. Краще використовувати WPA2. Алгоритм WPA2 є модифікацією алгоритму WPA. WPA2 – найбільш захищений алгоритм шифрування даних, що робить його просто незамінним для організації роботи бездротової локальної мережі. WPA2 використовується при шифруванні за допомогою алгоритму AES з 128-бітним ключем.

Встановіть значення WPA3 Personal для кращого захисту. Встановіть значення WPA2/WPA3 Transitional для сумісності зі старими пристроями. Параметр безпеки визначає тип автентифікації та шифрування, що використовуються вашим маршрутизатором, а також рівень захисту приватності даних, що передаються мережею. Який би параметр ви не обрали, обов'язково встановіть надійний пароль для підключення до мережі.

WPA3 Personal – це найновіший, найбезпечніший протокол для пристроїв Wi-Fi. Він працює на всіх пристроях, які підтримують Wi-Fi 6 (802.11ax), та на деяких старих пристроях.

WPA2/WPA3 Transitional – це комбінований режим, який використовує WPA3 Personal з пристроями, що підтримують цей протокол, і дозволяє старішим пристроям використовувати замість нього тип шифрування WPA2 Personal (AES).

Ви можете вказати список MAC-адрес мережевих адаптерів комп'ютерів, які зможуть одержати доступ до вашої мережі. Потрібно відзначити, що фільтрація MAC-адрес не забезпечує надійного захисту, а служить просто додатковим бар'єром.

Іноді за допомогою відновлення прошивки вдається додати підтримку WPA. У новій версії прошивки можуть бути усунуті помилки, наявні в її поточній версії, а також додані нові методи шифрування. Інструкції з перепрошивання точки доступу та її нову версію можна скачати із сайту виробника.

На допомогу адміністраторові також приходять методи аутентифікації: WPA-PSK і WPA2-PSK. RADIUS-сервер буде корисний у досить великих мережах, де потрібно аутентифікувати не тільки бездротових, але й інших клієнтів мережі, – наприклад, клієнтів, які підключаються за VPN.

Деякі точки доступу дають можливість знизити потужність передачі, що дозволяє знизити й кількість як навмисних, так і випадкових, несанкціонованих підключень до точки доступу. Знизивши потужність передачі, можна домогтися того, що точка доступу буде доступна тільки в межах офісу вашої компанії.

Вимикайте точку доступу, коли ви не працюєте – так ви на 100% будете впевнені, що ніхто не проникне у вашу мережу.

Інтерфейси керування бездротовими мережами не повинні бути доступні по бездротовій мережі – все керування бездротовою мережею повинне здійснюватися тільки по внутрішній (кабельній) мережі. Також доступ до портів керування варто дозволити тільки одним-двом конкретним станціям.

Антивіруси та брандмауери ніхто не скасовував і у випадку з бездротовим зв'язком. Бажано встановити не один загальний брандмауер/ антивірус – на сервері, але й встановити клієнтські брандмауери та антивіруси для захисту кожного комп'ютера мережі окремо .

Загальні питання для розгляду.

1. Зміна параметрів за замовчуванням.
2. Відключення широкомовлення SSID.
3. Використання протоколу WPA2.
4. Фільтрація MAC-адрес.
5. Відновлення прошивки устаткування.
6. Використання аутентифікації.
7. Зниження потужності передачі.
8. Відключення точки доступу, коли ви не працюєте.
9. Захист портів керування.
10. Захист від зовнішніх загроз (брандмауер і антивірус на кожному комп'ютері мережі).

3.2.11. Призначення IP-адрес

У кожного комп'ютера мережі TCP/IP повинна бути унікальна IP-адреса. З метою безпеки, комп'ютери із зареєстрованими IP-адресами розміщують в окремій мережі. Будь-яку мережу можна розбити на частини, виділивши трохи бітів ідентифікатора хоста під ідентифікатор підмережі. Щоб розрахувати маску підмережі та IP-адреси, представте адреси у двійковому вигляді, збільшить їх та переведіть результат назад у десятковий вид.

Настроювати TCP/IP на клієнтських комп'ютерах можна вручну або автоматично за допомогою DHCP-серверів, що призначають комп'ютерам IP-адреси та інші параметри конфігурації.

Більшість неполадок DHCP, якщо тільки вони не викликані збоями устаткування, виникають через невірне настроювання DHCP- клієнтів, DHCP-серверів і агентів DHCP-ретрансляції.

Для приватних адрес із загального діапазону адрес 0.0.0.0-255.255.255.255 виділено та зарезервовано три діапазони:

10.0.0.0 – 10.255.255.255 (мережа класу A, маска 255.0.0.0, кількість припустимих адрес $2^{24} = 16\ 777\ 216$);

172.16.0.0 – 172.31.255.255 (16 мереж класу B, маска 255.240.0.0, кількість припустимих адрес $2^{20} = 1\ 048\ 576$);

192.168.0.0 – 192.168.255.255 (256 мереж класу C, маска 255.255.255.0, кількість припустимих адрес $2^{16} = 65\ 536$).

Адреси із цих трьох діапазонів не видаються для використання в глобальній мережі Інтернет). Область застосування – тільки локальні мережі. Може існувати скільки завгодно багато локальних мереж, у яких буде використовуватися той самий діапазон IP-адрес, наприклад, 192.168.0.0 – 192.168.255.255. Природно, що в цьому випадку комп'ютери з різних локальних мереж будуть мати однакову IP-адресу, що неприпустимо. Для запобігання такої ситуації локальні мережі робляться закритими – жоден з комп'ютерів такої мережі не має прямого доступу в глобальну мережу (Інтернет).

У квітні 2012 року IANA виділила блок 100.64.0.0/10 адрес IPv4 спеціально для використання в сценаріях NAT оператора. Цей адресний блок не слід використовувати в приватних мережах або в загальнодоступному Інтернеті. Пристрої, які оцінюють, чи є IPv4-адреса загальнодоступною, повинні бути оновлені, щоб розпізнати новий адресний простір.

Один з комп'ютерів такої локальної мережі робиться трохи відособленим – перетворюється в шлюз ("ворота"). Такий шлюз має дві мережеві карти – одна підключена до локальної мережі, інша ж – підключена безпосередньо до Інтернету (має прямий доступ). Мережевій карті, підключеній до локальної мережі, призначається одна з адрес приватного діапазону (найчастіше, це адреса 192.168.0.1). Мережевій карті, підключеній до Інтернет, призначається IP-адреса, яка надається для глобального використання. Така адреса унікальна і тільки один комп'ютер в Інтернеті (а точніше – мережева карта цього комп'ютера) може мати її.

IP-адреса орендується в організації, що займається видачею та контролем використання всіх IP-адрес Інтернету – повноважний комітет з нагляду за присвоєнням номерів Internet (IANA). Дублювання точно такої ж адреси іншим комп'ютером неприпустимо.

Для простоти запису маски, після IP-адреси самого пристрою використовують запис в скороченій формі у вигляді числа. Це число – кількість біт у масці, які дорівнюють 1. Наприклад, якщо IP-адреса 192.168.58.4, а маска 255.255.255.0:

192.168.58.4 = 11000000. 10101000. 00111010. 00000100

255.255.255.0 = 11111111. 11111111. 11111111. 00000000

кількість біт, що встановлені у значення "1" у масці, дорівнює 24,

то IP-адресу можна записати в такий спосіб: 192.168.58.4/24.

Перетворення мережевих адрес (Network address translation, NAT) реалізовано програмою, вбудованою в маршрутизатор. Ця програма відіграє роль посередника між приватною мережею та Інтернет-серверами із зареєстрованими адресами. Навіть клієнтські комп'ютери із незареєстрованними адресами можуть відправляти запити серверам Інтернету та одержувати від них відповідь за допомогою NAT. Звичайні маршрутизатори змінюють дейтаграми не частіше, ніж працівники пошти звичайні конверти. На відміну від них маршрутизатор NAT замінює вміст поля з адресою відправника у всіх дейтаграмах, отриманих від комп'ютерів з незареєстрованою IP-адресою. Маршрутизатор NAT також підтримує таблицю незареєстрованних адрес приватної мережі – вона необхідна для відстеження оброблених їм дейтаграм.

Маршрутизатори, що працюють за протоколом IPv6, не виконують фрагментацію, як в IPv4, зменшуючи службову інформацію в заголовку IP-пакету. Замість фрагментації вони визначають MTU (maximum transmission unit, доступний максимальний розмір пакета) для кінцевого вузла в рамках конкретної сесії.

На початку передачі IPv6-пристрій відправляє пакет розміром, який вказаний одним з верхніх рівнів (транспортним або прикладним). При отриманні у відповідь ICMP-повідомлення "пакет занадто великий", виконується відправка пакету MTU-discover меншого розміру до тих пір, поки розмір не буде задовольняти всі проміжні пристрої – нове MTU встановлюється для всієї сесії. У ICMP-повідомленні "пакет занадто великий" може міститися пропонований розмір MTU. Для кожної сесії визначається своє значення MTU.

Структура IPv6-адрес описана в RFC3513 і RFC4291. Описують 3 типи адрес.

Unicast-адреси – призначені для ідентифікації конкретного пристрою в мережі. Пакет відправлений на Unicast-адресу доставляється на ідентифікований за допомогою адреси інтерфейс. Існує 2 типу Unicast адрес:

– Link-local unicast address (локальна Unicast-адреса) – може використовуватися тільки в рамках локальної мережі (аналог автономних адрес IPv4);

– Global unicast address (глобальна Unicast-адреса) – може використовуватися в мережах будь-якого розміру (аналог реальних адрес IPv4).

Кожен інтерфейс повинен мати мінімум одну локальну Unicast-адресу. Однак інтерфейс може мати одночасно декілька адрес всіх трьох типів.

Multicast-адреси – в IPv6 не використовуються широкомовні адреси, замість них застосовуються Multicast-адреси. Вони дозволяють відправляти пакети з даними одночасно кільком мережним інтерфейсам. Для цього

використовуються Multicast-групи, що дозволяють відправляти дані обмеженій групі вузлів. Кількість Multicast-адрес IPv6 значно перевищує кількість Multicast-адрес IPv4.

Anycast-адреси – anycast-адреса може посилатися одночасно на декілька інтерфейсів одного вузла. Пакет відправлений на Anycast-адресу буде доставлений на найближчий інтерфейс вузла, визначений за допомогою протоколу маршрутизації. Anycast-адреса не може використовуватися в якості адреси відправника.

У протоколі IPv6 зарезервовано декілька спеціальних IP-адрес:

:: / 128 – може використовуватися тільки при розробці програмного забезпечення;

:: 1/128 – локальна адреса кільцевого інтерфейсу. Використовується для звернення до самого себе (аналог 127.0.0.1 в IPv4);

2001: db8 :: / 32 – скрізь, де наводяться приклади IPv6-адрес, слід використовувати адреси цього діапазону;

fe80 :: /10 – локальний префікс, вказує, що адреса є дійсною тільки всередині місцевої фізичної мережі. Це аналог IP-адреси 169.254.0.0/16 в IPv4;

ff00 :: / 8 – багатоадресний префікс використовується для Multicast-розсилки.

Загальні питання для розгляду.

1. Загальні (зареєстровані) IPv4-адреси, їх призначення.

2. Приватні (незареєстровані) IPv4-адреси, їх призначення: три діапазони адрес для використання в приватних мережах:

10.0.0.0/8 – 10.255.255.255/8;

172.16.0.0/16 – 172.31.255.255/12;

192.168.0.0/16 – 192.168.255.255/16.

3. Доступ в Інтернет з приватної мережі: підключення до Інтернету через маршрутизатор NAT, підключення до Інтернету через проксі-сервер, вибір варіанта доступу.

4. Обчислення IPv4-адрес для комп'ютерів.

5. Вибір способу налаштування TCP/IP на клієнтських комп'ютерах: вручну, за допомогою сервера DHCP, вибір варіанта налаштування.

6. Вибір типу адресації IPv6. Використання Anycast-адрес.

3.3. Вимоги до змісту розділів, оформлення та обсягу пояснювальної записки

До пояснювальної записки (далі – ПЗ) необхідно включати матеріал, який безпосередньо відноситься до конкретної комп’ютерної мережі, що

підлягає проєктуванню, у відповідності до технічного завдання. Не рекомендується робити великі реферативні огляди. При необхідності можна робити посилання на відповідну літературу. Основний зміст ПЗ – це обґрунтування прийнятих рішень та проєкт об’єднаної мережі, згідно затвердженої назви. При цьому треба мати на увазі, що ПЗ складають тоді, коли розробку проєкту завершено, всі рішення прийнято, всі деталі є відомими, є кінцевий результат, і саме його необхідно привести у записці разом з аргументацією вибору рішень, необхідними розрахунками, таблицями, рисунками, діаграмами, іншими матеріалами, які обґрунтовують прийняті рішення.

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

У рефераті студент вказує мету, задачі, технології, вид обладнання, протоколи та стандарти, які використані у розробленому проєкті. Наводить ключові слова та об’єм ПЗ. Реферат рекомендовано оформити на заключному етапі (1 сторінка).

У вступі студент повинен висвітлити загальний стан питання, яке розглядається, обґрунтовувати необхідність і можливість його вирішення, описати зв'язок з виробничими задачами, а також обґрунтувати актуальність теми проєкту. Вступ має бути коротким (1-2 сторінки) і чітким. Його не слід перевантажувати загальними фразами. Головне, щоб було зрозуміло, чому присвячена робота, які завдання автор поставив сам для себе.

У першому розділі (5-7 сторінок) ПЗ необхідно провести аналіз технічного завдання, розглянути структуру підприємства в цілому, визначити яке обладнання потребує заміни, а яке необхідно придбати додатково для підключення віддалених сегментів об’єднаної мережі. Студент повинен 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 (5-8 сторінок) на підставі проведеного аналізу розробляються функціональна 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 50 одиниць.

Третій розділ (5-8 сторінок) повинен містити опис апаратної та кабельної частини проєкту з урахуванням попереднього вибору та можливості з'єднання через маршрутизатори окремих LAN підприємства, з метою здійснення віддаленого доступу. Цей розділ містить вибір конкретних елементів реалізації функціональної та структурної схем, розрахунок окремих елементів, вузлів та підсистем. Розробляється детальна монтажна схема мережі.

У четвертому розділі (4-7 сторінок) розкриваються питання вибору операційних систем робочих станцій та серверів, які в подальшому підтримають функціонування загальних сегментів мережі та об’єднаної мережі в цілому.

У п’ятому розділі (4-6 сторінок) розглядається підключення розробленої мережі підприємства до Internet.

Питання забезпечення мережевої безпеки, як у дротових так і в бездротових LAN треба розглянути в наступному розділі (4-7 сторінок) пояснювальної записки. Студентом розкриваються питання забезпечення якості та надійності розробленої мережі, питання апаратного та програмного захисту інформації, а також захист від несанкціонованого доступу.

У сьомому (3-5 сторінок) розділі розглядається призначення IP-адрес та подання мережі головного офісу організації (підприємства) в Інтернеті.

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

Оформлення ПЗ здійснюється у відповідності до діючих стандартів ДСТУ 3008-2015 “Документація. Звіти в сфері науки і техніки”. Бібліографічні описи в переліку посилань наводять відповідно до чинних стандартів з бібліотечної та видавничої справи відповідно ДСТУ ТОСТ 7.1:2006 "Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання".

До ПЗ додаються структурна, монтажна та функціональна схеми мережі, виконані на аркушах необхідного для зручного читання формату формату. Монтажна схема повинна відображати проходження кабелів на всіх ділянках мережі з роз’ясненням особливостей їх прокладання.

Загальний обсяг ПЗ – не менше 40 сторінок (не рекомендовано обсяг більший за 50 стор.), причому технічна її частина, має містити не менш ніж 30 сторінок тексту з рисунками. Рисунки можуть містити необхідні для пояснень і розрахунків фрагменти загального креслення мережі.

3.4. Порядок захисту курсового проєкту

Призначення захисту – оцінити складність розробленого проєкту, кваліфікацію студента і ступінь самостійності його праці.

Захист відбувається за графіком у присутності комісії з двох викладачів, один з яких є керівником курсового проєкту. На доповідь дається 8-10 хвилин. За цей час необхідно стисло викласти зміст поставленої задачі (одна хвилина), доповісти про власну роботу щодо розробки комп’ютерної мережі підприємства (6-8 хвилин) і зробити висновки (одна хвилина).

Необхідно розповідати про свою власну роботу, пояснювати, чому прийнято саме такі рішення при проєктуванні мережі, на основі яких міркувань було обрано те або інше апаратне та програмне забезпечення,

сформовано ті або інші LAN 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.

4. ВИМОГИ ДО ОФОРМЛЕННЯ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт виконують за допомогою комп'ютера на одній стороні аркуша білого паперу формату А4 (297х210 мм), 14-го розміру шрифту з інтервалом 1,5 із кількістю абзаців на сторінці не більше 5. Перед текстом курсового проєкту розмішують титульний лист (додаток А) та відгук (додаток В), підписані науковим керівником.

Необхідно дотримуватись таких розмірів полів: зліва – 30 мм для підшивки і зауважень, справа – 10 мм, знизу і зверху – 20 мм. Абзацний відступ повинен бути однаковим впродовж усього тексту роботи і дорівнювати 1,25 см.

Помилки, описки та графічні неточності допускається виправляти підчищенням або зафарбовуванням білою фарбою і нанесенням на тому ж місці або між рядками виправленого зображення від руки. Виправлене повинно бути чорного кольору.

Скорочення слів і словосполучень у курсовому проєкті має здійснюватись відповідно до чинних стандартів з бібліотечної та видавничої справи.

Заголовки розділів друкують великими літерами по центру. Заголовки підрозділів друкують маленькими буквами (крім першої великої) з абзацного відступу. Крапку наприкінці заголовка не ставлять.

Наприклад:

ВСТУП

або

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННН

1.1 Планування структури кожної ЛОМ об’єднаної мережі

Перенесення слів у заголовку розділу не допускається. Кожний розділ починається з нової сторінки. Текст підрозділів пишеться в межах одного розділу без розриву.

Відстань між заголовком розділу і підрозділу – 1 рядок, між заголовком підрозділу і текстом ПЗ – 1 рядок.

Не допускається розміщення назви розділу, параграфу в нижній частині

сторінки, якщо після неї розміщено тільки один рядок тексту.

Сторінки нумеруються арабськими цифрами. На титульному листі номер не ставиться, на наступних сторінках – у правому верхньому кутку без крапки (наскрізна нумерація з додатками).

Протягом всього тексту повинна бути одноманітність термінів, позначень, умовних скорочень та символів. Терміни повинні відповідати діючим стандартам.

У змісті (додаток В) вказують номери сторінок, з яких починаються розділи, підрозділи.

Всі наведені цитати, цифрові дані та іншу інформацію, запозичену з літературних джерел, необхідно чітко виділяти із посиланням на джерело (порядковий номер за списком використаних джерел), із зазначенням сторінки у квадратних дужках. Наприклад: [25, с.77]; [15, с.183].

При наявності у тексті переліку складових частин, фактів тощо, їх слід нумерувати порядковою нумерацією арабськими цифрами із дужкою, наприклад: 1), 2), і друкувати малими літерами із абзацного відступу.

4.1. Оформлення таблиць

Таблицю слід розміщувати одразу після тексту, в якому вона згадується вперше, або на наступній сторінці. На всі таблиці повинні бути посилання в тексті: "див. табл. 2.1". Кожна таблиця повинна мати назву, яку потрібно писати малими літерами (крім першої прописної). Назва розміщується над таблицею, є стислою і відображає зміст таблиці.

Таблиці нумеруються послідовно арабськими цифрами в межах кожного розділу (номер таблиці включає номер розділу і порядковий номер таблиці). При переносі частини таблиці на наступний аркуш зазначають: "Продовження табл. 2.1".

Заголовки граф починають з великих літер, а підзаголовки - із строчних, якщо вони складають одне речення із заголовком. Для скорочення тексту заголовків і підрозділів граф окремі поняття допускається заміняти літерними позначеннями, якщо вони пояснені в тексті, або приведені на малюнках.

Якщо цифрові дані в графах таблиці виражені в різних одиницях виміру, то їх указують в заголовках кожної графи. Якщо всі показники розміщені в таблиці, виражені в одній і тій же одиниці виміру, скорочене визначення одиниці виміру розміщають над таблицею в заголовку.

Графу "Номер з/п" у таблицю включати не слід, за винятком випадків, коли на ці номери є посилання.

Якщо текст, що повторюється в графі таблиці складає одне слово, то замість нього ставлять лапки, якщо із двох і більше слів то при першому повторі пишуть “те ж”, а потім ставлять лапки. Ставити лапки замість цифр,

знаків, математичних символів, які повторюються, не допускається. Якщо цифрові, або інші дані в таблиці не приводяться, замість них ставлять прочерк.

4.2. Оформлення формул

Формули та рівняння розміщуються безпосередньо за текстом, в якому вони згадуються по середині рядка. До і після кожної формули чи рівняння.залишається один вільний рядок.

Наведені в курсовому проєкті формули нумерують, при наявності на них посилань (наприклад: “див. формулу 1.1”), подвійною нумерацією арабськими цифрами в межах кожного розділу. Номери вказують з правої сторони аркуша на рівні формули в круглих дужках, наприклад (1.1) – перший розділ, перша формула. Пояснення значень символів і числових коефіцієнтів слід наводити під формулою у тій самій послідовності, в якій вони дані у формулі. Значення кожного символу і числового коефіцієнта треба подавати з нового рядка. Перед поясненням першого символу пишуть з абзацу слово "де" без двокрапки.

Наприклад:

$$E = т*с^2 \qquad (1.1)$$

де, Е – Енергія;
т – маса;
с – швидкість світла.

4.3. Оформлення рисунків

Ілюстрації (малюнки, графіки, схеми, діаграми) позначають словом "Рисунок". Ілюстрації необхідно розмішувати в роботі безпосередньо після тексту, де вони відзначаються вперше або, якщо не дозволяють їх розміри, на наступній сторінці.

При необхідності під ілюстрацією розміщують пояснювальні дані (підрисунковий текст). Ілюстрації повинні мати назву, яку розташовують під ілюстрацією після пояснювальних даних разом з номером ілюстрації. Нумерація ілюстрацій проводиться арабськими цифрами в межах розділу, наприклад: Рисунок 1.2 (другий рисунок першого розділу).

4.4. Оформлення додатків

Кожний додаток починається з нового аркуша і повинен мати заголовок, який відображає зміст додатку. З абзацу пишуть слово "Додаток". Додатки мають наскрізну одинарну нумерацію (в межах усієї роботи) великими літерами українського алфавіту, наприклад: "Додаток А". На додатки у тексті обов'язково слід робити посилання.

4.5. Оформлення посилань у тексті

Посилання в тексті роботи на літературні джерела необхідно позначати в кінці речення порядковим номером за переліком посилань, виділеними двома квадратними дужками, наприклад, «... у роботах [1-7] ...». При посиланні на рисунки, таблиці, формули, вказують їх порядковий номер, наприклад: на рисунку 2.1; дивись рисунок 2.1; у таблиці 2.1; за формулою (2.1); у формулі (2.1).

5. КРИТЕРІЇ ОЦІНКИ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт подається на кафедру для перевірки науковим керівником не пізніше ніж за тиждень до екзаменаційної сесії. Курсовий проєкт, який відповідає викладеним у методичних рекомендаціях вимогам, оцінюється для студентів за стобальною шкалою з врахуванням наступних критеріїв:

Таблиця 5.1 – Критерії оцінки курсового проєкту

Критерії	Бали
Оцінка структури проєкту (повнота розкриття теми у змісті)	60 балів
Оцінка теоретичного рівня проєкту	
Повнота аналізу технічного завдання	
Правильність вибору обладнання	
Характеристика аналітичного рівня проєкту	
Ілюстративність проєкту: наявність таблиць, рисунків	
Відповідність вступу та висновків вимогам, які викладено в методичних вказівках по написанню курсового проєкту	
Оцінка повноти та правильність складання переліку посилань	
Відповідність оформлення проєкту вимогам стандартів та правил	
Виконання календарного плану написання проєкту	
Оцінка доповіді студента при захисті проєкту	40 балів
Оцінка відповіді студента на додаткові запитання	
Всього	100

Проєкт може бути оцінений на "**відмінно**" в тому разі, якщо в ньому розкрита сутність проблеми дослідження, її актуальність, приведений огляд монографічної і періодичної літератури, статистичні матеріали. ПЗ містить аналіз проблеми, розрахунки та обґрунтування рішень щодо вдосконалення методів вирішення проблеми, заявленої в рамках обраної теми. Виконані вимоги щодо оформлення ПЗ.

Оцінка "**добре**" виставляється у разі, якщо в ПЗ недостатньо обґрунтовані пропозиції автора щодо вдосконалення ефективності діяльності об’єкту дослідження, інші вимоги, які були перелічені в попередньому пункті

виконані.

Оцінка "**задовільно**" виставляється у разі, якщо проєкт поверхово висвітлює зміст теми дослідження, не містить обґрунтованих рекомендацій по вирішенню проблем дослідження. Мають місце помилки в оформленні ПЗ.

Проєкт оцінюється на "**незадовільно**" та повертається на доопрацювання, якщо автор не розкрив зміст теми, не залучив практичний матеріал до аналізу проблеми дослідження та допустив помилки при викладенні змісту питань та оформленні ПЗ.

6. ОРГАНІЗАЦІЯ ЗАХИСТУ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт подається на кафедру для перевірки науковим керівником не пізніше ніж за тиждень до екзаменаційної сесії. Якщо проєкт виконаний і оформлений правильно, то науковий керівник пише відгук (зразок бланку подано у Додатку Б) і допускає курсовий проєкт до захисту.

Курсовий проєкт до захисту не допускається, якщо він:

поданий науковому керівникові на перевірку з порушенням строків, установлених календарним планом;

написаний на тему, яка своєчасно не була затверджена по кафедрі;

виконаний не самостійно;

не реалізовані запити, інструменти керування або інший елемент структури курсового проєкту;

побудова структури не відповідає вимогам.

Заключним етапом є захист курсового проєкту. Він проводиться у строки, визначені деканатом. Курсові проєкти захищають перед комісією, призначеною кафедрою. Студент за результатами дослідження готує роздатковий матеріал для членів комісії та презентацію в програмі PowerPoint (за бажанням) . Студенту надається слово для викладання змісту дослідження (до 10 хвилин).

Під час захисту курсового проєкту студент має виявити глибокі знання з вивчених розділів курсу, вміти розкрити зміст розглянутих у курсовому проєкті положень і відповісти на поставлені членами комісії запитання. За результатами захисту комісія може уточнити попередню оцінку курсового проєкту, що її запропонував рецензент.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Коробейнікова, Захарченко. Комп’ютерні мережі : навч. посіб. Львів. політехніка, 2022. 228 с.
2. Хомуляк М.О. Адміністрування комп'ютерних систем і мереж : навч. посіб. Магнолія, 2023. 154 с.
3. Микитишин А.Г., Митник М.М. , Стухляк П.Д. Комп’ютерні мережі, книга.1. Навчальний посібник для технічних спеціальностей ВНЗ (рекомендовано МОН України). Магнолія, 2021. 256 с.
4. Микитишин А.Г., Митник М.М. , Стухляк П.Д. Комп’ютерні мережі: навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.
5. Комп’ютерні мережі : навчальний посібник [Електронне видання] / О. В. Задерейко, Н. І. Логінова, А. А. Толокнов. – Одеса : Фенікс, 2022. – 249 с. – URL: http://dspace.onua.edu.ua/handle/11300/19423

ДОДАТКИ

Додаток А - Зразок титульного листа курсового проєкту

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

Прізвище, ім’я та по-батькові студента

КУРСОВИЙ ПРОЄКТ

з дисципліни**: "Комп’ютерні мережі"**

на **тему : "_____"**

Курс __ Група_____

Науковий керівник:

Проєкт поданий на кафедру	Проєкт допущений до захисту _____Науковий керівник	Проєкт захищений з **оцінкою** _____
"__"_____202__р.	"__"_____202__р.	"__"_____202__р.

Чернігів – 2023

Додаток Б – Приклад реферату до пояснювальної записки

РЕФЕРАТ

ПЗ: 50 с., 10 рис., 12 табл.

Об'єкт розробки – розподілена комп'ютерна мережа підприємства "ЧеЗаРа".

Мета роботи – створення розподіленої комп'ютерної мережі підприємства "ЧеЗаРа" для забезпечення працездатності основних баз даних.

Використання сучасних інформаційних технологій, єдиний підхід до формування розподіленої комп'ютерної мережі, оснащення підприємства швидкими каналами зв'язку, дозволить повною мірою забезпечити розвиток галузі. Основним завданням побудови єдиної комп'ютерної мережі, є підключення розрізнених елементів підприємства в єдину мережу, з підтримкою різних технологій доступу до серверів, враховуючи важкодоступність філій. Таке рішення є кращим в нашому випадку, коли прокладка кабелів в землі ускладнена і мережі створюються у важкодоступних районах. Важливою особливістю радіорелейних систем останнього покоління є їх масштабованість, тобто можливість збільшення їх пропускної спроможності у міру зростання трафіку без заміни радіорелейного обладнання.

Магістральні буде мережа, побудована із застосуванням радіорелейного зв'язку з обладнанням Ericsson Mini-Link, а всередині офісів і філій планується застосування бездротових і дротових технологій з обладнанням D-Link. Тому створювана система може бути легко розширена і модифікована.

РАДІОРЕЛЕЙНІ ЛІНІЇ, СЕРВЕР, БЕЗДРОТОВІ ТЕХНОЛОГІЇ, КОМУТАТОР, МАРШРУТИЗАТОР, ОПЕРАЦІЙНА СИСТЕМА, МЕРЕЖА.

Додаток В - Приклад відгуку на проєкт

ВІДГУК
НА КУРСОВИЙ ПРОЄКТ

предметна область "_____"

студента _____

_____курсу, групи_____, спеціальності _____

Курсовий проєкт з дисципліни "_____"

Реєстраційний №____ дата отримання "___"_____202__р.

Науковий керівник_____

Основна характеристика курсового проєкту:

Мета дослідження: досягнута повністю (частково, не досягнута) Завдання дослідження :виконані повністю (частково, не виконані)

Структура роботи: витримується згідно вимогам (частково відповідає вимогам, не відповідає вимогам)

Характер зовнішнього оформлення роботи: охайний (задовільний, неохайний)

Зауваження:

Недоліки:

Загалом проєкт заслуговує позитивної оцінки та може бути допущений до захисту

Науковий керівник_____ (підпис)

За результатами захисту проект оцінений_____

Члени комісії _____

_____