МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається

Завідувач кафедри

_____ Скарга-Бандурова І.С.

«____»_____ 2018 р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

«МЕТОДИ ПОШУКУ НЕСПРАВНОСТЕЙ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ»

Освітньо-кваліфікаційний рівень «Магістр»

Спеціальність 123 «Комп'ютерна інженерія» (освітня програма «Комп'ютерні системи і мережі»)

Науковий керівник роботи: _____ Кардашук В. С.
(підпис) (ініціали, прізвище)

Консультант з охорони праці: _____ Критська Я.О.
(підпис) (ініціали, прізвище)

Студент: _____ Оридорога А. О.
(підпис) (ініціали, прізвище)

Група: КСМ-16 зм

Сєвєродонецьк - 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет інформаційних технологій та електроніки

Кафедра комп'ютерної інженерії

Освітньо-кваліфікаційний рівень магістр

Спеціальність 123 «Комп'ютерна інженерія» (освітня програма «Комп'ютерні системи і мережі»)

«ЗАТВЕРДЖУЮ»
Завідувач кафедри
комп'ютерних наук та інженерії
д.т.н., доц., Скарга-Бандурова І. С.
_____
"____" _____ 2018 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Оридорозі Аліні Олександрівні
(прізвище, ім'я, по-батькові)

1. **Тема проекту (роботи):** «Методи пошуку несправностей в комп'ютерних системах та мережах» затверджена наказом по університету № 208/48 від «18» жовтня 2017 р.

2. Строк здачі студентом закінченого проекту (роботи): 10.01.2018 р.

3. Вихідні дані проекту (роботи): матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити):

1. Огляд теоретичної літератури 2. Дослідження методів пошуку несправностей в комп'ютерних системах та мережах 3. Розробка програмного забезпечення 4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точною назвою обов'язкових креслень):

не передбачено

6. Консультанти роботи, з вказівкою розділів, що до них відносяться

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основна частина	Кардашук В. С.		
Охорона праці та безпека в надзвичайних ситуаціях	Критська Я.О.		

7. Дата видачі завдання _____

Керівник _____ Кардашук В. С.

(підпис)

Завдання до виконання прийняв _____ Оридорога А. О.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітки
1.	Отримання завдання, збір матеріалів	18.10.17- 24.10.17	
2.	Огляд літератури й обґрунтування необхідності дослідження	25.10.17 –28.10.17	
3.	Дослідження методів пошуку несправностей	29.10.17 – 28.11.17	
4.	Розробка програмного забезпечення	28.11.17 –05.12.17	
5.	Розробка заходів з охороні праці	05.12.17 – 19.12.17	
6.	Оформлення пояснювальної записки	19.12.17 – 08.01.18	
7.	Підготовка та подання магістерської роботи до захисту	09.01.18 – 19.01.18	

Студент _____

(підпис)

Науковий керівник _____

(підпис)

АНОТАЦІЯ

Оридорога А. О. Методи пошуку несправностей в комп’ютерних системах та мережах.

Виконано дослідження методів пошуку несправностей в комп’ютерних системах та мережах. Розглянуті основні засобів моніторингу й аналізу мережі, фізичні основи діагностики мереж. Запропоновано алгоритм пошуку дефектів в локальній обчислювальній мережі, що базується на представленні об'єкта діагностування як моделі з ранжируваним графом та представленням мережевого сегмента у вигляді матриці досяжності. Проведена модифікація структурного методу пошуку дефектів стосовно локальної мережі.

Ключові слова: система, мережа, несправність, алгоритм, граф, таблиця несправностей.

THE ABSTRACT

Orydoroga A.O. Methods of troubleshooting of computer systems and networks.

The study of troubleshooting methods in computer systems and networks has been performed. The main means of monitoring and analysis of the network, physical bases of diagnostics of networks are considered. The algorithm for finding defects in a local computer network based on the representation of the object of diagnostics as a model with a ranked graph and representation of the network segment in the form of the matrix of reach is proposed. A modification of the structural method for defect detection in relation to the local network has been made.

Keywords: system, network, malfunction, algorithm, graph, fault table.

ЗМІСТ

ВСТУП

Інтенсивне поширення сфер використання мережної інфраструктури призводить до зростання вимог щодо надійності, відмовостійкості і продуктивності локальних обчислювальних мереж. Висока продуктивність мережі забезпечується, у першу чергу, відсутністю дефектів і вузьких місць, що призводять як до уповільнення швидкості роботи мережі, так і до недосяжності або до виходу з ладу комунікаційних компонентів. У разі виникнення зазначених проблем, істотним є час, який затрачується на їх пошук і відновлення працездатності мережної системи. На цей час вирішення задач діагностування локальних обчислювальних мереж, до яких відноситься наукова задача пошуку мережних несправностей, являє собою досить складну проблему. Це пов'язано, по-перше, з тим, що мережні несправності поділяються на різні типи, для пошуку кожного з яких необхідно використовувати різноманітні види діагностичного обладнання, а також застосовувати різноманітні методи, алгоритми і методики. Більш того, пошук та усунення несправностей програмного забезпечення не входить до задачі діагностування локальних обчислювальних мереж, і звідси виникає додаткова проблема відокремлення несправностей прикладного програмного забезпечення від несправностей мережі. По-друге, пошук навіть однотипних несправностей ускладнюється відсутністю єдиного формалізованого алгоритму дій адміністратора-діагноста, що підтверджується наявністю різноманітних способів представлення локальних обчислювальних мереж як об'єкта діагностування, кожний з яких має свої переваги і недоліки, але не є єдиним. Відсутність формалізованого методу визначення області підозрюваних несправностей також призводить до високих часових витрат на проведення діагностичного експерименту і, отже, пошук несправності. Також, на цей час відсутня єдина формалізована методика, що дозволяє виявити будь-який із видів несправностей. Це призводить до необхідності наявності у діагноста досить високого рівня досвіду і знань у галузі мережних технологій з метою забезпечення коректності постановки діагностичного експерименту і, як наслідок, поставленого діагнозу. Зазначені проблеми обумовлюють великі часові витрати на пошук несправності, а також звужують діапазон суб'єктів, що забезпечують коректне рішення задачі пошуку несправності, що призводить до високої трудомісткості і складності рішення вказаної задачі.

Таким чином, актуальною науково-технічною задачею є розробка методів пошуку несправностей в локальних обчислювальних мережах та їх сегментах, що забезпечать зниження трудомісткості, скорочення часових витрат на пошук несправності в локальних

обчислювальних мережах і підвищення ефективності процедури постановки діагнозу за рахунок забезпечення відповідної глибини пошуку несправності.

Значний вклад в розробку методів пошуку несправностей в локальних обчислювальних мережах внесли такі вчені як К.Гі, М.Като, Д.Їмура, Д.Мартін, Д.Чалліс, Д.Несер, Л.Чапел, Дж. Хогдал, С. Юдицький, В. Борисенко, П. Адаскін, І. Іванцов та ін.

Об'єкт дослідження – процеси діагностування комп'ютерних систем та локальних обчислювальних мереж

Предмет дослідження – методи і засоби зниження трудомісткості, скорочення часових витрат і підвищення ефективності процедури пошуку несправностей у локальних обчислювальних мережах.

Методи дослідження. Для методу пошуку явних адресованих несправностей і методів визначення області підозрюваних несправностей явного і прихованого виду використовується апарат теорії графів, теорії множин і технічної діагностики цифрових пристроїв. Для методів пошуку явних і прихованих несправностей у локальних обчислювальних мережах і методу відокремлення несправностей прикладного програмного забезпечення від мережних несправностей використовується апарат теорії планування пасивного й активного експерименту та інші розділи математичної статистики.

Наукова новизна магістерської роботи полягає в дослідженні методів побудови тестів в системах діагностики комп'ютерних систем та мереж. На основі дослідження вироблені рекомендації щодо подальшого використання досліджених методів.

Структура і обсяг роботи.

Магістерська робота складається зі вступу, 4 розділів, висновків, переліку посилань з 43 найменувань на 3 сторінках. Загальний обсяг роботи складає 86 сторінок. Магістерська робота містить 47 рисунків, 8 таблиць.

РОЗДІЛ 1
ДІАГНОСТИКА ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

1.1 Діагностика локальної мережі

За час, що минув з моменту появи перших локальних мереж, було розроблено десятки різних мережевих технологій, однак значного розповсюдження набули не всі. Це пов'язано, перш за все, з високим рівнем стандартизації принципів організації мереж і з підтримкою їх відомими компаніями. Тим не менш, не завжди стандартні мережі мають рекордними характеристиками, забезпечують найбільш оптимальні режими обміну. Але великі обсяги випуску їх апаратури і, отже, її невисока вартість дають їм величезні переваги. Важливо й те, що виробники програмних засобів також в першу чергу орієнтуються на найпоширеніші мережі. Тому користувач, що вибирає стандартні мережі, має повну гарантію сумісності апаратури і програм.

В даний час зменшення кількості типів використовуваних мереж стало тенденцією. Справа в тому, що збільшення швидкості передачі в локальних мережах до 100 і навіть до 1000 Мбіт / с вимагає застосування самих передових технологій, проведення дорогих наукових досліджень. Природно, це можуть дозволити собі тільки найбільші фірми, які підтримують свої стандартні мережі і їх більш досконалі різновиди. До того ж більшість споживачів вже встановило у себе якісь мережі і не бажає відразу і повністю замінювати мережеве обладнання, В найближчому майбутньому навряд чи варто очікувати того, що будуть прийняті принципово нові стандарти.

Діагностика локальної мережі – це комплекс заходів, який включає в себе кілька видів тестування:

– тестування кабельного господарства;

– виявлення прихованих дефектів обладнання і системного ПО;

– оцінка якості архітектурного рішення мережі, тобто визначення її пропускної здатності і вузьких місць, ступеня збалансованості її різних компонентів по навантаженню і т. п.

Часто під діагностикою мережі розуміється тільки тестування кабельного господарства: вимір фізичних характеристик ліній зв'язку. Це не вірно. Тестування кабельного господарства є безумовно важливою складовою діагностики, але аж ніяк не єдиною і не найскладнішою. Є багато спеціальних приладів: кабельних аналізаторів або кабельних сканерів, які сильно спрощують її рішення.

Значно більш тривалим і трудомістким є процес виявлення прихованих дефектів обладнання і ПЗ, а також оцінка якості архітектурного рішення мережі.

Приховані дефекти – це такі дефекти, які проявляються нерегулярно. Вони мають особливість проявлятися в самі невідповідні моменти. Поки мережа невелика, приховані дефекти виявляються рідко і на них не звертають особливої уваги. При розширенні мережі та збільшенні її завантаженості ймовірність прояву прихованих дефектів зростає.

Існують два основні підходи до виявлення прихованих дефектів і оцінці якості архітектури локальної мережі: пасивна діагностика і стресове тестування.

Метод пасивної діагностики полягає в постійному (у всякому разі, тривалому) спостереженні за станом мережі та реєстрації змін в її поведінці. Він заснований на використанні спеціальних засобів пасивного спостереження за роботою мережі: аналізаторів протоколів або програм на основі протоколу SNMP. Цей метод отримав дуже широке поширення, і сьогодні вже існує діагностичні засоби, що містять вбудовану експертну систему, яка спрощує процес діагностики.

Метод стресового тестування полягає в створенні в мережі великого навантаження і перевірці її працездатності в цих екстремальних умовах. Метод стресового тестування доповнює метод пасивної діагностики. Він дозволяє перевірити мережу в екстремальних умовах експлуатації і побудувати "систему координат", яка полегшує інтерпретацію даних, отриманих в результаті пасивної діагностики. Зазвичай метод стресового тестування використовується на етапі налаштування мережі і після істотних модифікацій її архітектури або топології. Метод пасивної діагностики доцільно використовувати в процесі експлуатації мережі після вже проведеного стресового тестування.

В даний час спостерігається широке застосування локальних обчислювальних мереж (ЛОМ), як в науково–виробничій, загальноосвітній, комерційній, так і в побутовій діяльності людини. Даний процес завжди супроводжується внесенням змін в архітектуру обчислювальної мережі, що призводить до зростання її складності, а також зростання ймовірності виникнення дефекту в мережі під час її модифікації і експлуатації. При цьому, відсутність дорогого устаткування для тестування і діагностики (ліцензійні аналізатори протоколів, кабельні сканери), а також відсутність єдиної універсальної методики діагностування та пошуку дефектів в мережі значно ускладнює процес її діагностичного обслуговування. Найбільш трудомістким завданням діагностування мережі є локалізація дефекту.

У зв'язку з цим, є актуальною задача розробки методів діагностування мережі, зокрема, методів пошуку дефектів в ЛОМ, із застосуванням методів і алгоритмів технічної діагностики цифрових пристроїв.

Існує 3 основних види діагностики мережі:

1. Діагностика на випередження, яка полягає в спостереженні за роботою мережі з моменту її установки в цілях визначення порогових значень параметрів, що впливають на роботу мережі. Перевищення даних значень свідчить про наявність проблеми в мережі.

2. Стресове діагностування – створення в мережі великого навантаження і перевірка її працездатності в цих екстремальних умовах на етапі налаштування мережі і після істотних модифікацій її архітектури або топології.

3. Комплексна – комплекс заходів і методів, що дозволяють швидко і ефективно локалізувати і усунути несправність в мережі при її появі.

Перші два види діагностики виконуються в профілактичних цілях, коли мережа знаходиться в справному стані і працює в штатному режимі. Можна сказати, що на даному етапі працює теорія надійності, коли необхідно визначити ймовірність появи несправності. Отже, немає необхідності застосовувати алгоритми технічної діагностики, завданням яких є, власне, виявлення несправності. Однак, як тільки мережа починає працювати в позаштатному режимі зі стабільним порушенням працездатності, в роботу включаються механізми комплексного діагностування, спрямовані на виявлення та усунення дефекту в мережі за мінімально можливий час з метою запобігання відмови і простою мережі.

1.2 Загальні питання діагностики мереж

Зазначимо ряд основних визначень технічної діагностики адаптований стосовно до даного розділу:

Діагностування мережі – процес виявлення несправностей і відновлення працездатності мережі шляхом застосування моделей, методів і алгоритмів технічної діагностики.

Мережа як об'єкт діагностування являє собою сукупність трьох складових: активне і пасивне устаткування, передає середовище, сукупність протоколів обміну даними в мережі. Технічний стан згаданих компонент мережі впливає на її працездатність.

Технічний стан сукупність справного і всіх несправних станів. Стосовно до мережі як об'єкту діагностування під технічним станом буде розумітися сукупність {ФС, ЛС}, де ФС – фізичне, підтримуване нижніми рівнями моделі OSI, і ЛС – логічне, підтримуване верхніми рівнями моделі OSI, стану мережевого обладнання. У свою чергу, кожен з елементів множини {ФС, ЛС} є сукупністю справного і всіх несправних станів, згідно.

Справний стан–стан об'єкта, при якому він відповідає всім вимогам нормативно–технічної та конструкторської документації. У працездатному стані параметри об'єкта повинні відповідати виконанню заданих функцій навіть при наявності пошкоджень. Стан правильного функціонування допускає наявність несправностей, які не порушують правильну роботу об'єкта.

Мережа є працездатною, якщо її функціонування не викликає появи помилок на будь–якому з рівнів моделі OSI. Відмова мережі – подія, що полягає в порушенні працездатності мережі при виникненні дефекту, який призводить або до значного обмеження доступу до мережевих ресурсів і послуг, або до припинення її функціонування.

Дефект – кожна окрема невідповідність виробу встановленим вимогам. У ЛОМ до таких належать: фізичне пошкодження пристрою, включаючи кабельну систему; перешкоди навколишнього середовища і логічне пошкодження: дефекти мережевого драйвера, втрата інформації, неправильна конфігурація маршрутизаторів, шлюзів та інших комутуючих пристроїв, неправильна конфігурація програмного забезпечення, що призводять до непрацездатного стану пристрою і мережі в цілому, або однією зі складових мережі, зазначених вище. Математична модель дефекту – несправність.

При застосуванні моделей, методів і алгоритмів технічної діагностики цифрових пристроїв до обчислювальної мережі, необхідно адаптувати їх до нового об'єкту діагностування – локальної/корпоративної обчислювальної мережі. Вона має наступні відмінності від цифрового пристрою:

1. Наявність вихідних і вхідних адрес у будь–якого пакета, що передається.

2. Розосередження цифрової апаратури обчислювальної системи в просторі в масштабах офісу, університету, підприємства.

3. Наявність значних по довжині кабельних з'єднань і допоміжного пасивного обладнання: елементи структурованої кабельної системи (патч–панелі, пасивне обладнання, коннектори, розетки).

4. Поєднання каналів введення, передачі, перетворення і спостереження інформації на одній робочій станції – контрольній точці.

5. Різноманіття типів логічних і фізичних дефектів, що призводять до непрацездатного стану мережі або її компонентів.

6. Наявність правил обміну даними – мережевих протоколів.

Мережевий сегмент – структура з єдиним логічним адресним простором, розосереджена фізично.

Тест – вхід–вихідна послідовність, призначена для встановлення відповідності технічного стану об'єкта заданим технічним станам. У мережі тест здійснюється

сервісним обладнанням апаратної, або програмної реалізації. До першого відноситься перевірка кабелю кабельним сканером, тестером, мультиметром, термінатором на цілісність або ідентифікацію місця і причини несправності. До другого: команда ping – перевірка цілісності кабелю, справності мережевого адаптера або ідентифікація несправності. Слід зауважити, що тест може носити як активний, пов'язаний з виконанням дій, що впливають на функціонування мережі, наприклад, перевірка кабельної системи, так і пасивний характер, здійснюваний шляхом спостереження за мережею і збору статистичної інформації без втручання в роботу мережі.

Таким чином, в мережі може виконуватися як функціональне технічне діагностування, здійснюване під час роботи об'єкта, на який надходять тільки робочі впливу, наприклад, обчислення контрольної суми функціонуючим мережевим пристроєм, так і тестове технічні діагностування з подачею тестових впливів на об'єкт.

Елементарна перевірка – процедура, яка полягає в подачі тесту на мережевий компонент і спостереженні реакції на нього, виконувана з метою визначення технічного стану компонента шляхом порівняння отриманої реакції з еталонним станом (робота в штатному режимі).

Реакція – інформація про технічний стан компонента, який тестується, що надається тестовим обладнанням та дозволяє зробити висновки про відповідність / невідповідність технічного стану еталонному. Відповідність технічного стану компонента еталонному супроводжується відсутністю повідомлень про помилки на консолі тестового обладнання (позитивна реакція) і навпаки (негативна реакція).

Результат елементарної перевірки – отримання реакції при подачі тесту і її порівняння з еталоном. Результат елементарної перевірки позитивний, якщо реакція свідчить про відповідність технічного стану тестового компонента еталонному. Результат елементарної перевірки негативний, якщо реакція свідчить про невідповідність технічного стану тестового компонента еталонному.

1.3 Класифікація засобів моніторингу й аналізу мережі

Все різноманіття засобів, застосовуваних для моніторингу й аналізу обчислювальних мереж, можна розділити на кілька великих класів:

Системи керування мережею (NetworkManagementSystems) – централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафіку, що циркулює в мережі. Ці системи не тільки здійснюють моніторинг й аналіз мережі, але й виконують в автоматичному або напівавтоматичному

режимі дії по керуванню мережею – включення й відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів і т.п. Прикладами систем керування можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView.

Засоби керування системою (SystemManagement). Засоби керування системою часто виконують функції, аналогічні функціям систем керування, але стосовно інших об'єктів. У першому випадку об'єктом керування є програмне й апаратне забезпечення комп'ютерів мережі, а в другому – комунікаційне встаткування. Разом з тим, деякі функції цих двох видів систем керування можуть дублюватися, наприклад, засобу керування системою можуть виконувати найпростіший аналіз мережного трафіку.

Вбудовані системи діагностики й керування (Embeddedsystems). Ці системи виконуються у вигляді програмно–апаратних модулів, установлюваних у комунікаційне встаткування, а також у вигляді програмних модулів, убудованих в операційні системи. Вони виконують функції діагностики й керування тільки одним пристроєм, і в цьому їхню основну відмінність від централізованих систем керування. Прикладом засобів цього класу може служити модуль керування концентратором Distrebuted 5000, що реалізує функції автосегментації портів при виявленні несправностей, приписування портів внутрішнім сегментам концентратора й деякі інші. Як правило, убудовані модулі керування "по сумісництву" виконують роль SNMP–агентів, що поставляють дані про стан пристрої для систем керування.

Аналізатори протоколів (Protocolanalyzers). Являють собою програмні або апаратно–програмні системи, які обмежуються на відміну від систем керування лише функціями моніторингу й аналізу трафіку в мережах. Гарний аналізатор протоколів може захоплювати й декодувати пакети великої кількості протоколів, застосовуваних у мережах – звичайно кілька десятків. Аналізатори протоколів дозволяють установити деякі логічні умови для захоплення окремих пакетів і виконують повне декодування захоплених пакетів, тобто показують у зручній для фахівця формі вкладеність пакетів протоколів різних рівнів друг у друга з розшифровкою змісту окремих полів кожного пакета.

Устаткування для діагностики й сертифікації кабельних систем. Умовно це встаткування можна поділити на чотири основні групи:

- мережні монітори;
- прилади для сертифікації кабельних систем;
- кабельні сканери;
- тестери (мультиметри).

Мережні монітори (називані також мережними аналізаторами) призначені для тестування кабелів різних категорій. Варто розрізняти мережні монітори й аналізатори протоколів. Мережні монітори збирають дані тільки про статистичні показники трафіка – середньої інтенсивності загального трафіка мережі, середній інтенсивності потоку пакетів з певним типом помилки й т.п.

Призначення пристроїв для сертифікації кабельних систем, безпосередньо треба з їхньої назви. Сертифікація виконується відповідно до вимог одного з міжнародних стандартів на кабельні системи.

Кабельні сканери використаються для діагностики мідних кабельних систем.

Тестери призначені для перевірки кабелів на відсутність фізичного розриву.

Експертні системи. Цей вид систем акумулює людські знання про виявлення причин аномальної роботи мереж і можливих способів приведення мережі в працездатний стан. Експертні системи часто реалізуються у вигляді окремих підсистем різних засобів моніторингу й аналізу мереж: систем керування мережами, аналізаторів протоколів, мережних аналізаторів. Найпростішим варіантом експертної системи є контекстно–контекстно–залежна help–система. Більше складні експертні системи являють собою так названі бази знань, що володіють елементами штучного інтелекту. Прикладом такої системи є експертна система, убудована в систему керування Spectrum компанії Cabletron.

Багатофункціональні пристрої аналізу й діагностики. В останні роки, у зв'язку з повсюдним поширенням локальних мереж виникла необхідність розробки недорогих портативних приладів, що сполучають функції декількох пристроїв: аналізаторів протоколів, кабельних сканерів й, навіть, деяких можливостей ПЗ мережного керування. Як приклад такого роду пристроїв можна привести Compas компанії MicrotestInc. або 675 LANMeter компанії FlukeCorp.

1.4 Системи керування мережею

Відповідно до рекомендацій ISO можна виділити наступні функції засобів керування мережею:

Керування конфігурацією мережі й іменуванням – складається в конфігуруванні компонентів мережі, включаючи їхнє місце розташування, мережні адреси й ідентифікатори, керування параметрами мережних операційних систем, підтримка схеми мережі: також ці функції використаються для іменування об'єктів.

Обробка помилок – це виявлення, визначення й усунення наслідків збоїв і відмов у роботі мережі.

Аналіз продуктивності – допомагає на основі накопиченої статистичної інформації оцінювати час відповіді системи й величину трафіка, а також планувати розвиток мережі.

Керування безпекою – містить у собі контроль доступу й збереження цілісності даних. У функції входить процедура аутентифікації, перевірки привілеїв, підтримка ключів шифрування, керування повноваженнями. До цієї ж групи можна віднести важливі механізми керування паролями, зовнішнім доступом, з'єднання з іншими мережами.

Облік роботи мережі – включає реєстрацію й керування використовуваними ресурсами й пристроями. Ця функція оперує такими поняттями як час використання й плата за ресурси.

З наведеного списку видно, що системи керування виконують не тільки функції моніторингу й аналізу роботи мережі, необхідні для одержання вихідних даних для настроювання мережі, але й включають функції активного впливу на мережу – керування конфігурацією й безпекою, які потрібні для відпрацьовування виробленого плану настроювання й оптимізації мережі. Сам етап створення плану настроювання мережі звичайно залишається за межами функцій системи керування, хоча деякі системи керування мають у своєму складі експертні підсистеми, що допомагають адміністраторові або інтегратору визначити необхідні заходи щодо настроювання мережі.

Засоби керування мережею (NetworkManagement), не слід плутати із засобами керування комп'ютерами і їхніми операційними системами (SystemManagement).

Засоби керування системою звичайно виконують наступні функції:

Облік використовуваних апаратних і програмних засобів. Система автоматично збирає інформацію про обстежені комп'ютери й створює запису в базі даних про апаратні й програмні ресурси. Після цього адміністратор може швидко з'ясувати, чим він розташовує й де це перебуває. Наприклад, довідатися про те, на яких комп'ютерах потрібно обновити драйвери принтерів, які ПК мають достатню кількість пам'яті й дискового простору й т.п.

Розподіл й установка програмного забезпечення. Після завершення обстеження адміністратор може створити пакети розсилання програмного забезпечення – дуже ефективний спосіб для зменшення вартості такої процедури. Система може також дозволяти централізовано встановлювати й адмініструвати додатка, які запускаються з файлових серверів, а також дати можливість кінцевим користувачам запускати такі додатки з будь–якої робочої станції мережі.

Вилучений аналіз продуктивності й виникаючих проблем. Адміністратор може видалено управляти мишею, клавіатурою й бачити екран будь–якого ПК, що працює в мережі під керуванням тієї або іншої мережної операційної системи. База дані системи

керування звичайно зберігає детальну інформацію про конфігурації всіх комп'ютерів у мережі для того, щоб можна було виконувати вилучений аналіз виникаючих проблем.

Прикладами засобів керування системою є такі продукти, як SystemManagementServer компанії Microsoft або LANDeskManager фірми Intel, а типовими представниками засобів керування мережами є системи HPOpenView, SunNetManager й IBMNetView.

Останнім часом в області систем керування спостерігаються дві досить чітко виражені тенденції:

– інтеграція в одному продукті функцій керування мережами й системами,

– розподіл системи керування, при якій у системі існує кілька консолей, що збирають інформацію про стан пристроїв і систем і керуючих дій, що видає.

Створення систем керування мережами немислимо без орієнтації на певні стандарти, тому що керуюче програмне забезпечення й мережне встаткування, а, виходить, і агентів для нього, розробляють сотні компаній. Оскільки корпоративна мережа напевно неоднорідна, що управляють інструменти не можуть відбивати специфіки однієї системи або мережі.

Найпоширенішим протоколом керування мережами є протокол SNMP (SimpleNetworkManagementProtocol), його підтримують сотні виробників. Головні достоїнства протоколу SNMP – простота, доступність, незалежність від виробників. У значній мірі саме популярність SNMP затримала прийняття CMIP, варіанта керуючого протоколу за версією OSI. Протокол SNMP розроблений для керування маршрутизаторами в мережі Internet й є частиною стека TCP/IP.

SNMP – це протокол, використовуваний для одержання від мережних пристроїв інформації про їхній статус, продуктивність і характеристики, які зберігаються в спеціальній базі даних мережних пристроїв, називаної MIB (ManagementInformationBase). Існують стандарти, що визначають структуру MIB, у тому числі набір типів її змінних (об'єктів у термінології ISO), їхні імена й припустимі операції цими змінними (наприклад, читати). В MIB, поряд з іншою інформацією, можуть зберігатися мережний й/або MAC–адреси пристроїв, значення лічильників оброблених пакетів і помилок, номера, пріоритети й інформація про стан портів. Деревоподібна структура MIB містить обов'язкові (стандартні) піддерева, а також у ній можуть перебувати частки (private) піддерева, що дозволяють виготовлювачеві інтелектуальних пристроїв реалізувати які–небудь специфічні функції на основі його специфічних змінних.

Агент у протоколі SNMP – це обробний елемент, що забезпечує менеджерам, розміщеним на керуючих станціях мережі, доступ до значень змінних MIB, і тим самим

дає їм можливість реалізовувати функції по керуванню й спостереженню за пристроєм. Основні операції по керуванню винесені в керуючу станцію. При цьому пристрій працює з мінімальними витратами на підтримку керуючого протоколу. Воно використає майже всю свою обчислювальну потужність для виконання своїх основних функцій маршрутизатора, моста або концентратора, а агент займається збором статистики й значень змінні стани пристрою й передачею їхньому менеджерові системи керування. SNMP – це протокол типу "запит–відповідь", тобто на кожен запит, що надійшов від менеджера, агент повинен передати відповідь. Особливістю протоколу є його надзвичайна простота – він містить у собі всього кілька команд.

Типова структура системи керування зображена на рис. 1.1.

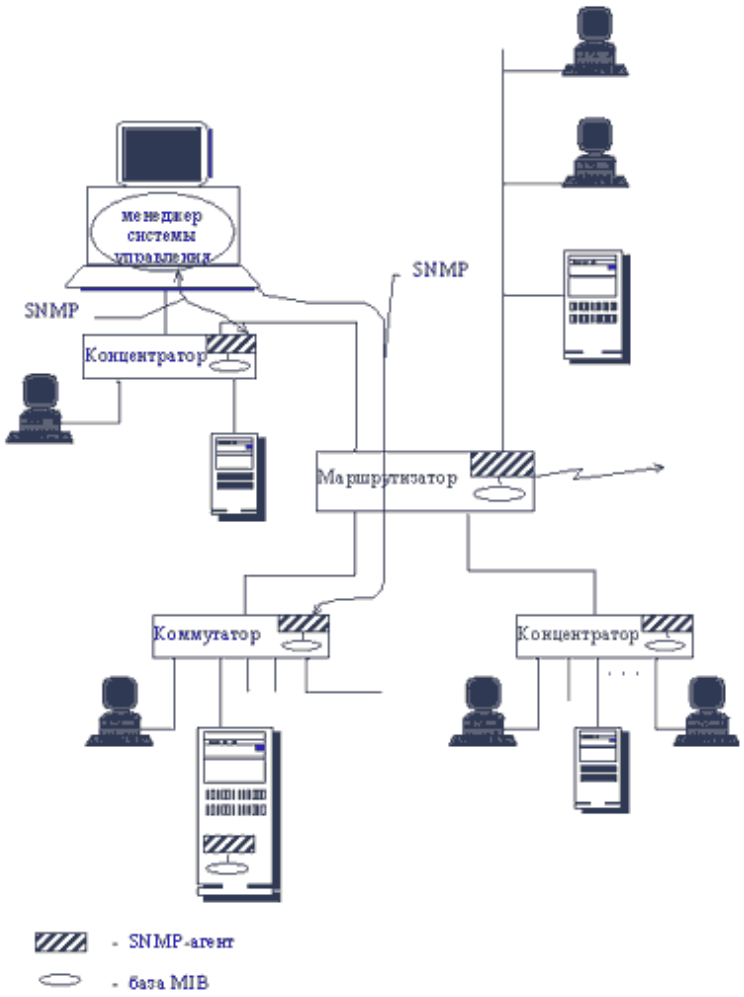


Рисунок 1.1 – Типова структура системи керування мережею.

Команда Get–request використається менеджером для одержання від агента значення якого–небудь об'єкта по його імені.

Команда GetNext–request використовується менеджером для витягу значення наступного об'єкта (без вказівки його імені) при послідовному перегляді таблиці об'єктів.

За допомогою команди Get–response агент SNMP передає менеджерові відповідь на одну з команд Get–request або GetNext–request.

Команда Set використається менеджером для встановлення значення якого–небудь об'єкта або умови, при виконанні якого агент SNMP повинен послати менеджерові відповідне повідомлення. Може бути визначена реакція на такі події як ініціалізація агента, рестарт агента, обрив зв'язку, відновлення зв'язку, невірна аутентифікація й втрата найближчого маршрутизатора. Якщо відбувається кожне із цих подій, то агент ініціалізує переривання.

Команда Trap використається агентом для повідомлення менеджерові про виникнення особливої ситуації.

Версія SNMP v.2 додає до цього набору команду GetBulk, що дозволяє менеджерові одержати кілька значень змінних за один запит.

1.5 Фізичні основи діагностики мереж

Розглянемо базові мережеві топології і їх стан при наявності несправності.

Отже, по загальній конфігурації розрізняють наступні топології локальної обчислювальної мережі:

– шинна;

– зіркоподібна;

– кільцева;

– деревоподібна.

1.5.1 Шинна топологія

У локальних мережах з шинної топологією всі абонентські системи за допомогою мережевих адаптерів підключаються до загальної магістралі (шини). В якості середовища найчастіше використовується коаксіальний кабель.

В процесі роботи мережі інформація від передавальної абонентської системи надходить на адаптери всіх абонентських систем, проте сприймається тільки адаптером тієї абонентської системи, якій вона адресована. Використання абонентськими системами

загального передавального середовища передбачає вирішення завдання організації почергового доступу до неї (рис. 1.2).

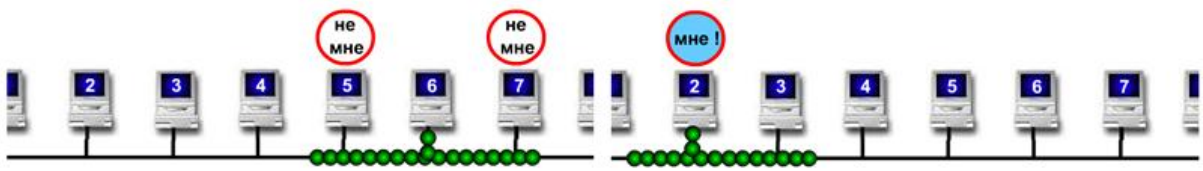


Рисунок 1.2 – Шинна топологія мережі

Метод доступу для мережі шинної топології – множинний доступ з контролем несучої і виявленням конфліктів (МДКН / ВК). Найбільш характерним представником мереж з шинної топологією є мережа Ethernet (стандарт організації локальних обчислювальних мереж , який описаний в специфікаціях IEEE і інших організацій (IEEE 802.3). Смуга пропускання – 10…1000 Mbps, метод доступу до середовища – CSMA / CD. Найбільш популярна реалізація Ethernet – 10Base–T. Розвитком технології Ethernet в подальшому є Fast Ethernet (100 Мбіт/с), яка є найбільш поширена на сьогоднішній день з поряд мережею на 1000 Мбіт/с.

Обов'язковим елементом подібного передавального середовища є термінатор, що представляє собою опір узгодження, за допомогою якого усувається ефект відбитої хвилі на кінцях коаксіального кабелю. У разі відсутності термінатора мережа шинної топології працювати не буде (рис. 1.3).

Рисунок 1.3 – Мережа з відсутнім термінатором

При обриві кабелю відбудеться такий же ефект, як і при відсутності термінатора, що призведе до появи колізій та припинення функціонування мережі (рис.1.4).

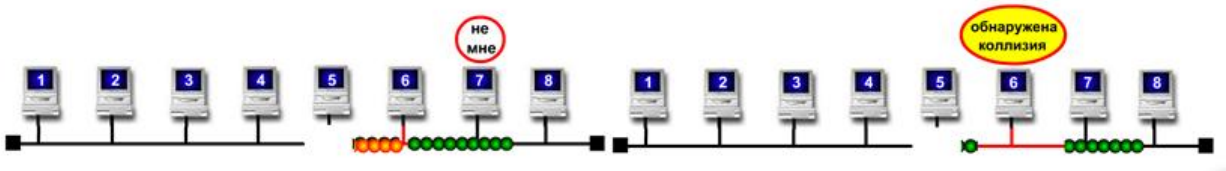


Рисунок 1.4 – Обрив кабелю мережі та поява колізій

При виході з ладу будь–якого мережевого адаптера дана несправність відіб'ється на мережевому функціонуванні абонентської станції–володаря дефектного адаптера, але не позначиться на функціонуванні мережі в цілому.

1.5.2 Топологія типу "зірка"

Зіркоподібна локальна мережа характеризується наявністю центрального вузла комутації, через який посилаються всі повідомлення. При використанні в якості концентратора (вузла комутації) багатопортового повторювача інформація передається так само, як і в мережі з шинною топологією: пакет надходить на всі вузли мережі і приймається тільки вузлом–адресатом (рис. 1.5).

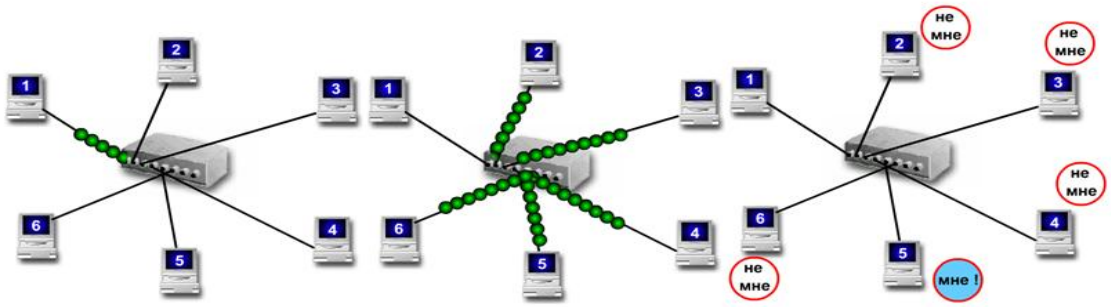


Рисунок 1.5 – Передача інформації в зіркоподібній локальній мережі

Дана топологія має більш високу живучістю у порівнянні з шинної топологією. При обриві сегмента кабелю припиняється мережеве функціонування тільки тієї абонентської системи, яка була підключена даними кабелем до концентратора, але не всієї мережі (рис. 1.6).

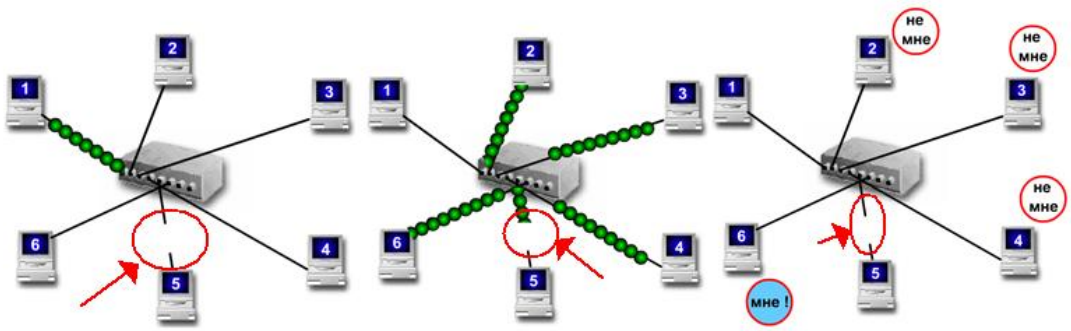


Рисунок 1.6 – Обрив сегмента кабелю в зіркоподібній мережі

Аналогічним чином вплинуть на мережу дефекти мережевого адаптера абонентської системи або самої абонентської системи (рис. 1.7).

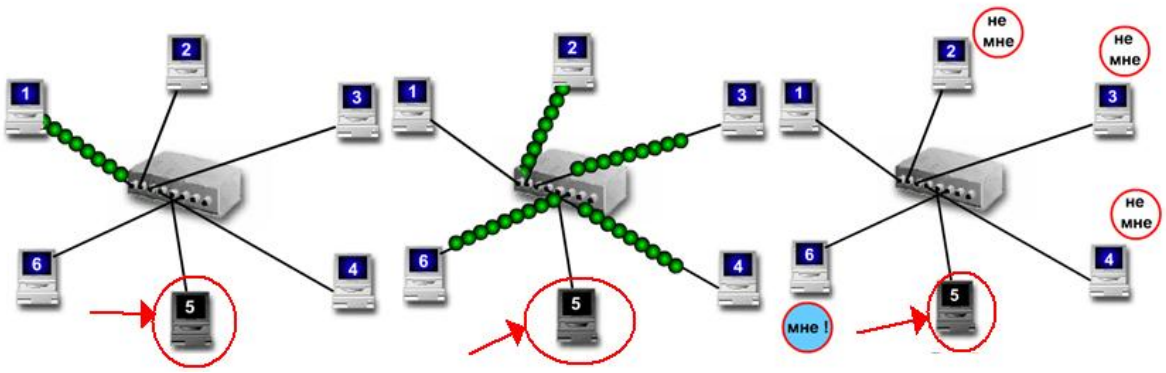


Рисунок 1.7. – Зіркоподібна мережа з непрацездатним мережевим адаптером

Критичним компонентом в мережі зіркоподібної топології є концентратор: при виході його з ладу припиняється функціонування всієї мережі.

1.5.3 Кільцева топологія

Кільцева локальна мережа характеризується наявністю замкнутого односпрямованого каналу передачі даних, у вигляді кільця або петлі. У цьому випадку інформація передається послідовно між адаптерами абонентських систем до тих пір, поки не буде прийнята одержувачем і потім видалена з мережі. Зазвичай за видалення інформації з мережі відповідає її відправник. Управління роботою кільцевої мережі може здійснюватися централізовано за допомогою спеціальної моніторної станції, або децентралізовано за рахунок розподілу функцій управління між усіма абонентськими системами. Як і в мережах з шинної топологією послідовність передачі інформації абонентськими системами регулюється за допомогою певного методу доступу (маркерний доступ).

Один з істотних недоліків кільця – вихід її з ладу при розриві кільця, як правило, усувається за рахунок використання "подвійного" кільця. Для цього до складу локальної мережі включають додаткові лінії зв'язку і пристрої реконфігурації, які представляють собою спеціальні пристрої – перемикачі.

1.5.4 Деревоподібна топологія

Деревоподібна топологія широко використовується в сучасних високошвидкісних локальних комп'ютерних мережах. У якості вузлів комутації найчастіше виступають високошвидкісні комутатори (хаби) (рис. 1.8). Найбільш характерним представником мереж з подібною структурою є мережа 100VG Any Lan (локальна комп'ютерна мережа деревовидної топології з пропускною спроможністю 100 Mbps, використовує в якості методу доступу протокол пріоритетів запитів – DDP (Demand Priority Protocol), що забезпечує відсутність колізій). Цікаво відзначити, що високошвидкісний варіант магістральної мережі Ethernet – Fast Ethernet (оснащена швидкодіючими комутаторами мережі типу Ethernet з пропускною спроможністю 100 Mbps) також має деревоподібну структуру.

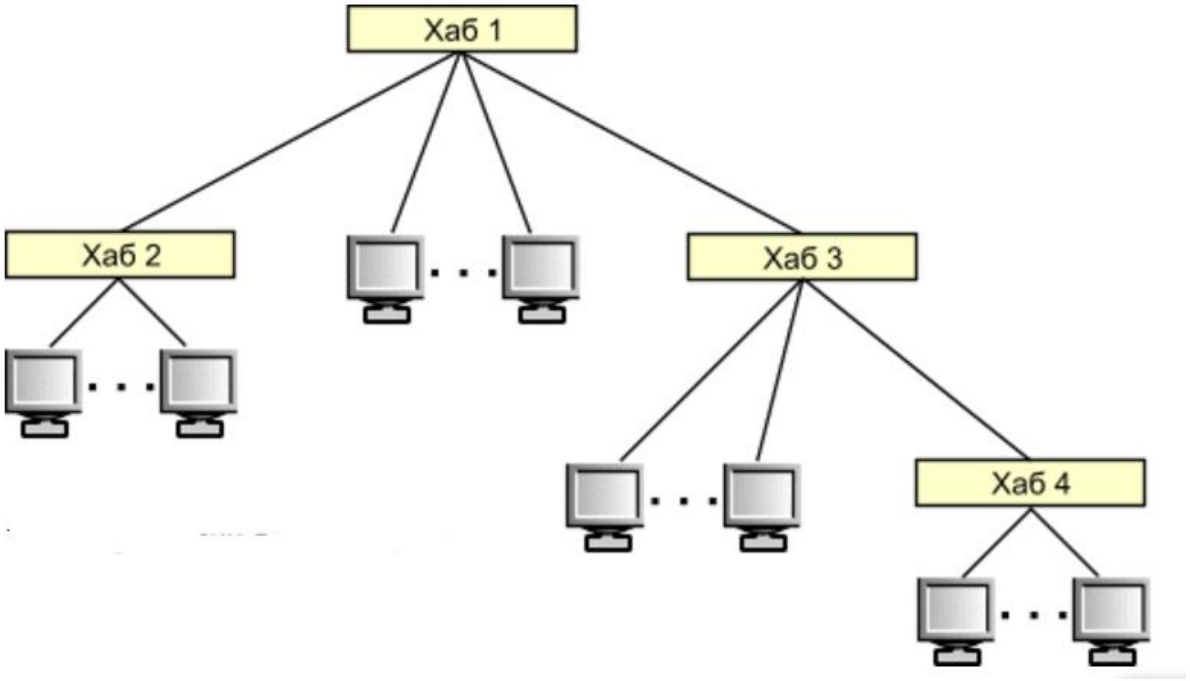


Рисунок 1.8 – Деревоподібна структура мережі

У порівнянні з шинними і кільцевими мережами деревовидні локальні мережі мають більш високу живучістю. Відключення або вихід з ладу однієї з ліній або комутатора, як правило, не робить істотного впливу на працездатність решти локальної мережі.

1.6 Висновки до розділу 1 та постановка задачі дослідження

В першому розділі магістерської роботи розглянуті загальні питання діагностики комп’ютерних систем та мереж, проведено огляд фізичні основ діагностики мереж. На основі проведеного дослідження визначені основні задачі магістерської роботи, а саме:

– розробити алгоритми пошуку типових несправностей та дефектів в локальній обчислювальній мережі;

– розробити та дослідити модель мережі для пошуку дефектів структурним немодифікованим методом;

– побудувати імітаційну модель сегменту мережі;

– на основі імітаційної моделі розробити програмне забезпечення для діагностики та моделювання типових несправностей комп’ютерної мережі.

РОЗДІЛ 2
ПОШУК ДЕФЕКТІВ В ЛОКАЛЬНІЙ ОБЧИСЛЮВАЛЬНІЙ МЕРЕЖІ

2.1 Типові несправності мережі

Найбільш частими несправностями в мережі є помилки маршрутизації трактів низького рівня:

1. Обрив лінії зв'язку або оптичного волокна. Типові причини – випадковий обрив при проведенні грабарств, осідання ґрунту, землетрус.

2. Погіршення якості зв'язку (неприйнятно високий коефіцієнт фонових помилок). Типові причини – нагромадження тремтіння фази (джиттера), низька прийнята потужність, оптичні відбиття через неякісне з’єднання або неточного зварювання волоконно-оптичного кабелю.

3. Відмова апаратних засобів. Типові причини – хоча мережеві елементи, подібно всім сучасним електронним пристроям, є високонадійними, в процесі їхньої експлуатації можливі відмови.

4. Помилка маршрутизації тракту (поява несправності на рівні трактів низького або високого рівня). Типові причини – неправильна маршрутизація трактів у мультиплексорах вводу/виводу або цифрових крос-комутаторах (можливо викликана помилкою оператора в процесі установки мережевих трактів при використанні декількох систем керуванням конфігурацією або в результаті збою в програмному забезпеченні системи керування конфігурацією). Коли інженер по обслуговуванню мережі знає про існування проблеми, йому необхідно локалізувати джерело й усунути несправність. Методологія практичної локалізації несправностей представлена на рис. 2.1.

Рисунок 2.1. – Практична локалізація несправностей

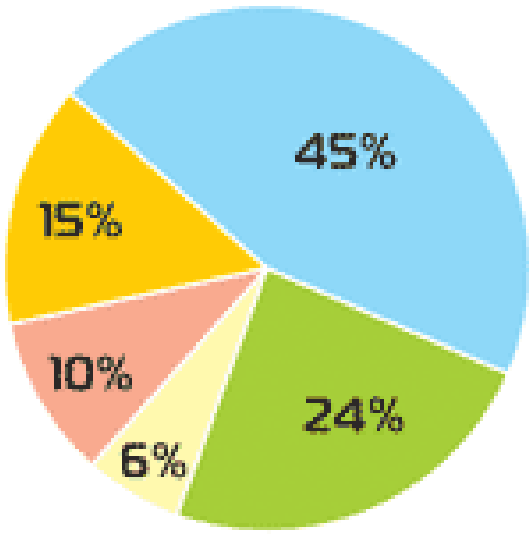
Очевидно, що локалізація джерела несправності є значно більш складним завданням, чим просто її виявлення. Гарантією того, що обслуговуючий персонал мережі має здатність локалізувати всі загальновідомі мережеві несправності, є обов'язкове дотримання наступних умов:

– наявність інтерфейсу обслуговуючого рівня для доступу до даних про помилки й аварійні сигнали в системі керування обробкою несправностей
– наявність портативного тестового встаткування для отримання тестових даних від тих точок мережі, звідки не надходять дані внутрішньої діагностики.

Тестові дані від цих двох джерел необхідні для локалізації типових несправностей, таких, як помилка маршрутизації тракту (поява несправності на рівні трактів низького або високого рівня), а також для локалізації деяких типів несправностей апаратної частини мережевих елементів.

2.1.1 Несправності кабельних ліній зв'язку

Порушення нормального функціонування кабельних систем на базі крученої пари можуть бути викликані грубими помилками при монтажі, прихованими дефектами конструкції кабелю й ушкодженням при його прокладки, процесами старіння самих кручених пар й арматури кабельних ліній зв'язку, а також іншими причинами (рис. 2.2).



45% — порушення герметичності муфт і місць зварювань;
15% — проведення сторонніх робіт на трасі;
10% — розтріскування кабелю в результаті перегину;
6% — розтріскування кабелю на прямолінійній ділянці;
24% — ушкодження кабелю гризунами, промерзання кабельної каналізації та інші ушкодження.

Рисунок 2.2 – Розподіл ушкоджень по кабельних ліній

2.1.2 Основні ушкодження крученої пари

До явних недоліків монтажу ставляться помилки з'єднання жил кручених пар у кросах АТС, на стиках будівельних довжин, у розподільних шафах і коробках, вилучених терміналах і т.д. Нижче наведені опису, а також устояні англомовні назви дефектів, використовувані в різних вимірювальних приладах для індикації типу несправності.

Відповідно до прийнятої термінології, дві пари, у яких порушений правильний порядок підключення жил, називаються розщепленими (split) (рис. 2.3).

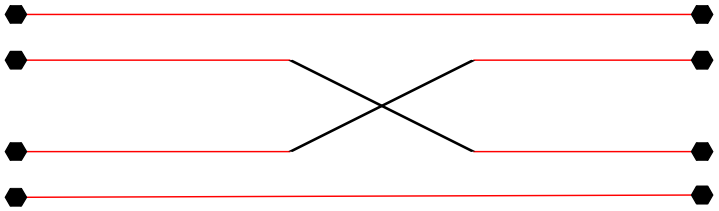


Рисунок 2.3 – Розщеплена (split) вита пара

Ознаками розщеплених пар можуть бути збільшений резистивний й ємнісної дисбаланс. Неправильно змонтована кручена пара, де прямий і зворотний дроти переставлені місцями, називається перевернеою або схрещеною (reversal) (рис. 2.4).

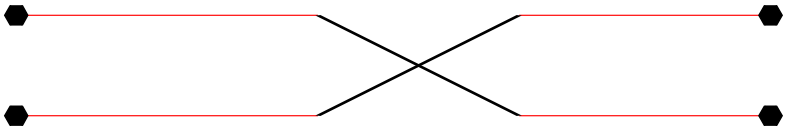


Рисунок 2.4 – Перевернена або схрещена (reversal) кручена пара

У такому випадку лінія tip (T) підключена до мінуса станційної батареї, а лінія ring (R) - до її плюса. Гнучка частина термінального устаткування (у тому числі всі телефонні апарати) мають захист від порушення полярності станційної батареї. Але в кабельних лініях локальної мережі порядок підключення жили крученої пари вкрай важливий.

Дві кручені пари з помилковим підключенням до контактів термінала називаються транспонованими парами (transposition) (рис. 2.5).

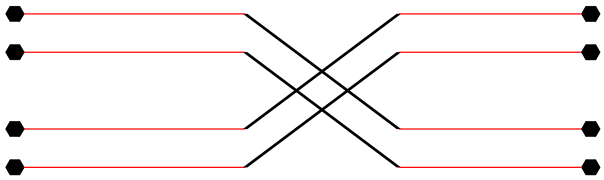


Рисунок 2.5 – Транспонована вита пара (transposition)

На телефонній мережі такий дефект монтажу приведе до підключення невірного номера. У випадку ж локальної мережі підключене до лінії устаткування виявитися непрацездатним.

До основних прихованих дефектів кабельних ліній зв'язку відноситься:

– неякісний монтаж муфт;
– обрив на стиках будівельних конструкцій.

У першому випадку на рис. 2.6 порушується герметичність оболонки кабелю й виникає небезпека його намокання, а для іншого характерна поява поганих контактів (partial open) і навіть обрив жили крученої пари (open). До таких же результатів приводити корозія контактів кросових пристроїв і неякісний крос (рис. 2.7).

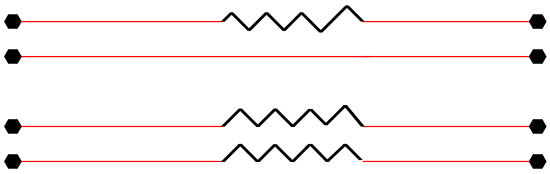


Рисунок 2.6 – Неякісний монтаж муфт

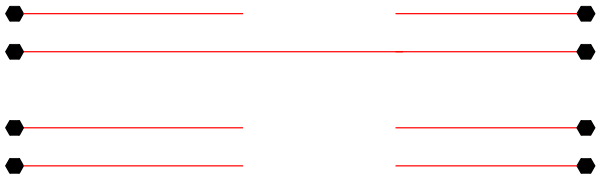


Рисунок 2.7 – Обрив на стиках будівельних конструкцій

Дефекти й пробої ізоляції жил, волога в кабелі й забруднення терміналів нерідко ведуть до замикання жил пари між собою.

Замикання може бути низькоомним (short) (рис. 2.8) або високоомним (partial short) (рис. 2.9).

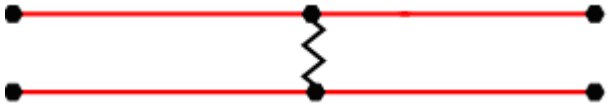


Рисунок 2.8 – Низькоомне (short) замикання

Рисунок 2.9 – Високоомне (partial short) замикання

Ще один аналогічний вид дефектів крученої пари - замикання на землю однієї або декількох її жил (ground) (рис. 2.10).

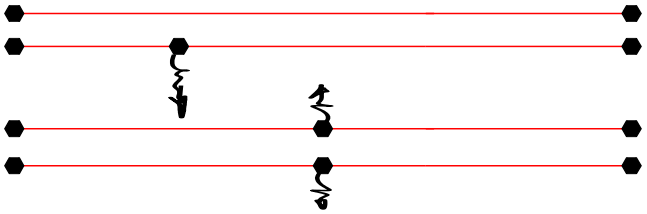


Рисунок 2.10 – Замикання на землю однієї або декількох жил (ground)

Причому контакт жили з землею зовсім не обов'язково буде перебувати недалеко від місця ушкодження ізоляції жили - електричний шлях від провідника жили до землі пройде через екран кабелю, металеві елементи конструкції терміналів і несучі елементи кабелю.

Замикання трапляється й між жилами двох різних пар, причому замкнуті можуть бути як однойменні, так і різнойменні жили (cross й battery cross, відповідно). Такий вид дефектів приводити до наявності сторонньої напруги на лінії, перехідним явищам, ослабленню сигналу. На телефонній мережі можливий ефект постійного сигналу готовності станції на лінії.

Природний процес старіння крученої пари проявляється у вигляді збільшення внесеного нею загасання внаслідок погіршення діелектричних властивостей ізоляції крученої пари. Тому при проектуванні ЦСП, включаючи й лінії xDSL, повинні бути передбачені підвищені запаси по внесеному загасанню.

При ідентифікації несправностей пари завжди потрібно мати на увазі, що її дефекти можуть бути множинними (кілька однотипних дефектів) на рис. 2.11 або комбінованими

(кілька різнотипних дефектів) на рис. 2.12, а показання приладів при вимірах з різних сторін можуть істотно відрізнятися.

Рисунок 2.11 – Множинні (кілька однотипних дефектів) дефекти

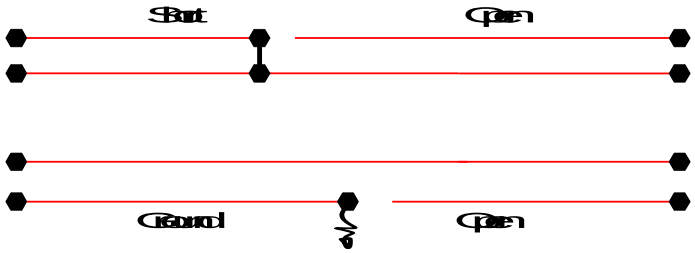


Рисунок 2.12 – Комбіновані (кілька різнотипних дефектів) дефекти

Як уже згадувалося, джерелами перешкод крученої пари служать внутрішні й зовнішні перешкоди кабелю. До основних джерел внутрішніх перешкод відносять сусідні кручені пари того ж кабелю, а до основних джерел зовнішніх перешкод - перешкоди від мережі змінного току й атмосферні явища, включаючи розряди блискавки й радіоперешкоди.

Ефективність придушення зовнішніх перешкод, і в першу чергу гармонік мережі змінного току, забезпечується трьома механізмами:

– високим ступенем симетрії крученої пари;
– цілісністю оболонки кабелю, що служити екраном;
– високоякісним періодичним заземленням екрана уздовж кабельної лінії.

Порушення нормальної роботи шкірного з їх може статі причиною підвищених шумів крученої пари. Більше того, навіть при високій якості симетрії порушення цілісності екрана кабелю й/або дефекти його заземлення здатні привести до появи сильних шумів в абонентській лінії.

У великому числі випадків наслідком всіх порушень нормальної роботи крученої пари є зменшення загасання її асиметрії - саме воно, внаслідок різних причин, робить кручену пару практично беззахисної перед всіма перешкодами як з боку сусідніх пар тієї ж кабельної лінії зв'язку, так і з боку зовнішніх джерел перешкод.

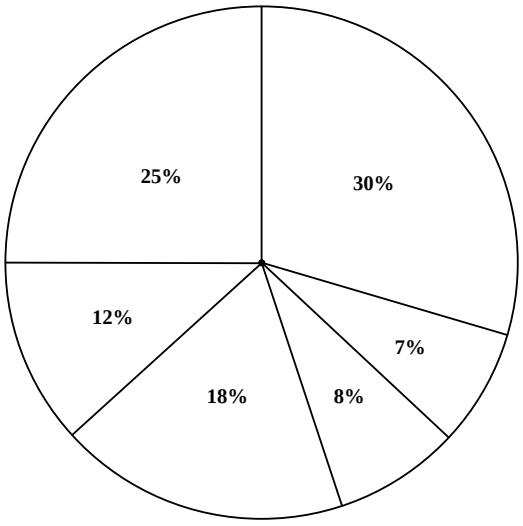
При обстеженні крученої пари, де виявлена сильна перешкода, важливо зрозуміти характер останньої: зокрема, чи постійний її рівень. Залежність рівня перешкоди від години дня, погоди й сезону може вказує на те, що причина криється в режимі роботи мережі змінного току, а також дефектах устаткування цієї мережі.

З першого погляду може здатися незрозумілим, чому, наприклад, рівень перешкод крученої пари зростає в жарку літню погоду й залишається в межах норми в прохолодні дні. Відповідь, однак, простий - у жарі збільшується навантаження на мережі змінного току в результаті масового використання вентиляторів і кондиціонерів, а разом з нею й число низькочастотних перешкод, індукованих у кручених парах мережею змінного току. Сказане, зрозуміло, ставитися й до сильних морозів, коли повсюдно включаються обігрівачі. Точно так саме на рівень перешкод впливають година доби й дні тижня. Тому при оцінці заподій скарги, що надійшла від абонента, варто обов'язково з'ясувати, чи є порушення нормальної роботи крученої пари постійним або виникає лише періодично.

У більшості випадків сильна перешкода - наслідок зміни навантаження мережі змінного струму або режиму роботи таких її елементів, як конденсаторні регулятори косинуса, які працюють у режимі періодичного автоматичного включення.

2.2 Основні несправності волоконно-оптичних ліній зв'язку

Розподіл ушкоджень, основні види несправностей на волоконно-оптичних лініях зв'язку (ВОЛЗ) та їх характеристики наведені на рис. 2.13 та в табл. 2.1.



30% - Зовнішні впливи.

25% - Пил або забруднення.

18% - Перекручування кабелю.

12% - Неякісне зварювання.

Втрати, пов'язані із близьким розташуванням волокон у зварювальному вузлі.

8% - Локальний сплеск загасання в кабелі.

7% - Неякісний кабель.

Рисунок 2.13 - Розподіл ушкоджень на волоконно-оптичних лініях зв'язку

Таблиця 2.1 – Основні види несправностей на ВОЛЗ

Несправність	Співвідно-шення, %	Причина	Устаткування діагностики	Процедура усунення
Конектор	25	Пил або забруднення	Мікроскоп	Очищення, полірування, відновлення
Кабель pigtail	18	Перекручування кабелю	Візуальний дефектоскоп	Усунення перекручування
Локальний сплеск загасання в кабелі	8	Перекручування кабелю	OTDR	Усунення перекручування
Розподілене збільшення загасання в кабелі	7	Неякісний кабель	OTDR	Заміна ділянки кабелю
Втрати у зварювальному вузлі	12	Неякісне зварювання. Втрати, пов'язані із близьким розташуванням волокон у зварювальному вузлі	OTDR Візуальний дефектоскоп	Розкриття вузла й проведення зварювання заново
Обрив кабелю	30	Зовнішні впливи	OTDR, візуальний дефектоскоп	Ремонт/заміна

Пошук несправності в кабелі починається з аналізу його зв’язності з використанням візуального дефектоскопа у випадку кабелів малої довжини або OTDR у випадку протяжних кабелів. Основними несправностями кабелю звичайно є коннектори, зварювання з поганою якістю, з'єднання й обриви кабелю, обумовлені зовнішніми впливами.

Для пошуку несправності в коннекторах застосовуються експлуатаційні мікроскопи. Для діагностики зварювань і локалізації обривів застосовуються OTDR з обліком описаних вище обмежень на точність вимірів.

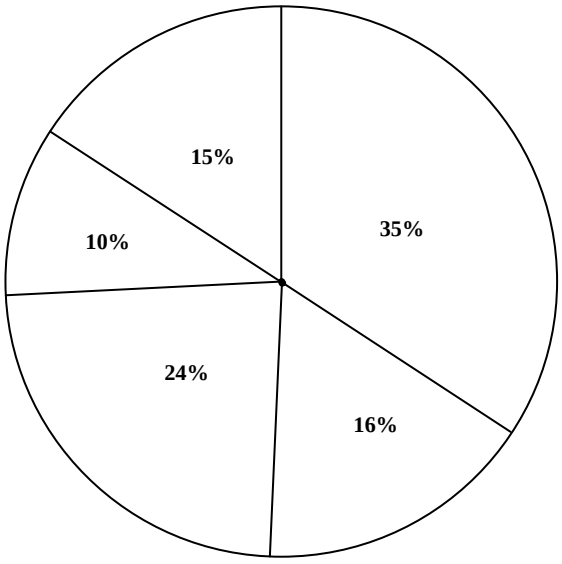
Першим завданням пошуку несправності у ВОСП є аналіз, чи ставитися несправність до електричної частини встаткування або до оптичного. Для цього за допомогою ОРМ виміряється рівень оптичної потужності й потім виробляється порівняння з нормативним.

Якщо рівень оптичної потужності перебуває в межах норми, несправність перебуває в електронній частині апаратури передачі, що має потребу в заміні або ремонті. Якщо рівень прийнятої потужності занадто низький, несправність перебуває або в передавачі, або у волоконно-оптичному кабелі.

Для подальшого пошуку необхідний вимір вихідної потужності передавача, для цього використаються ОРМ і тестовий кабель. Якщо вихідна потужність передавача низька, він винний бути відремонтований. Якщо потужність перебуває в межах норми, несправність пов'язана з волоконним кабелем.

2.3 Розподіл несправностей у бездротових лініях зв'язку

Розподіл та основні види несправностей у бездротових лініях зв'язку наведено на рис. 2.14.



35% - Пошкодження інтерференції.

24% - Пошкодження при перемиканні в роумінг.

16% - Втрата з'єднання з магістральною локальною мережею

15% - Помилка в передачі інформації в інфраструктурі базових станцій і повторювачів

10% - Порушення потужності каналів

Рисунок 2.14 - Розподіл ушкоджень та основні види несправності на бездротових лініях зв'язку

2.4 Модифікація структурного методу пошуку дефектів стосовно ЛОМ

Алгоритми пошуку дефектів у вигляді структурних дерев застосовуються в цифрових схемах при наявності двох умов:

1. Імовірність виникнення дефектів на всіх компонентах схеми приймається рівною.

2. Ціна елементарної перевірки у всіх контрольних точках (КТ) також приблизно однакова.

Для цифрових схем локальних пристроїв ці дві умови зазвичай дотримуються. Інша справа – мережа як об'єкт діагностування. Імовірність виникнення дефекту в пасивних компонентах (кабельна система) в умовах працюючої мережі вкрай мала.

Набагато більша ймовірність непрацездатності мережі через ПК (мережева карта – самий ненадійний компонент мережі), несправності мережного ПО, зазвичай пов'язані з невірними налаштуваннями. Ціна елементарної перевірки (ЕП) різна для кожного компонента мережі. Наприклад, перевірка кабельного сегмента, покладеного в важкодоступному місці, по трудомісткості набагато вище, ніж перевірка мережевої карти вбудованим програмним тестом при перекладі ПК в локальний режим.

ЕП з найнижчою ціною – це тестування ПК за мережевою адресою (ping), коли позитивним результатом є відгук ПК на ping (досяжність тестованого вузла), негативним – його відсутність (недосяжність). Виходячи з цього, є ідея використовувати методи пошуку дефектів, засновані на аналізі структури тестового пристрою.

Запропонований метод заснований на поєднанні МТН і аналізу структури об'єкта, представленої у вигляді безлічі вектор–списків матриці досяжності графа функціонально–гальванічних зв'язків. Побудова такого графа не складає труднощів, використання МТН дозволяє відмовитися від дорогої процедури зондового діагностування, а також скоротити область підозрюваних дефектів за мінімально можливий час. Однак мають місце високі витрати часу на моделювання несправностей, необхідне для побудови самої МТН. Більш того, побудова МТН для такого об'єкта як мережа – питання неоднозначне (не можна однозначно задати тип несправності і еталон контрольної точки / лінії), тому є ідея з'єднати метод структурного аналізу багатозначних ТН з використанням векторів експериментальної перевірки (ЗЕП) з методом структурного пошуку дефектів по матриця досяжності, де рядки матриці досяжними будуть використовуватися замість рядків ТН. Даний підхід дозволяє уникнути процедури моделювання, а також дозволяє перейти від тестового діагностування до функціонального, коли в якості тесту використовується адресний тест, а еталоном є позитивна реакція на тест (доступність тестового компонента).

Слід зазначити, що тут структурний метод застосовується в єдиному мережевому сегменті, що має на увазі єдиний адресний простір. Таким чином, об'єктом застосування структурного методу буде обчислювальна мережа на рівні ЛОМ.

Як КТ в цьому випадку будуть використовувати ПК мережі (нижче буде пояснено – чому), в якості тесту – ping за мережевою адресою всіх ПК з одного джерела тестів. Передбачається, що дефект впливає на всі трафіки, що проходять через несправний компонент, і компенсації виниклих дефектів у мережі немає. (При цьому передбачається, що джерело тестів свідомо справний). Вектор ЕП формується за всіма КТ, крім джерела тестів.

Вектор експериментальної перевірки (ВЕП) V – використовується для визначення технічного стану об'єкта по таблиці несправностей (ТН), де довжина ЗЕП дорівнює числу k вхідних тестових наборів, і Vi = 1, якщо реакція хоча б одного спостережуваного виходу об'єкта діагностування на і–м тестовому векторі відмінна від еталонної, а Vi = 0 – в іншому випадку.

В даному випадку, ВЕП використовується для визначення технічного стану ЛОМ як об'єкта діагностування по матриця досяжності, де довжина ВЕП дорівнює кількості компонентів мережі, на яких спостерігається реакція на тест.

Зауваження. Так як подача адресується тесту (ping) і спостереження реакції на нього виробляються на призначеному для користувача рівні, спостерігаються компонентами якого є ПК мережі, то буде достатнім формування ВЕП тільки з цих ПК, не беручи до уваги інші мережеві компоненти.

$V = \{V_1, \ldots, V_i, \ldots, V_n\}$ – вектор елементарної перевірки,

$i = 1, n$, де n – число ПК, крім джерела тестів;

$V_i=0$ – тест пройшов; $V_i=1$ – помилка.

Звідси:

$V_i = 0$ – мережа справна,

$V_i = 1$ – несправна кабельна система або головний концентратор (хаб, свіч).

$V_i=0$ – при позитивній елементарній перевірці; $V_i=0$ – при негативній елементарній перевірці.

Моделлю об'єкта діагностування вибирається ранжируваних граф структури мережевого сегмента, представлений у вигляді матриці досяжності.

Правила ранжирування графа:

1. Джерело тестів нумерується першим номером.

2. В порядку зростання нумерують приймачі тесту, крім термінальних вершин.

3. Нумеруються термінальні вершини.

У разі припущення наявності одиночного дефекту для знаходження області підозрюваних дефектів застосовується формула, яка зазвичай використовується для аналізу багатовиходових схем в структурному методі пошуку дефектів:

$$D = \bigcap M_j^{V_i=1} - \bigcup M_j^{V_i=0} \tag{2.1}$$

де Mj – рядок матриці досяжності, Vi = {0, 1} – значення ЗЕП після подачі тесту.

Потім для отриманої області застосовуються традиційні дерева з рівною ціною ЕП. У разі виникнення кратного дефекту в мережі (наприклад, дана ситуація природна в шинній топології), застосовується формула:

$$D = \bigcup M_j^{V_i=1} - \bigcup M_j^{V_i=0} \tag{2.2}$$

2.5 Опис діагностичного експерименту

Як джерело тестів вибирається один з комп'ютерів мережі, що володіє властивістю явної справності всіх його компонентів. На всі інші комп'ютери мережі надсилається адресний тест (ping), і за результатами його проходження заповнюється вектор експериментальної перевірки (ВЕП). Як було сказано раніше, діагностування мережі відбувається на так званому "призначеному для користувача" рівні (стан мережі та її компонентів відстежується на комп'ютерах–вузлах мережі), тому в безліч ЗЕП включають тільки ПК мережі (крім джерела тестів). У матриця досяжності входять всі компоненти, що тестується мережі, крім компонентів джерела тестів.

Розглянемо застосування зазначеної стратегії знаходження області підозрюваних дефектів в результаті проведення діагностичного експерименту в мережах Ethernet топологій "шина" (рис. 2.15) і деревовидної топології (див. рис. 1.8).

Експеримент 1. Для експерименту обрана невелика мережа Ethernet шинної топології з п'яти комп'ютерів (рис. 2.15).

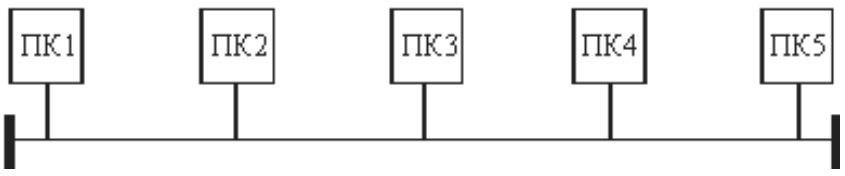


Рисунок 2.15 – Експериментальна шинна структура

У якості джерела тестів вибирається 1–й комп'ютер. Шинна топологія має на увазі вихід з ладу всієї мережі при наявності хоча б одного несправного сегмента кабелю (рис. 2.16).

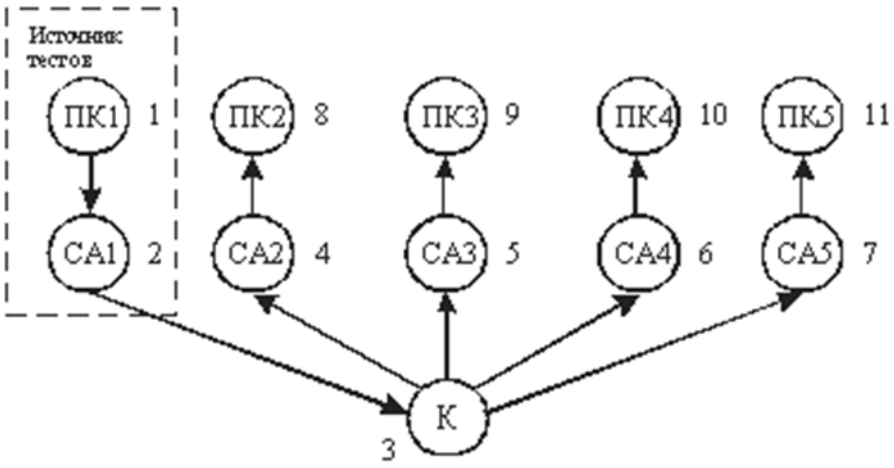


Рисунок 2.16 – Мережа Ethernet у вигляді графової моделі

ПКi – робоча станція, CAi – мережевий адаптер + (Т–коннектор BNC), К – кабельна мережа.

Побудована на основі мережі (рис. 2.17) матриця досяжності має наступний вигляд (рис. 2.3).

	3	4	5	6	7	8	9	10	11	V_i
3	1	.	.	.	.	.	.	.	.	V_3
4	1	1	.	.	.	.	.	.	.	V_4
5	1	.	1	.	.	.	.	.	.	V_5
6	1	.	.	1	.	.	.	.	.	V_6
7	1	.	.	.	1	.	.	.	.	V_7
8	1	1	.	.	.	1	.	.	.	V_8
9	1	.	1	.	.	.	1	.	.	V_9
10	1	.	.	1	.	.	.	1	.	V_{10}
11	1	.	.	.	1	.	.	.	1	V_{11}

Рисунок 2.17 – Матриця досяжності

ВЕП V = {8, 9, 10, 11};

Vi = 0 – мережа справна, Vi = 1 – присутня несправність.

Для визначення області підозрюваних дефектів застосуємо формулу (2.1):

V = {0, 0, 1, 0}, D = {3, 6, 10} – {3, 4, 5, 7, 11} = {6, 10} – несправний або ПК4 або його мережевий адаптер.

V = {1, 1, 1, 1}, D = {3} – виникнення дефекту в кабелі.

V = {0, 0, 1, 1}, D = {3} – {3, 4, 5, 8, 9} =∅ – кратна несправність, отже, за формулою (2.2):

V = {0, 0, 1, 1}, D = {3, 6, 7, 10, 11} – {3, 4, 5, 8, 9} = {6, 7, 10, 11} – несправні або мережеві карти 4–го і 5–го ПК, або самі ПК4 і ПК5.

Експеримент 2. Діагностичний експеримент буде проводитися на ЛОМ деревовидної топології, що складається з 6 комп'ютерів, 2 концентраторів і 1 комутуючого пристрою. На рис. 2.18 і 2.19 представлені, відповідно, сама ЛВС і її орієнтована графова модель у вигляді сукупностей тестових компонентів.

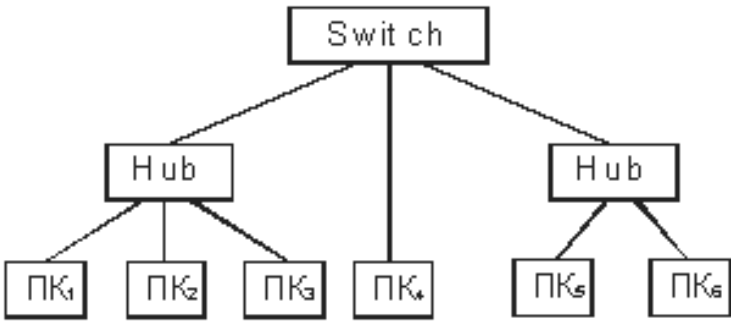


Рисунок 2.18 – Мережа Ethernet деревоподібної топології

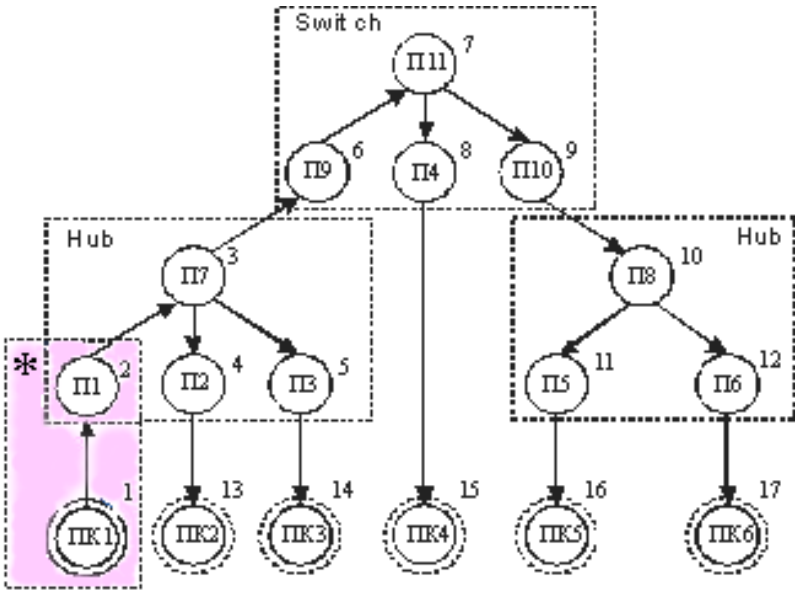


Рисунок 2.19 – Мережа Ethernet деревоподібної топології у вигляді графової моделі

Сукупність (ПК1, П1) представляє вузол – джерело тестів, що є попередньо справним.

Сукупність (ПКі, Пі) являє собою безліч (ПКі, САі, Кі, Пі), де ПКі – робоча станція, САі – мережевий адаптер, Кі – кабельний сегмент, Пі – порт концентратора / комутатора. Так як в якості тесту використовується тест адреси, то позитивна реакція від (ПКі, Пі), що складається у відгуку тестового вузла на ping, за замовчуванням має на увазі і позитивну реакцію від (САі, Кі). В іншому випадку, для подальшого пошуку дефекту будуть використовуватися інші види тестів, задані для кожного тестового компонента, що входить в сукупність, яка дала негативну реакцію.

Таким чином, з точки зору застосування структурного методу безлічі (ПКі, Пі) і (ПКі, САі, Кі, Пі) є такими, які не розрізняються, що призводить до скорочення розмірів таблиці досяжності.

Побудована таблиця досяжності має вигляд, що наведений на рис. 2.20.

	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	V_i
3	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	V_3
4	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	V_4
5	1	.	1	.	.	.	.	.	.	.	.	.	.	.	.	V_5
6	1	.	.	1	.	.	.	.	.	.	.	.	.	.	.	V_6
7	1	.	.	1	1	.	.	.	.	.	.	.	.	.	.	V_7
8	1	.	.	1	1	1	.	.	.	.	.	.	.	.	.	V_8
9	1	.	.	1	1	.	1	.	.	.	.	.	.	.	.	V_9
10	1	.	.	1	1	.	1	1	.	.	.	.	.	.	.	V_{10}
11	1	.	.	1	1	.	1	1	1	.	.	.	.	.	.	V_{11}
12	1	.	.	1	1	.	1	1	.	1	.	.	.	.	.	V_{12}
13	1	1	.	.	.	.	.	.	.	.	1	.	.	.	.	V_{13}
14	1	.	1	.	.	.	.	.	.	.	.	1	.	.	.	V_{14}
15	1	.	.	1	1	1	.	.	.	.	.	.	1	.	.	V_{15}
16	1	.	.	1	1	.	1	1	1	.	.	.	.	1	.	V_{16}
17	1	.	.	1	1	.	1	1	.	1	.	.	.	.	1	V_{17}

Рисунок 2.20 – Матриця досяжності для Ethernet деревоподібної топології

ВЕП V = {13, 14, 15, 16, 17}

Vi = 0 – мережа справна, Vi = 1 – присутня несправність.

Нехай V = {0, 0, 0, 1, 1}:

D = {2, 3, 6, 7, 9, 10} – {2, 3, 4, 5, 6, 7, 8, 13, 14, 15} = {9, 10};

Нехай V = {0, 0, 1, 0, 0}:

D = {2, 3, 6, 7, 8, 15} – {2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 16, 17} = {8, 15 }.

2.6 Ієрархія мережі і вибір типу тесту в залежності від рівня пошуку несправності

Корпоративна мережа являє собою складну ієрархічну структуру, яка поєднувала в собі різні мережеві технології, протоколи, топологічні реалізації, взаємодіючі на різних рівнях ієрархії.

Крім того, в більшості випадків структурно–логічна реалізація корпоративної мережі являє собою сукупність діючих окремо підмереж, що взаємодіють одна з одною тільки в міру необхідності. Така жорстка сегментація, здійснювана на практиці за допомогою мостів, комутаторів і маршрутизаторів, дозволяє уникнути проблем, пов'язаних з перевантаженістю мережі, за рахунок ізоляції міжсегментного трафіків.

Також, у разі виникнення несправності в сегменті, можна з великою ймовірністю стверджувати, що вона вплине на стан тільки того сегмента, в якому знаходиться даний несправний компонент (якщо він – не комутатор чи маршрутизатор; в такому випадку, його несправність буде впливати на всі сегменти, підключені до нього).

Сегментація мережі відповідає принципу вкладеності, тобто кожен сегмент може складатися з декількох під сегментів. Наприклад, мережа університету ділиться на підмережі кафедр, деканатів, відділів; в мережу кафедри входять мережі лабораторій при кафедрі, які також можуть включати в себе кілька сегментів.

У такій мережі при виникненні несправності доцільно проводити її пошук "зверху вниз": починаючи від рівня, на якому несправність проявляється у вигляді повідомлень про помилки і, закінчуючи рівнем, до якого безпосередньо належить несправний компонент.

Звідси видно, що на кожен з цих рівнів має подаватися тест, функціональність якого дозволить отримати достовірну інформацію про стан компонента на даному рівні. Так, для виявлення несправності на рівні корпоративної мережі слід використовувати аналізатор протоколів стандарту віддаленого доступу (наприклад, протокол SNMP), який дозволяє отримувати діагностичну інформацію від будь–якого вузла мережі, для мережі на рівні кафедри / відділу доцільно використовувати аналізатор протоколу, що працює в тому сегменті, в якому він встановлений, для пошуку несправності в мережевому адаптері – команда ping 127.0.0.1 і т.д.

Таким чином, простежується наступний ланцюжок: рівень спостереження несправності n> рівень n–1> рівень n–2> ...> рівень 1> мережевий компонент.

Виходячи з принципу вкладеності, під мережевим компонентом буде розумітися фізична/логічна структура, що є елементарною (примітивною) для розглянутої ієрархічної

рівня мережі. Наприклад, для ЛОМ лабораторії елементарними структурами є робочі станції, сервер, кабельна система, хаб; для ЛОМ кафедри – ЛОМ лабораторії і т.д.

Мережевий компонент 0–го рівня – це кінцеве мережевий пристрій (мережева карта, сегмент кабелю, коннектор і т.д.), неподільні на підрівні з точки зору діагностики мережі.

Слід звернути особливу увагу на кабельну систему, яка тут представлена окремим мережевим компонентом. Так як приблизно 90% мережевих проблем пов'язані саме з кабелями, то пошук несправностей треба починати саме з кабельної системи, використовуючи для цього відповідне тестове обладнання і методи пошуку дефекту.

Існує методологія діагностики мережі, звана "від низу до верху" і прив'язана до семи рівнів моделі OSI. Пошук несправності проводиться, починаючи з фізичного (нижнього) рівня і закінчуючи прикладним (верхнім) рівнем. Тут мережа розглядається як неподільний об'єкт, структура якого не залежить від її логіко–топологічної конфігурації і розміщення в просторі, ієрархічна ідентифікація відбувається на функціональному рівні (рівні протоколів), а не на структурно–логічному рівні (рівні сегментації). Звідси видно, що дану методологію можна використовувати на кожному з рівнів ієрархії мережі як засіб вибору тесту і методів пошуку дефекту для мережевого компонента будь–якого ієрархічного рівня.

2.7 Алгоритм побудови загальної моделі мережі

Як і цифровий пристрій, мережа як об'єкт діагностування повинна бути представлена у вигляді моделі (рис. 2.21)..

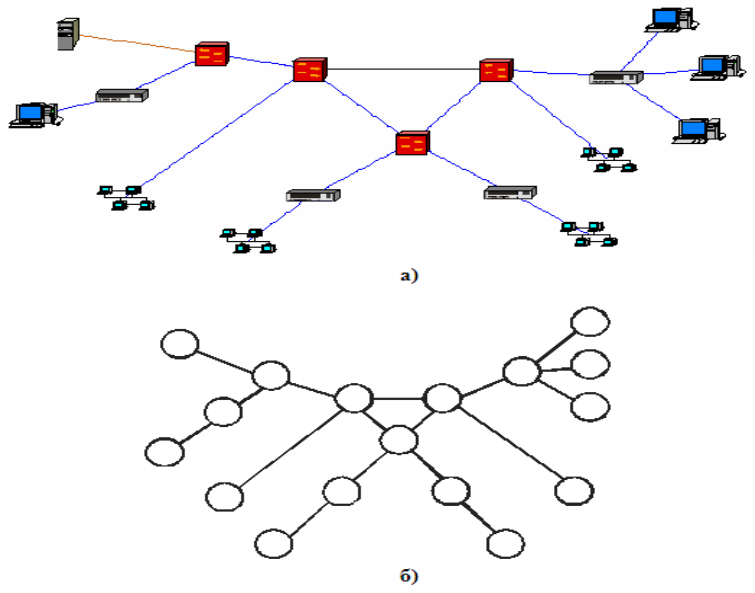


Рисунок 2.21 – Проект корпоративної мережі та її модель у вигляді графа

Так як одними з основних особливостей мережі є наявність адреси–джерела і адреси–приймача у будь–якого сигналу, що передається та доступність будь–якого мережевого компонента в якості точки контролю, то модель мережі зручно представити у вигляді графа G = {V, E}, де V – безліч вершин графа, що представляють собою безліч мережевих компонентів, E – безліч дуг графа, які задають відносини прийому / передачі діагностичної інформації між компонентами мережі.

Під діагностичною інформацією розуміється інформація, отримана в процесі подачі тестового впливу на той чи інший компонент мережі. Діагностичній інформації відповідає реакція мережі на тест.

Приклади діагностичної інформації: вимірювання параметрів, отримані за допомогою мережевого тестера, відомості з журналів відстеження аналізатора протоколів, відомості з консолі SNMP, таблиці маршрутизації, статистичні дані про роботу комутаторів і концентраторів, технічна документація та емпіричні спостереження користувачів мережі.

Графова модель мережі також відповідає принципу вкладеності, тобто будь–яку вершину, аж до компонента 0–го рівня, можна "розвернути" у вигляді підграфа, що є складним для n–1–го рівня і елементарним для n+1–го рівня. Таким чином, множина V містить в собі підмножини $\{v_n, v_{n-1}, v_{n-2}, \ldots v_1, v_0\}$, де n – вага ієрархічного рівня розглянутого компонента.

Безліч дуг графа E задає тільки відносини прийому/передачі інформації і може не збігатися зі структурою кабельної системи мережі. Кабельна система є компонентом мережі і задається у вигляді вершин графа. Причому структура моделі кабельної системи буде залежати від топологічної реалізації мережі і методів доступу до середовища. Доцільно будувати для кабельної системи окремий граф.

Тест для цифрового пристрою подається одночасно на всі його входи, а реакція на тест спостерігається на виходах пристрою. Однак, структурно–функціональні особливості мережі: поєднання каналів введення, передачі, перетворення і спостереження інформації на одному і тому ж мережевому компоненті, ієрархічна структура мережі, а також віддаленість контрольних точок в просторі (причому, чим вище рівень ієрархії, тим більше відстань між контрольними точками), призводять до ускладнення використання даного підходу стосовно моделі мережі.

Проблему подачі тесту на всі вузли мережі і спостереження реакції від них можна вирішити шляхом використання методів централізованого моніторингу корпоративної мережі, що широко використовуються в реальному житті (протокол SNMP, де має місце центральний вузол, який займається збором діагностичної інформації від вузлів–зондів). У

підмережах корпоративної мережі також можна використовувати аналізатор протоколів, тоді хост, на якому він встановлений, буде центральним з точки зору діагностування мережі.

Таким чином, в графовій моделі мережі необхідно виділити вузол, умовно названий діагностичним вузлом (початкова вершина графа), з якого буде виходити діагностичний трафік до кожного з решти вузлів мережі (кінцеві вершини графа) (рис. 2.22).

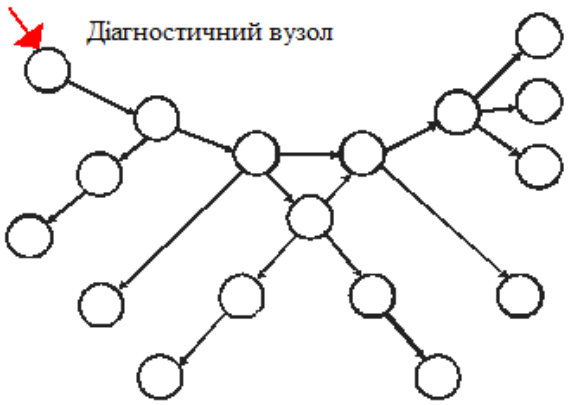


Рисунок 2.22 – Орієнтований однонаправлений граф

До отриманої моделі мережі можна застосовувати методи пошуку несправностей, відомі в технічній діагностиці. Зокрема, така модель є придатною для застосування до неї відомого структурного методу з побудовою дихотомічного дерева пошуку дефектів.

2.8 Модель мережі для пошуку дефектів структурним немодифікованим методом

Відповідно до методології "від низу до верху" даний метод буде застосовуватися на верхньому рівні моделі OSI, так як побудова графової моделі мережі, таблиці досяжності і дихотомічного дерева передбачає роботу додатка. Далі на етапі обробки контрольних точок можуть застосовуватися тести інших рівнів.

Для застосування структурного методу до графової моделі мережі вона повинна мати властивості орієнтованості (що їй притаманне завдяки наявності адреси–джерела і адреси–приймача у будь–якого сигналу, що передається) і однонаправленість. Однак, насправді діагностичний трафік в мережі є двонаправленим (від центрального діагностичного вузла надходить запит на інші вузли мережі про їх стан, на який кожен з вузлів шле необхідну інформацію). Тому з метою забезпечення однонаправленості графа

буде накладено обмеження на діагностичний трафік, згідно з яким відповідь на запит діагностичного вузла буде отриманий ним в будь–якому випадку (недоступність вузла, що діагностується, зважаючи на його несправність, також вважається реакцією на запит), і по тому ж маршруту, по якому був відправлений запит (рис. 2.22).

Для побудови таблиці досяжності необхідно виконати ранжування графа за таким правилом:

Перший номер призначається початковій вершині графа – діагностичному вузлу, потім нумеруються внутрішні вершини, що представляють собою мережеве обладнання корпоративної мережі, в останню чергу нумеруються кінцеві вершини (вузли) (рис. 2.23).

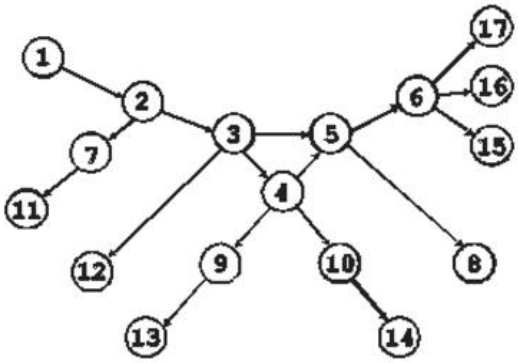


Рисунок 2.23 – Ранжирований граф

Далі побудова матриці досяжності для моделі мережі проводиться так само, як і для моделі ЦУ: в рядках матриці для кожної вершини графа "одиницями" відзначаються її вершини–попередники, а в стовпчиках, таким чином, будуть вказані вершини–наступники.

Так як в графовій моделі мережі присутні кілька кінцевих вершин (відповідних вузлів–приймачів діагностичного трафіку), то побудова дихотомічного дерева пошуку дефектів для моделі мережі повинно виконуватись так само, як і для цифровий схеми, що має багато виходів. Відповідно до алгоритму структурного методу проводиться розбиття графів на підграфи, кожен з яких відповідає заданим маршрутам діагностичного трафіку від діагностичного вузла до кожного з кінцевих вузлів мережі, причому одна і та ж вершина графа може входити в кілька підграфів (зазвичай така вершина являє собою комутатор або маршрутизатор). Потім для кожного з підграфів будується власна матриця досяжності і за матрицями будуються дихотомічні дерева.

Зважаючи на наявність в мережі маршрутизаторів може виникнути ситуація, коли трафік від діагностичного вузла до кінцевого вузла може пройти по одному маршруту, а повернутися – по іншому. Проходження по декількох маршрутах одночасно виключається

через функціонування в маршрутизаторах алгоритмів вибору найкоротшого шляху. Дана ситуація ускладнює пошук дефекту по дихотомічному дереву, так як несправний вузол може бути обійдений за іншим маршрутом, і через це елементарна перевірка на якомусь етапі просування по дереву дасть позитивний результат замість негативного. Однак, обмеження, накладене раніше на графову модель мережі (двунаправленна фіксованість маршруту діагностичного трафіку, що забезпечує однонаправленість графа), буде діяти і при розбитті графа на підграфи і надалі побудові дихотомічного дерева, що дозволить уникнути згаданої ситуації.

Таким чином, якщо в мережі може існувати кілька маршрутів діагностичного трафіку від діагностичного вузла до кінцевого вузла, при побудові моделі мережі необхідно вибрати найкоротший маршрут (за кількістю внутрішніх вершин між вузлом–джерелом і вузлом–приймачем тесту) і будувати дихотомічне дерево з урахуванням цього маршруту, виключаючи з розгляду інші (рис. 2.24).

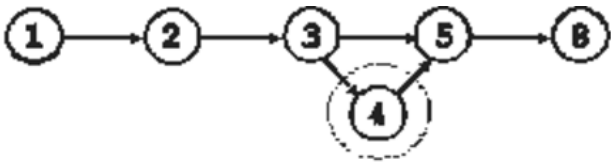


Рисунок 2.24 – Виключення маршруту (1–2–3–4–5–8) и перевага маршруту (1–2–3–5–8) як найкоротшого

2.9 Проведення діагностичного експерименту

Для проведення діагностичного експерименту в якості прикладу виберемо підграф з діагностичним трафіком (1–2–3–4–10–14) (рис. 2.25а, б) і побудуємо для нього матрицю досяжності і дихотомічне дерево (рис. 2.26а, б).

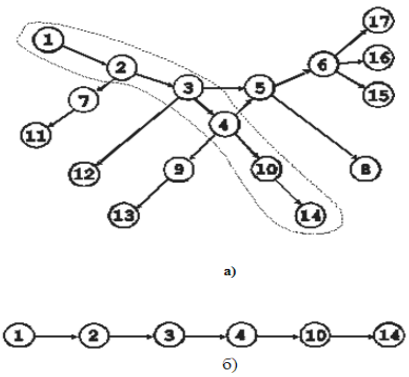


Рисунок 2.25 – Підграф з заданим діагностичним трафіком

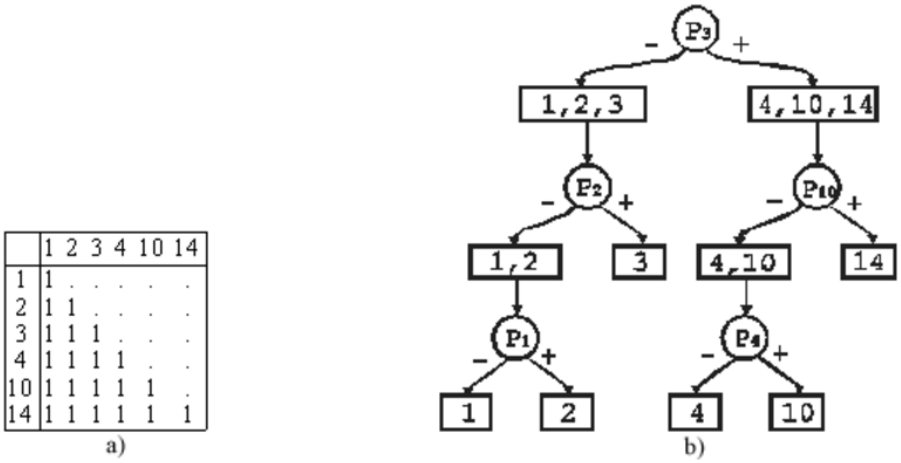


Рисунок 2.26 – Матриця досяжності (а) та дихотомічне дерево (б)

Внесемо несправність на мережевий компонент № 4 і виберемо будь–яке з дихотомічних дерев, в яке входить даний компонент (рис. 2.27)

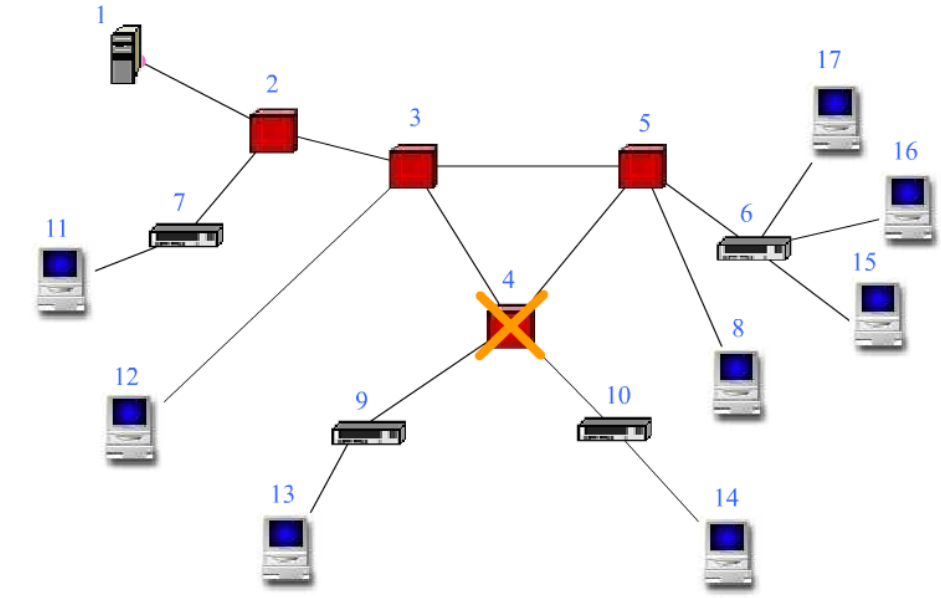


Рисунок 2.27 – Несправний комутатор (Switch)

На рисунку 2.12 представлені пристрої мережі: 2–5 – комутатори; 6,7, 9, 10 – концентратори; 1,8, 11–17 – робочі станції

Так як у нас вже є побудоване дерево для трафіку (1–2–3–4–10–14), то будемо використовувати його. Отже, перша експериментальна перевірка виявилася позитивною (вузол № 3 доступний з діагностичного вузла), тому рухаємося по правій гілці. Друга перевірка дала негативний результат (вузол № 10 недоступний), і тому переходимо на ліву гілку до області підозрюваних дефектів (4, 10). Наступна перевірка, – в вузлі №4, – дала також негативний результат, що і дозволило нам виявити несправність компонента №4.

2.10 Висновки до розділу 2

В другому розділі магістерської роботи розглянуті типові несправності комп'ютерної мережі побудованої на кабельних та волоконно-оптичних лініях зв'язку, розподіл несправностей у бездротових мережах, структурний метод пошуку дефектів, опис діагностичного експерименту, ієрархія мережі і вибір типу тесту в залежності від рівня пошуку несправності та алгоритм побудови загальної моделі мережі

Визначено, що в мережі може існувати кілька маршрутів діагностичного трафіку від діагностичного вузла до кінцевого вузла, при побудові моделі мережі необхідно вибрати найкоротший маршрут (за кількістю внутрішніх вершин між вузлом–джерелом і вузлом–приймачем тесту) і будувати дихотомічне дерево з урахуванням цього маршруту, виключаючи з розгляду інші.

РОЗДІЛ 3

ДОСЛІДЖЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДІАГНОСТИКИ МЕРЕЖІ

3.1 Перевірка підключення до мережі за допомогою exo-запиту команди ping

Програмне забезпечення для трасування маршруту - це утиліта, яка містить списки мереж, по яким повинні пройти дані від відправника кінцевого пристрою користувача до віддаленої мережі призначення.

Зазвичай цей мережевий інструмент виконується в командному рядку як

tracert <destination network name or end device address>

(Операційні системи Microsoft Windows)

або

traceroute <destination network name or end device address>

(Для Unix і подібних систем)

Утиліти трасування маршруту дозволяють визначати шляхи або маршрути, а також обчислювати час затримки в IP-мережі. Для виконання цієї функції існує кілька засобів.

Інструмент traceroute (або tracert) часто використовується для пошуку та усунення неполадок в мережі. З його допомогою можна відобразити список пройдених маршрутизаторів і визначити, який шлях використовувався для досягнення певного пункту призначення в одній мережі або переходу між декількома мережами. Кожен маршрутизатор є точкою, в якій одна мережа з'єднується з іншою і через яку пересилається пакет даних. Кількість маршрутизаторів називається кількістю «переходів», скоєних даними на шляху від джерела до місця призначення.

В результаті виконання команди відображається список, що дозволяє виявити проблеми з потоком даних, які можуть виникати при спробі доступу до сервісу, наприклад до веб-сайту. Також список може стати в нагоді при виконанні таких завдань, як завантаження даних. Якщо для одних і тих же даних доступні кілька сайтів (дзеркал), то можна прокладати шлях до кожного дзеркала, щоб визначити, який з них є найбільш швидким у використанні.

Дві траси маршруту, виконані між одними і тими ж вузлами джерела і адресата в різний час можуть дати різні результати. Це може бути пов'язано з «повнозв'язаним» характером взаємно підключених мереж, що складаються з можливостей Інтернету і протоколів Інтернету вибирати різні канали зв'язку для відправки пакетів.

Засоби трасування маршруту с використанням командного рядка звичайно закладені в операційну систему кінцевого пристрою.

Інші інструменти, такі як VisualRoute ™, є пропрієтарними програмами і дозволяють отримувати більш детальну інформацію. VisualRoute формує графічне відображення маршруту, використовуючи доступну інформацію в мережі.

Для виконання даної роботи необхідна програма VisualRoute, яку можна завантажити за посиланням http://www.visualroute.com/download.html.

Для перевірки трасування маршруту до віддаленої мережі ПК повинен мати підключення до Інтернету та скористатись інструментом відправки ехо-запитів командою ping. Відправка луна-запитів за допомогою команди ping дозволяє перевірити доступність вузлів. Пакети даних відправляються на віддалений вузол для отримання відповіді. Ваш локальний ПК визначає, отриманий

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Рисунок 3.1 – Результат виконання команди ping

Аналізуючи результат виконання команди ping можна визначити час проходження пакетів, що визначає швидкодію вузла в мілісекундах.

У першому рядку отриманих даних відображається повне доменне ім'я (Full Qualified Domain Name, FQDN) e144.dscb.akamaiedge.net. Потім слід IP-адреса 23.1.48.170. Для прикладу обрано веб-сайт компанії Cisco.

Веб-сайти компанії Cisco містять одну і ту ж інформацію, розміщуються на різних серверах (так званих дзеркалах) по всьому світу. Це означає, що ім'я FQDN і IP-адреса будуть відрізнятися в залежності від вашого місцезнаходження.

На рис. 3.2 наведена статистика вузла.

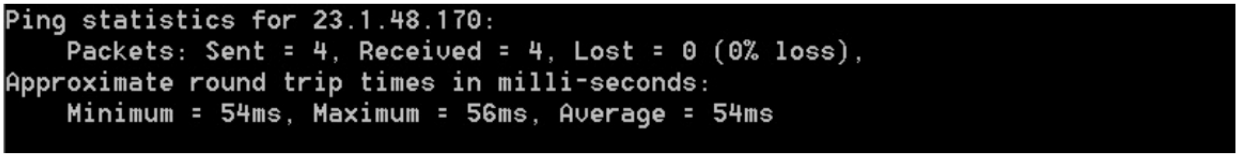


Рисунок 3.2 – Статистика вузла

З результатів видно, що були відправлені чотири ехо-запити за допомогою команди ping, на кожен з яких була отримана відповідь. Відповідь надійшла на все ехо-запити за допомогою команди ping, значить, втрати пакетів немає (0% втрат). В середньому для передачі пакетів по мережі потрібно 54 мс.

Від втрати пакетів або повільного з'єднання з мережею першу чергу страждає якість потокового відео і онлайн-ігор. Щоб визначити швидкість інтернет-підключення більш точно, можна відправити не 4 ехо-запити за допомогою команди ping, передбачених за замовчуванням, а 100. Для цього використовується зазначена нижче команда.

C:\ping –n 100 www.cisco.com

Результат виконання команди буде виглядати наступним чином (рис. 3.3):

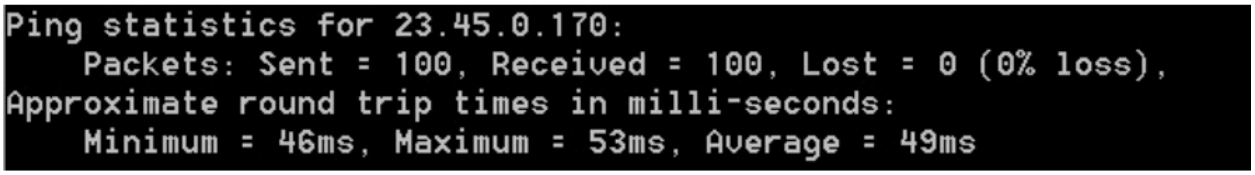


Рисунок 3.3 – Результат виконання команди на 100 ехо-запитів

Дослідження показують, що чим далі розташовані вузли між собою, тим більший час проходження повідомлень між ними (рис. 3. 4).

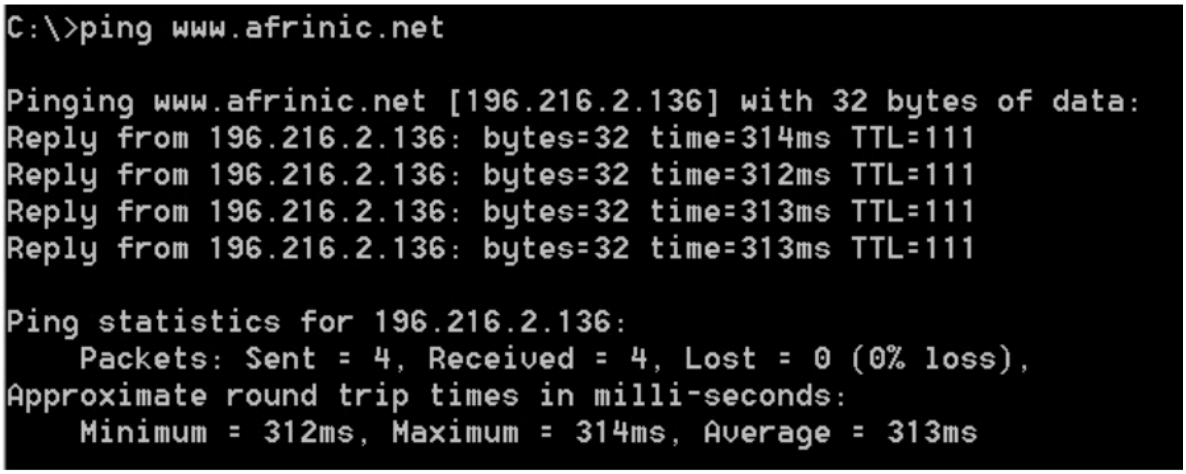


Рисунок 3.4 – Проходження повідомлень між віддаленими вузлами

При недоступності вузла йде втрата пакетів (рис. 3.5).

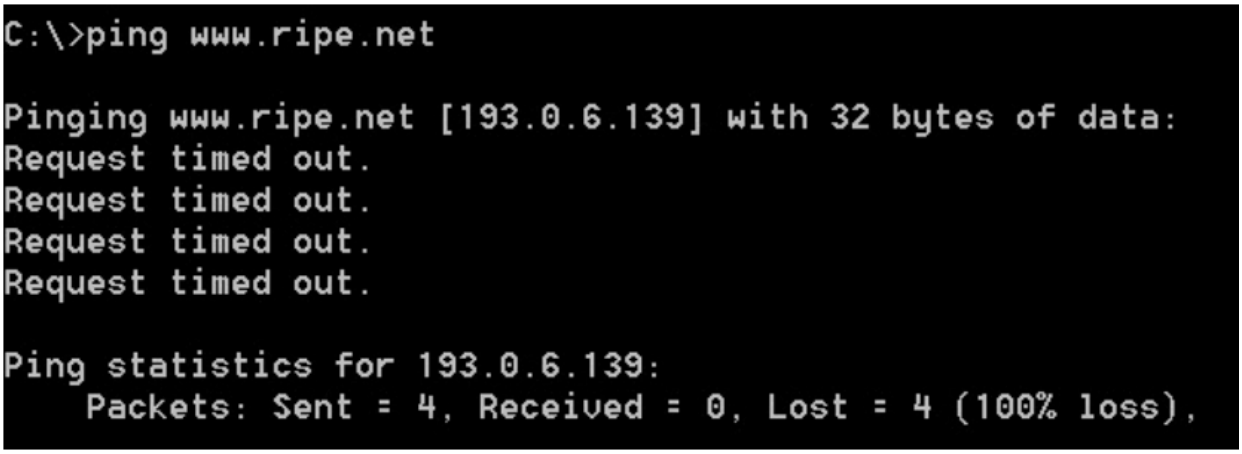


Рисунок 3.5 – Втрата пакетів під час передачі при недоступності вузла

3.2 Трасування маршруту до віддаленого сервера за допомогою команди tracert

Для більш детального дослідження мережі після виконання команди *ping* слід скористатись командою *tracert*, яка набирається у командному рядку. Результат її виконання має наступний вигляд представлений на рис. 3.6.

Рисунок 3.6 – Результат виконання команди *tracert*

Залежно від зони охоплення інтернет-провайдера і розташування вузлів джерела і призначення маршрути можуть перетинати безліч переходів і мереж. Кожен перехід - це

один маршрутизатор. Маршрутизатор представляє собою технічний засіб, який використовується для перенаправлення трафіку через Інтернет.

Оскільки комп'ютери використовують мову цифр, а не слів, маршрутизаторів присвоюються унікальні IP-адреси (номери в форматі x.x.x.x). Утиліта tracert показує, яким шляхом проходить пакет даних до кінцевого пункту призначення. Крім того, за допомогою утиліти tracert можна визначити, з якою швидкістю проходить трафік через кожен сегмент мережі. Кожному маршрутизатору на шляху проходження даних відправляються три пакети, час відповіді на які вимірюється в мілісекундах. Використовуючи дану інформацію, можна проаналізувати результати, отримані за допомогою утиліти tracert при відправці пакетів до www.cisco.com. Нижче представлений весь маршрут трасування (рис. 3.7).

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Рисунок 3.7 – Маршрут трасування

На рис. 3.8 наведена деталізація маршруту.

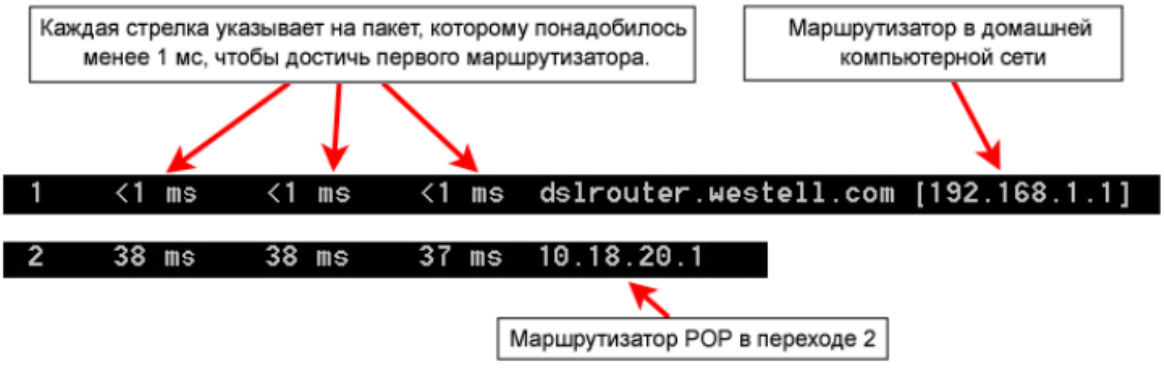


Рисунок 3.8 – Деталізація маршруту

У наведеному вище прикладі пакети, відправлені за допомогою утиліти tracert, пересилаються з ПК джерела на основний шлюз локального маршрутизатора (перехід 1: 192.168.1.1), а потім на маршрутизатор в точці підключення (Point of Presence, POP) до інтернет-провайдера (перехід 2:10.18.20.1). У кожного провайдера є безліч маршрутизаторів POP. Вони відзначають кордони мережі інтернет-провайдера і служать точками підключення до Інтернету для клієнтів. Пакети передаються по мережі компанії Verizon, перетинають два переходи і потрапляють в маршрутизатор, який належить alter.net. Це може означати, що пакети досягли іншого інтернет-провайдера.

Цей момент дуже важливий, оскільки при пересиланні пакетів від одного провайдера до іншого провайдеру можливі втрати. Також важливо пам'ятати, що не всі інтернет-провайдери здатні забезпечити однакову швидкість передачі даних. Як визначити, чи є alter.net тим же самим або іншим інтернет-провайдером?

Існує інтернет-сервіс whois, за допомогою якого можна дізнатися власника доменного імені. Веб-інструмент whois (інформаційна служба) доступний за адресою

http://whois.domaintools.com/. Згідно з інформацією, отриманою за допомогою whois, домен alter.net також належить компанії Verizon (рис. 3.9).

Рисунок 3.9 – Інформація від домена alter.net

Таким чином, інтернет-трафік «починається» на домашньому ПК і проходить через домашній маршрутизатор (перехід 1). Потім він підключається до інтернет-провайдера і передається по його мережі (переходи2-7), поки не досягне віддаленого сервера (перехід 8). Це досить нетиповий приклад, в якому від початку до кінця задіяний тільки один провайдер. Як видно з наступних прикладів, найчастіше в пересиланні даних беруть участь два і більше інтернет-провайдерів.

Розглянемо приклад з пересилкою інтернет-трафіку через кілька інтернет-провайдерів. Нижче наведені результати застосування утиліти tracert до вузла www.afrinic.net (рис.3 10).

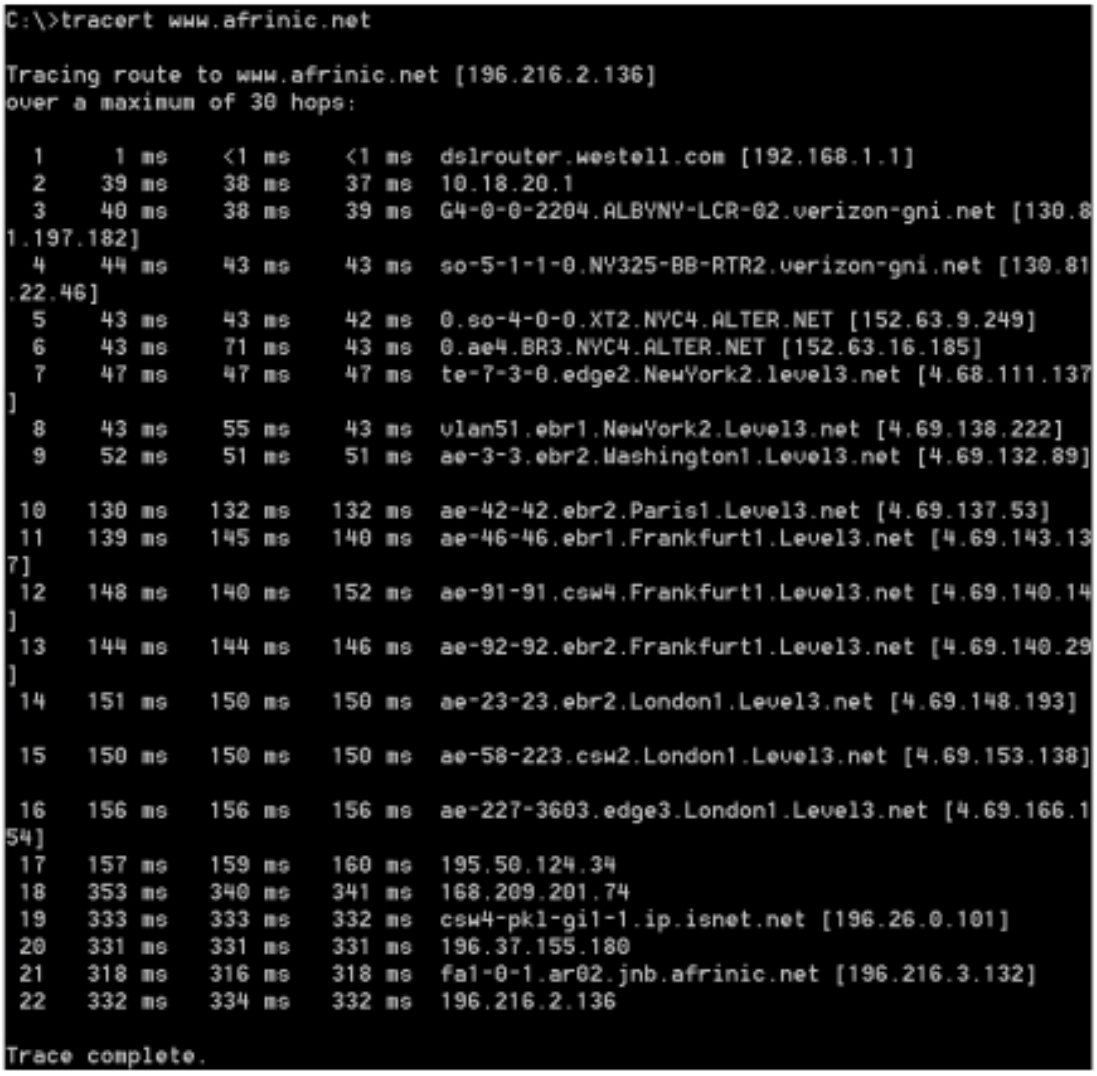


Рисунок 3.10 – Результати застосування утиліти tracert до вузла www.afrinic.net

3.3 Відстеження маршруту до віддаленого сервера за допомогою програмних і веб-засобів

VisualRoute- це пропріетарна програма, що дозволяє наочно відобразити результати трасування маршруту.

VisualRoute - програма об'єднує в собі функціональність декількох утиліт, які здійснюють пінгування, опитування і відстежування шляхів передачі пакетів до серверів, але на відміну від інших програм відображає всю інформацію в доступному до сприйняття графічному вигляді. VisualRoute автоматично аналізує проблеми з з'єднанням і швидкодією передачі даних, потім відображає отримані результати у вигляді легко-яку читає таблиці, а також показує шляху проходження пакетів на світовій карті. На додаток

до цього VisualRoute має можливість ідентифікувати географічне положення роутерів, серверів та інших мережевих пристроїв по IP-адресами (рис. 3.11).

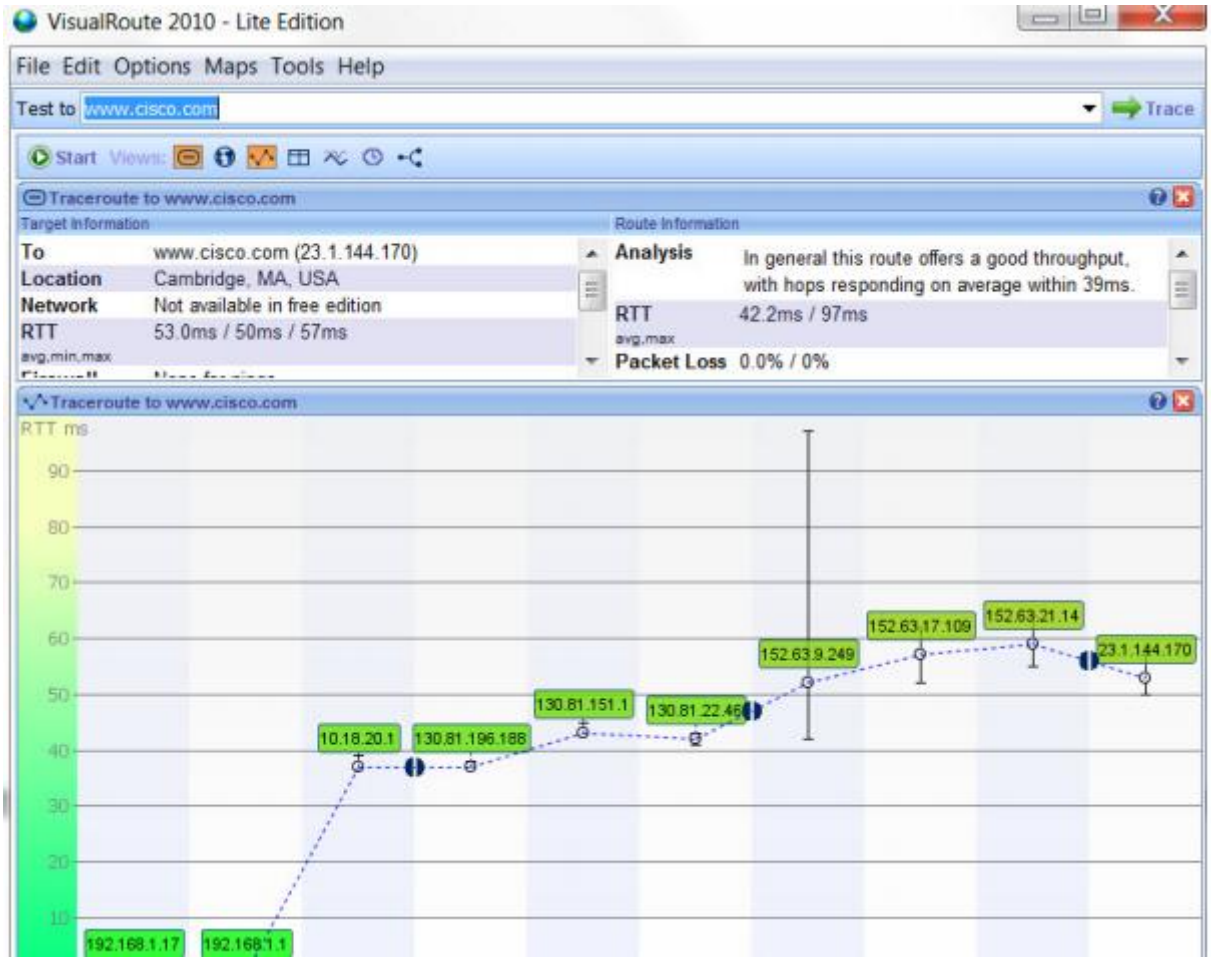


Рисунок 3.11 – Ідентифікація положення роутерів, серверів та інших мережевих пристроїв по IP-адресами

3.4 Використання програми Packet Tracer

Packet Tracer - симулятор мережі передачі даних, що випускається фірмою Cisco Systems (рис. 3.12). Дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори і комутатори, взаємодіяти між декількома користувачами (через хмару). У симуляторі реалізовані серії маршрутизаторів Cisco 800, 1800, 1900, 2600, 2800, 2900 і комутаторів Cisco Catalyst 2950, 2960, 3560, а також міжмережевий екран ASA 5505. Бездротові пристрої представлені маршрутизатором Linksys WRT300N, точками доступу і стільниковими вишками. Крім того є сервери DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP і EMAIL, робочі станції, різні модулі до

комп'ютерів і маршрутизаторів, IP-фони, смартфони, хаби, а також хмара, що емулює WAN. Об'єднувати мережеві пристрої можна за допомогою різних типів кабелів, таких як прямі і зворотні пасивні, оптичні і коаксіальні кабелі, послідовні кабелі та телефонні пари.

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

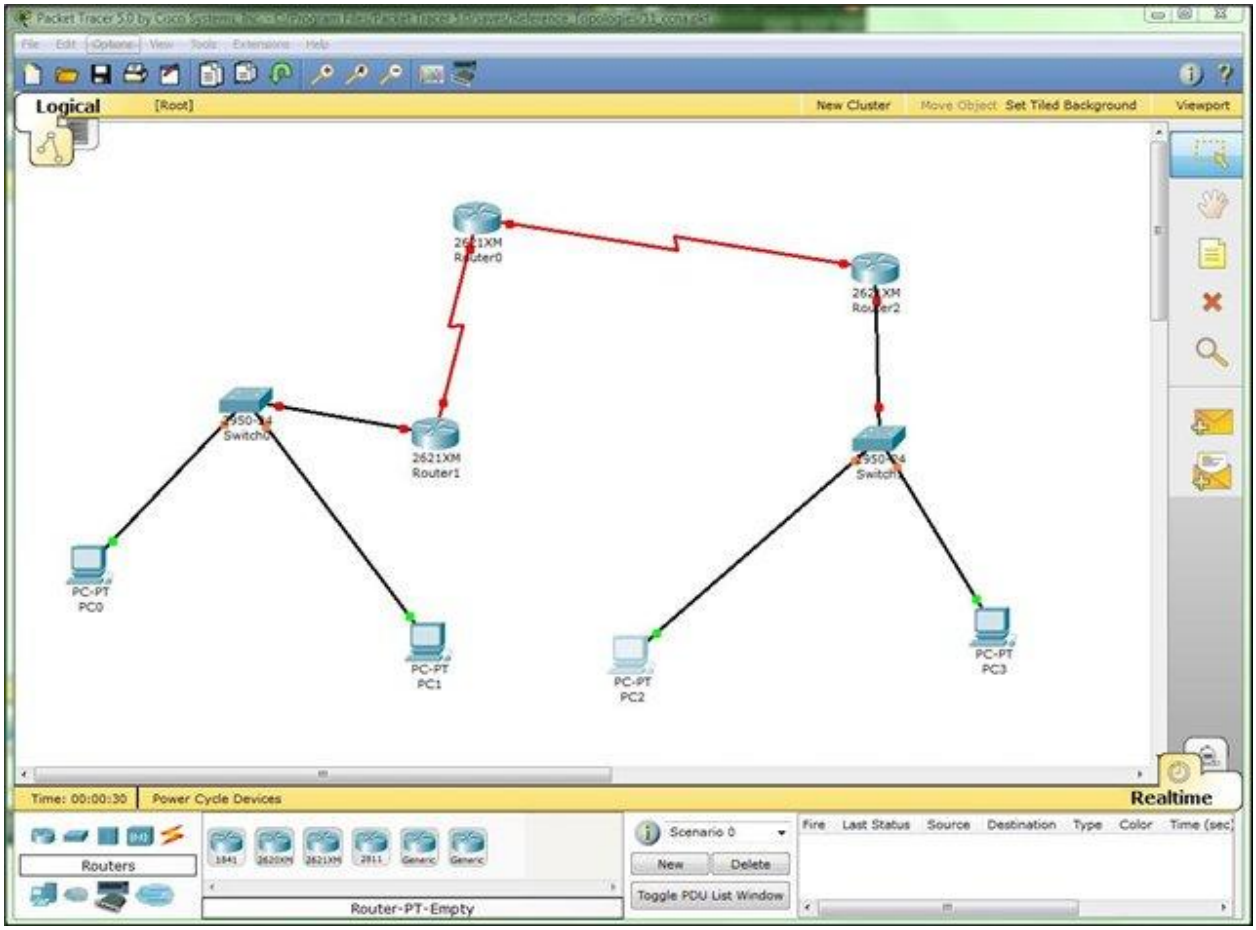


Рисунок 3.12 – Загальний вигляд програми Packet Tracer

3.5 Висновки до розділу 3

У третьому розділі магістерської роботи проведено дослідження застосування мережевих утиліт для перевірки функціонування мережі.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно–побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В [23] визначається, що охорона праці – це система правових, соціально–економічних, організаційно–технічних, санітарно–гігієнічних і лікувально–профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

Завданням даної магістерської роботи було дослідити методи виявлення несправностей в комп’ютерних мережах. Дана робота з точки зору питань з охорони праці проводилась в офісному приміщенні при нормальних кліматичних умовах з використанням сучасного персонального комп’ютера та офісної техніки (принтера та сканера).

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Повітря забруднюється шкідливими хімічними речовинами антропогенного походження за рахунок деструкції полімерних матеріалів, які використовуються для обробки приміщень та обладнання. Неправильна організація робочого місця сприяє загальному і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, викривлення хребта і розвитку остеохондрозу. На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно–побутові умови повинні відповідати вимогам нормативних актів про охорону праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно–гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Він не має права вимагати від працівника виконання роботи, поєднаної з явною небезпекою для життя, а також в умовах, що не відповідають законодавству про охорону праці. Працівник має

право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я або людей, які його оточують, і навколишнього середовища.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Державна політика в галузі охорони праці визначається відповідно до Конституції України Верховною Радою України і спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням. Відповідно до статті 3 [23] законодавство про охорону праці складається з [24, 25] та прийнятих відповідно до них нормативно–правових актів, норм міжнародного договору (ратифіковані Конвенції і Рекомендації МОТ, директиви Європейської Ради).

На законодавчому рівні визначено такі пріоритетні напрямки з безпеки праці:

– кожен працівник несе безпосередню відповідальність за порушення зазначених Законом, нормами і правилами вимог;

– напрямки реалізації конституційного права громадян на їх життя і здоров’я в процесі трудової діяльності:

– пріоритет життя і здоров’я працівників по відношенню до результатів виробничої діяльності підприємства;

– повна відповідальність роботодавця за створення належних – безпечних і здорових умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– комплексне розв’язання завдань охорони праці;

– підвищення рівня промислової безпеки шляхом забезпечення суцільного технічного контролю за станом виробництв, технологій та продукції, а також сприяння підприємствам у створенні безпечних та нешкідливих умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– використання економічних методів управління охороною праці, участь держави у фінансуванні заходів щодо охорони праці;

– використання світового досвіду організації роботи щодо поліпшення умов і підвищення безпеки праці на основі міжнародної співпраці.

Користувачі персональних комп'ютерів, для яких ця робота є головною, підлягають медичним оглядам: попереднім — під час влаштування на роботу і періодичним — протягом професійної діяльності раз на два роки. Жінок з часу встановлення вагітності та в період годування дитини грудьми до роботи з ПК не допускають.

Обов'язки працівників щодо додержання вимог нормативно–правових актів з охорони праці (ст. 14), відповідальність робітників всіх категорій за порушення вимог щодо охорони праці (ст. 44) та структура організації/виробництв системи управління охорони праці визначені безпосередньо «Інструкцією на робоче місце № 1», та іншими затвердженими власними нормативними актами з питань охорони праці (правилами, нормами, регламентами, положеннями, стандартами, інструкціями та іншими документами, обов'язковими до виконання), тобто тих, що діють на підприємстві/організації, і визначені в [26].

Наявні трудові відносини між працівниками і роботодавцями в Україні за темою роботи регулюються [24], відповідно до якого права працюючої людини на охорону праці охороняються всебічно та норми охорони праці неухильно інтегровані до правил внутрішнього розпорядку організації/підприємства.

4.1.2 Організаційно–технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог [27], затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511.

Також впроваджені організаційні заходи з пожежної безпеки – навчання і перевірку знань відповідно до вимог [28], затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 29.09.2003 N 368, зареєстрованого в Міністерстві юстиції України 11.12.2003 за N 1148/8469.

Обов'язковими вимогами враховане наступне:

– не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки та цих Правил.

– на підприємстві/організації, де експлуатуються ПК з ВДТ і ПП, розробляється інструкція з охорони праці відповідно до [29], затвердженого наказом

Держнаглядохоронпраці від 29.01.98 N 9, зареєстрованого в Міністерстві юстиції України 07.04.98 за N 226/2666.

–ознайомлення з правилами безпеки праці, одержання відповідних інструктажів засвідчується у журналі інструктажів.

–перед допуском до самостійної роботи кожен працівник має право на навчання з питань охорони праці і роботодавець зобов'язаний, і проводить таке навчання у вигляді двох інструктажів з питань охорони праці:

1. Вступного, який проводять працівники служби охорони праці об'єкта господарювання з усіма працівниками, яких приймають на роботу незалежно від їхньої освіти та стажу роботи за програмою, в якій подають загальні питання охорони праці із врахуванням її особливостей на об'єкті господарювання;

2. Первинного, який проводять керівники структурних підрозділів на місці праці з кожним працівником до початку їхньої роботи на цьому робочому місці.

Проходження працівником цих інструктажів з питань охорони праці підтверджується записами у відповідних журналах обліку інструктажів і скріплюється підписами осіб, які проводили інструктажі та осіб, які отримали інструктажі.

3. Повторний (не рідше одного разу в 6 місяців);

4. Позаплановий (при зміні правил охорони праці);

5. Поточний (проводять з працівниками перед виконанням робіт, на яких оформляється наряд–допуск)

– обов'язкові організаційні заходи перед початком, під час і після завершення роботи повинні включати перевірку (візуально) наявності і справності електрообладнання та його заземлення, а під час виконання роботи вимогу «не залишати без нагляду обладнання, яке працює». Після закінчення роботи – вимагається прибирання робочого місця, відключення всіх електроприладів від електромережі.

Не допускається:

– виконувати обслуговування, ремонт та налагодження ПК з ВДТ і ПП безпосередньо на робочому місці оператора;

– зберігати біля ПК з ВДТ і ПП папір, дискети, інші носії інформації, запасні блоки, деталі тощо, якщо вони не використовуються для поточної роботи;

– відключати захисні пристрої, самочинно проводити зміни у конструкції та складі ПК з ВДТ і ПП або їх технічне налагодження;

–працювати з ВДТ, у яких під час роботи з'являються нехарактерні сигнали, нестабільне зображення на екрані тощо;

– працювати з матричним принтером за відсутності вібраційного килимка та зі знятою (піднятою) верхньою кришкою.

4.2 Аналіз стану умов праці

4.2.1 Вимоги до приміщень

Робота над створенням такої системи проходитиме в приміщенні відповідної установи (компанії, підприємстві тощо). Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером. ГПКетричні розміри приміщення зазначені в таблиці 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	5
Висота, м	3
Площа, $м^2$	25
Об'єм, $м^3$	75

Згідно з [30] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам. Для зручності спільної роботи з іншими працівниками (обговорення ідей, з'ясування проблем і т.д.) в кімнаті є дивани і журнальний стіл, обставлені живими квітами. Також робочий процес пов'язаний з багатьма документами, теками, журналами для чого приміщення облаштоване принтером і шафою для зручності. Задля дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціонування. Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця [31] і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність в таблиці 4.2.

Таблиця 4.2 – Характеристики робочого місця

Найменування параметра	**Фактичне значення**	**Нормативне значення**
Висота робочої поверхні, мм	750	680 ÷800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷800

Робочий стіл на досліджуваному місці також містить достатньо простору для ніг. Крісло, що використовується в якості робочого сидіння, є підйомно–поворотним, має підлокітники і можливість регулювання за висотою і кутом нахилу спинки, також воно м'яке і виконане з екологічної шкіри, що дає можливість працювати у комфорті. Екран монітору знаходиться на відстані 0.8 м, клавіатура має можливість регулювання кута нахилу 5–15°. Отже, за всіма параметрами робоче місце відповідає нормативним вимогам.

Приміщення кабінету знаходиться на другому поверсі трьох поверхової будівлі і має об’єм 78 м^3, площу — 18 м^2. У цьому кабінеті обладнано три місця праці, з яких два укомплектовані ПК.

Температура в приміщенні протягом року коливається у межах 18–24°С, відносна вологість — близько 50%. Швидкість руху повітря не перевищує 0,2 м/с. Шум на робочому місці знаходиться на рівні 50 дБА. Система вентилювання приміщення — природна неорганізована, а опалення — централізоване.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою восьми люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

У кабінеті є електрична мережа з напругою 220 В, яка створює небезпеку ураження електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин (часток тонеру, оксидів нітрогену та озону).

За ступенем пожежної безпеки приміщення належить до категорії В. Кабінет має бути оснащений переносним вуглекислотним вогнегасником ВВК–5.

Наявна аптечка для надання долікарської допомоги, а також у кабінеті роблять вологе прибирання та щоденно провітрюють приміщення.

4.2.3 Навантаження та напруженість процесу праці

Як приклад наведено опис процесу праці оформлення роботи під час виконання магістерської роботи за фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організації роботи, то розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово–психічної напруги виконання роботи можна віднести до II – III ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Під час виконання робіт використовують ПК та периферійні пристрої, що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м’язово скелетна система, нервово–психічна діяльність, репродуктивна функція у жінок.

Тобто наявне психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

– статичного;

– динамічного;

б) нервово–психічного перевантаження:

– розумового перенапруження;

– монотонності праці;

– перенапруження аналізаторів;

– емоційних перевантажень.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви:

– для розробників програм тривалістю 15 хв. через кожну годину роботи.

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3.1 Аналіз небезпечних та шкідливих факторів при роботі на ПК

Роботу, пов'язану з персональним комп’ютером (далі – ПК) з відео дисплейними терміналами (далі – ВДТ), у тому числі на тих, які мають робочі місця, обладнані ПК з ВДТ і периферійними пристроями (далі – ПП), виконують із забезпеченням виконання [32], які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ПК з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої.

Робочі місця мають відповідати вимогам [31, 32].

Це передбачає, що визначена виробнича діяльність пов’язана з наявністю певної кількості небезпечних та/або шкідливих виробничих факторів. Тому у першій частині цього підрозділу за результатами аналізу повинні бути визначені такі фактори.

Робота ПК та периферійних пристроїв супроводжує виділення багатьох хімічних речовин, зокрема озону, оксидів нітрогену та аерозолів (високодисперсних частинок тонера). Для прикладу, за умов роботи з ПК виникають наступні небезпечні та шкідливі

чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами (джерелом яких може бути принтер, сканер та ін.), шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3).

Таблиця 4.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
фізичні			
– підвищена температура поверхонь обладнання	Експлуатація ПК	2	ДСН 3.3.6.042–99
– підвищений рівень шуму на робочому місці	Система охолодження ПК	2	ДСН 3.3.6.037–99
– підвищений рівень вібрації	Система охолодження ПК, привід	2	ДСН 3.3.6.039–99 ДСТУ ГОСТ 12.1.012–90
– недостатність природного світла	Порушення умов праці (вимог до приміщень)	2	ДБН В.2.5–28:2015
– недостатнє освітлення робочої зони	Порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5–28:2015
– підвищена яскравість світла	Порушення умов праці (організації місця праці– налагодження моніторів)	1	ДСанПіН 3.3.2.007–98
психофізіологічні:			
– нервово–психічна перевантаження (розумове, перенапруження аналізаторів–зорових)	– пошук інформації для постановки теми; – пошук та аналіз аналогів і літератури; – пошук наявних технологій,	4	НПАОП 0.00–1.28–10 ДСанПіН 3.3.2.007–98

	моделювання та аналіз алгоритмів; – виконання роботи за темою диплома, тестування; – оформлення роботи		
– фізичні (статичне – сидіння)	порушення умов праці (організації місця праці– сидіння користувача,) та організації робочого часу – безпервна робота)	2	НПАОП 0.00–1.28–10 ДСанПіН 3.3.2.007–98

4.3.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ПК, вентиляції і кондиціювання. Небезпека загоряння пов'язана з особливістю комп'ютерів – із значною кількістю щільно розташованих на монтажній платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Надійна робота окремих елементів і мікросхем в цілому забезпечується тільки в певних інтервалах температури, вологості і при заданих електричних параметрах. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Висока щільність елементів в електронних схемах призводить до значного підвищення температури окремих вузлів (80…100 ℃). При проходженні електричного струму по провідниках і деталей виділяється тепло, що в умовах їх високої щільності може привести до перегріву, і може служити причиною запалювання ізоляційних матеріалів. Слабкий опір ізоляційних матеріалів дії температури може викликати порушення ізоляції і привести до короткого замикання між струмоведучими частинами обладнання (шини, електроди). Також ймовірна небезпека внаслідок перевантаження напруги, розрядки зарядів статичної електрики, пошкодження обладнання та електропроводки. Електростатичний розряд виникає під час тертя двох ізольованих матеріалів.

Пожежна безпека при застосуванні ПК забезпечується:

– системою запобігання пожежі;

– системою протипожежного захисту;

–організаційно–технічними заходами.

Згідно [33] таке приміщення, площею 25 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків–сповіщувачів РІД–1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

–ручний вуглекислий вогнегасник ОУ–5 в кількості 1 шт. або хімічний пінний ОХП–10 – 1 шт;

–повсть 1 1 м2, кошму 2×1,5 м2 або азбестове полотно 2×2 м2 в кількості 1 шт.

Виникнення пожежі можливе, якщо на об'єкті є горючі речовини, окислювач і джерела запалювання. Вірогідність пожежної небезпеки приймається значною, якщо ймовірна взаємодія цих трьох чинників. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, підлоги, двері, ізоляція силових, сигнальних кабелів і т.д.

Горючими матеріалами в приміщенні, де розташовані ПК, є:

–поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420 ˚С,

–полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335˚С, температура самозаймання 530 ˚С,

–склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.74, не схильний до температурного самозаймання,

–пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,

–деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255 ℃, температура самозаймання 399 ˚С.

Для відводу теплоти від ПК діє система кондиціонування. Тому кисень, як окиснювач процесів горіння, є в будь–якій точці приміщень ВЦ.

Простори усередині приміщень в межах, яких можуть утворюватися або знаходиться пожежонебезпечні речовини і матеріали відповідно [33] відносяться до пожежонебезпечної зони класу П–IIа. Це обумовлено тим, що в приміщенні знаходяться тверді горючі та важкозаймисті речовини та матеріали. Приміщенню, у якому розташоване робоче місце, присвоюється II ступень вогнестійкості.

Потенційними джерелами запалювання можуть бути:

– іскри і дуги короткого замикання;

– електрична іскра при замиканні і розмиканні ланцюгів;

– перегріви від тривалого перевантаження,

– відкритий вогонь і продукти горіння,

– наявність речовин, нагрітих вище за температуру самозаймання,

– розрядна статична електрика.

Причинами можливого загоряння і пожежі можуть бути:

– несправність електроустановки;

– конструктивні недоліки устаткування;

– коротке замикання в електричних мережах;

– запалювання горючих матеріалів, що знаходяться в безпосередній близькості від електроустановки.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол [34].

Для захисту персоналу від дії небезпечних і шкідливих чинників пожежі проектом передбачається застосування промислового протигаза, що фільтрує, з коробкою марки «В» із сірою відміткою забарвлення – захист від неорганічних газів (хлор, фтор, бром, сірководень, сірковуглець, хлорциан, галогени), а цей фільтр не захистить від СО (тобто від чадного газу).

Можливе також відповідне застосування фільтрувальної коробки з маркуванням «СО» із фіолетовим забарвленням на фільтрі означає, що він захищає від Чадного газу. Або фільтру для протигазу з літерним маркуванням «SX» із фіолетовим забарвленням захистить від спец речовин таких як (зарин, зоман та фосген).

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три–провідна мережа,

шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється – заземлюючий провідник.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [35] і наведені в таблиці 4.4:

Таблиця 4.4 – Норми мікроклімату робочої зони об’єкту

Період року	Категорія робіт	Температура C^0	Відносна вологість %	Швидкість руху повітря, м/с
Холодна	легка–1 а	22 – 24	40 – 60	0,1
Тепла	легка–1 а	23 – 25	40 – 60	0,1

Дане приміщення обладнане системами опалення, кондиціонування повітря або припливно–витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності [35]. Рівні позитивних і негативних іонів у повітрі мають відповідати [35]. Для забезпечення оптимальних параметрів мікроклімату в приміщенні проводяться перерви в роботі користувача, з метою його провітрювання.

Існують спеціальні системи кондиціонування, які забезпечують підтримання в приміщенні балансу оптимальних параметрів мікроклімату. Контроль параметрів мікроклімату в холодний і теплий період року здійснюється не менше 3–х разів на зміну (на початку, середині, в кінці).

4.4.2 Освітлення

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності.

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

Освітленість приміщення має велике значення при роботі на ППК. Вона багато в чому визначається колірною і мережевий обстановкою. Для зменшеного поглинання світла стеля і стіни вище панелей (1,5–1,7м.). Якщо вони не облицьовані звукопоглинальним матеріалом, фарбуються білою водоемульсійною фарбою (коефіцієнт відбиття повинен бути не менше 0,7). Для забарвлення стіни панелей рекомендується віддавати перевагу світлим фарбам.

Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працівника на ППК.

Робота на ППК може здійснюватися за таких видах освітлення:

–загальному штучному освітленні, коли відео монітори розташовуються по периметру приміщення або при центральному розташуванні робочих місць у два ряди по довжині кімнати з екранами, звернені в протилежні сторони;

–суміщене освітлення (природне + штучне) тільки при одному і трьох рядном розташуванні робочих місць, коли екран і поверхню робочого столу знаходяться перпендикулярно світла несучій стіні. При цьому штучне освітлення буде виконане стельовими або підвісними люмінесцентними світильниками, рівномірно розміщеними по стелі рядами паралельно світловим прорізам так, щоб екран відео монітора знаходився в зоні захисного кута світильника, і його проекції не доводилися на екран. Працюючі на ППК не повинні бачити відображення світильників на екрані. Застосовувати місцеве

освітлення при роботі на ППК не рекомендується.

Природне освітлення, коли робочі місця з ППК розташовуються в один ряд по довжині приміщення на відстані 0,8 – 1,0 м від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працює на ППК. Оптимальна відстань очей до екрана відео монітора повинна становити 60–70 см, допустиме не менше 50 см. Розглядати інформацію ближче 50 см не рекомендується.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

Штучне освітлення в робочому приміщенні передбачається здійснювати з використанням люмінесцентних джерел світла в світильниках загального освітлення, оскільки люмінесцентні лампи мають високу потужність (80 Вт), тривалий термін служби (до 10000 годин), спектральний складом випромінюваного світла, близький до сонячного. При експлуатації ПК виконується зорова робота IV в розряду точності (середня точність). При цьому нормована освітленість на робочому місці (Ен) рівна 200 лк. Джерелом природного освітлення є сонячне світло.

У приміщенні, де розташовані ПК передбачається природне бічне освітлення, рівень якого відповідає [36]. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє [36] і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для будівель виробництв світловий коефіцієнт приймається в межах 1/6 – 1/10:

$$\sqrt{a^2+b^2}\cdot S_b = (1/8 \div 1/10)\cdot S_n \qquad (4.1)$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$S_n = a \cdot b = 5 \cdot 5 = 25$ м^2

$S_{вік} = 1/8 \cdot 25 = 3{,}125$ м^2

Приймаємо 2 вікна площею $S = 1,6$ м^2 кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно–прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників *N* здыйснюэться по формулі:

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M} \qquad (4.2)$$

де *E* – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м2; S = 25 м2;

Z – поправочний коефіцієнт світильника (для стандартних світильників Z = 1.1 – 1.3) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм.

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 \cdot 25 \cdot 1,1 \cdot 1,5}{5400 \cdot 0,575 \cdot 2} \approx 2,64$$

Приймаємо освітлювальну установку, яка складається з 3–х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

Потужність електроосвітлювальної установки з урахуванням місцевого освітлення визначається за формулою:

$$N = \frac{n \cdot W + (0,1 \div 0,2) \cdot n \cdot W}{1000}, \text{ кВт} \quad (4.3)$$

де n– розрахункова кількість ламп для освітлення даного приміщення;

W – потужність однієї лампи, Вт;

(0,1÷0,2) – додаткова потужність для ламп місцевого освітлення, Вт.

$$N = \frac{3 \cdot 160 + 0,2 \cdot 3 \cdot 160}{1000} = 0,576 \text{ кВт}$$

4.4.3 Шум та вібрація, електромагнітне випромінювання

Рівень шуму, що супроводжує роботу користувачів персональних комп'ютерів, а також зовнішніми чинниками, коливається у межах 50–65 дБА [33]. Шум такої інтенсивності на тлі високого ступеня напруженості праці негативно впливає на функціональний стан користувачів. Тому на практиці рекомендують знижувати фактичний рівень шуму у приміщеннях, де створюють комп'ютерні програми, виконують теоретичні та творчі роботи, проводять навчання до 40 дБА, а в приміщеннях, де виконують роботу, що потребує зосередженості, — до 55 дБА. У залах опрацювання інформації та комп'ютерного набору рівні шуму не повинні перевищувати 65 дБА.

Шум часто є причиною зниження рівня працездатності, підвищення рівня загальної та професійної захворюваності, частоти виробничих травм. Шум є загальнобіологічним подразником, який негативно впливає на всі органи і системи організму. У разі тривалого систематичного впливу шуму може виникнути патологія з переважним ураженням слуху, центральної нервової і серцево–судинної систем.

Для зниження шуму на шляху його поширення передбачається розміщення в приміщенні штучних поглиначів. Для зниження рівня шуму стелю або стіни вище 1.5 – 1.7 метра від підлоги повинні облицьовуватися звукопоглинальним матеріалом з максимальним коефіцієнтом звукопоглинання в області частот 63–8000 Гц. Додатковим звукопоглинанням в КВТ можуть бути фіранки, підвішені в складку на відстані 15–20 см. Від огорожі, виконані з щільної, важкої тканини. У приміщенні з ПК коректований рівень звукової потужності не перевищує 45 дБА. Оскільки рівень шуму не перевищує гранично допустимих величин, які встановлені санітарними нормами, заходи для зниження шуму не проводяться.

Віброізоляція можливо здійснювати за допомогою спеціальної прокладки під системний блок, який послаблює передачу вібрацій робочого столу. Вібрація на робочому місці в приміщенні, що розглядається, відповідає нормам [33]. Допустимий рівень вібрацій на робочому місці: – для 1 ступеня шкідливості до 3 дБ; – для 2–3 – 1–6 дБ; – для 3 – більше 6 дБ.

Для захисту від електромагнітного випромінювання передбачаються наступні заходи:

– застосування нових плазмових моніторів,

– віддалення робочого місця не менше, ніж на 0,4 – 0,5 м, оскільки напруженість електричного поля зменшується при віддаленні від джерела поля,

– встановлення раціональних режимів роботи персоналу (обмеження часу перебування),

– раціональне розміщення в робочому приміщенні устаткування, що випромінює електромагнітну енергію.

4.4.4 Вентилювання

У приміщенні, де знаходяться ПК, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти). Цей метод має забезпечити приток потрібної кількості свіжого повітря, що визначається [36] (30 $м^3$ на годину на одного працюючого).

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.5 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно–гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

Заходи безпеки під час експлуатації персонального комп’ютера та периферійних пристроїв передбачають:

– правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;

– експлуатацію сертифікованого обладнання;

– дотримання заходів електробезпеки;

– забезпечення оптимальних параметрів мікроклімату;

– забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення).

Зниження рівня шуму та вібрації:

– у джерелі виникнення, шляхом застосування раціональних конструкцій, нових матеріалів і технологічних процесів;

– звукоізолювання устаткування за допомогою глушників, резонаторів, кожухів, захисних конструкцій, оздоблення стін, стелі, підлоги тощо;

– використання засобів індивідуального захисту).

Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

– постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під’єднують до електромережі;

– постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

– не тягнути за мережевий кабель, щоб витягти вилку з розетки;

– не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

– не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

– не залишати включені електроприлади без нагляду;

– не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

– не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, загорітися (канцелярські товари, сувенірну продукцію тощо).

4.6 Охорона навколишнього природного середовища

4.6.1 Загальні дані з охорони навколишнього природного середовища

Діяльність за темою магістерської роботи в процесі її виконання впливає на навколишнє природне середовище і регламентується нормами діючого законодавства [39–43].

Основним екологічним аспектом в процесі діяльності за даними спеціальностями є процеси впливу на атмосферне повітря та процеси поводження з відходами, які утворюються, збираються, розміщуються, передаються на видалення (знешкодження), утилізацію, тощо в ІТ галузі.

Немає впливу на атмосферне повітря при нормальних умовах праці, бо в приміщенні не використовуються сканери, принтери та інші джерела викиду забруднюючих речовин в повітря робочої зони.

В процесі діяльності користувача виникають процеси поводження з відходами ІТ галузі. Види відходів, утворення, яких можливо:

– відпрацьовані люмінесцентні лампи – І клас небезпеки;
– батарейки та акумулятори (малі) –ІІІ клас небезпеки;
– змінні носії інформації – IV клас небезпеки;
– відпрацьований ізолюючий матеріал, дроти та кабелі – IV клас небезпеки;
– макулатура – IV клас небезпеки;
– побутові відходи – IV клас небезпеки.

4.6.2 Вимоги до збору, пакування та розміщення відходів ІТ галузі

Вимоги зберігання виявлених за своєю роботою відходів визначаються відповідно [40].

Відходи в міру їх накопичення збирають у тару, відповідну класу небезпеки, з дотриманням правил безпеки, після чого доставляють до місця тимчасового зберігання відходів відповідно до затвердженої схеми їх розміщення, зазначені для зберігання відходів місця чи об'єкти повинні використовуватися лише для заявлених відходів.

Не допускається зберігання відходів у невстановлених схемою місцях, а також перевищення норм тимчасового зберігання відходів.

Способи тимчасового зберігання відходів визначаються видом, агрегатним станом і класом небезпеки відходів:

–відходи I класу небезпеки зберігаються в герметичній тарі (сталеві бочки, контейнери). У міру наповнення тару з відходами закривають герметично сталевий кришкою;

–відходи II класу небезпеки в залежності від агрегатного стану зберігаються в поліетиленових мішках, бочках, сховищах та інших видах тари, яка запобігає поширенню шкідливих речовин;

–відходи III класу небезпеки зберігаються в тарі, яка забезпечує локалізацію зберігання, дозволяє виконувати вантажно–розвантажувальні і транспортні роботи і виключає поширення в ОС шкідливих речовин;

–відходи IV класу небезпеки можуть зберігатися відкрито на промисловому майданчику у вигляді конусоподібної купи, звідки їх автонавантажувачем перевантажують у самоскид і доставляють на місце утилізації або захоронення;

–в разі тимчасового зберігання відходів у стаціонарних складах або промислових приміщеннях повинні бути забезпечені санітарно–гігієнічними етичні вимоги до повітря робочої зони згідно [35].

Не допускається змішування відходів різних видів і класів небезпеки з будівельними і побутовими відходами, відходами дерев'яної, металевої, синтетичної тари, відходами текстильних матеріалів (старий спецодяг, ганчірки) та інше.

Проведення заготовки, здачі, переробки та реалізації металобрухту встановлені в [44].

Особливий контроль наділяється збору і зберіганню відпрацьованих ртутьвмісних ламп (енергоощадних) як відходам I класу небезпеки, що збираються і обов’язково передаються на утилізацію підприємствам, що мають ліцензію на поводження з такими небезпечними відходами.

Всі відходи, що утворюються в процесі діяльності/роботи, підлягають обліку.

4.6.3 Визначення впливу та заходів щодо поводження з відходами ІТ галузі

З метою визначення та прогнозування впливу відходів на навколишнє середовище, своєчасного виявлення негативних наслідків, їх запобігання відповідно [45] повинен здійснюватися моніторинг місць утворення, зберігання, і видалення відходів. Відомості про місце утворення та місце розташування відходів зазначаються на «План схемі місці розміщення відходів організації / виробництва» та наводяться у таблиці 4.5, а відомості про склад і властивості відходів, що утворюються, а також ступінь їх небезпечності для навколишнього природного середовища та здоров'я людини у таблиці 4.6.

Таблиця 4.5 Відомості про місце утворення та місце розташування відходів

Код та найменування відходів за ДК –005–96	Технологічний процес або виробництво, де утворюються відходи / клас небезпеки	Місце розташування відходу, тара та її кількість, місткість, розміри у разі наявності майданчиків розташування відходів необхідно зазначити тип покриття та наявність даху)	№ на схемі (додається масштабна схема місць розміщення відходів)
7710.3.1.26 Лампи люмінесцентні, та відходи, які містять ртуть, інші зіпсовані або відпрацьовані (Відпрацьовані ртутьвмісні люмінесцентні лампи)	1	буд.4, в приміщені кладової S=100м^2, в кількість 20 од.	8401–ТХ
7720.3.1.01 Відходи комунальні (міські) змішані, у т.ч. сміття з урн (Побутові відходи)	4	зовнішній майданчик зберігання побутових відходів біля буд .4 S=5м² V= 2,08м³– 2од.	8401–ТХ
7710.3.1.01 Макулатура паперова та картонна (Макулатура)		буд .4 4 поверх в кім. 412 S =5,0 м.^{2}	8401–ТХ
7730.3.1.02 Матеріали пакувальні пластмасові зіпсовані, відпрацьовані чи забруднені (Матеріали пакувальні	4	буд .4 контейнер V=0,9м^3 (3 од.)	8401–ТХ

забруднені			
Змінні носії інформації	4	контейнер V=0,04м^3 (2 од.) буд .4	8401–ТХ
Батарейки та акумулятори (малі)	3	контейнер V=0,09м^3 (4 од.) буд .4	8401–ТХ

Таблиця 4.6 – Відомості про склад і властивості відходів, що утворюються, а також ступінь їх небезпечності для навколишнього природного середовища та здоров'я людини.

Назва відходів	Клас небезпечності	Хімічний (у долях відсотків складників або інших одиницях виміру) та морфологічний склад	Фізико–хімічні властивості
Відпрацьовані люмінесцентні лампи	I	**Ртуть** – 0,013 **Hg** **Скло** – 98,787**(Na, K)$_2$ O 2SiO$_2$** **Алюміній** – 1,2 **Al**	**Ртуть** – $T_{кип.}$ = 356,58°С $T_{плав.}$ = **–38,87°С** **Скло** –$T_{плав.}$=800°С **Алюміній** – $T_{кип.}$ = 2348°С $T_{плав.}$ = 660,1°С
Макулатура	IV	**Цинк** – 0,000053 – 0,000056 **Zn** **Свинець** – 0,000049 – 0,000051 **Pb** **Хром** – 0,000051 – 0,000054 **Cr**	Уривки та обрізки з паперових мішків **Цинк** $T_{кип.}$= 913°С $T_{плав.}$= 4,19°С **Свинець** $T_{кип.}$= 1751°С $T_{плав.}$= 327,3°С **Хром**

		Мідь – 0,000033 – 0,000035 **Cu** **Целюлоза** – 97,299814 – 96,999804 **$(C_6H_{10}O_5)_n$** **Вода** – 2,7 – 3,0	$T_{кип.}$= 1890°C $T_{плав.}$= 2480°C **Мідь** $T_{кип.}$= 2580°C $T_{плав.}$= 1083°C **Целюлоза** $T_{возг. с обуглив.} \geq 100°C$
Побутові відходи	IV	Побутові відходи – 100 – 100, в т. ч.: Папір –30 – 17; [**$(C_6H_{10}O_5)_n$** – целюлоза] Поліетилен –20 – 24; **$(– CH_2 – CH_2 –)_n$** Деревина –5 – 3; [**$(C_6H_{10}O_5)$** – целюлоза, лігнін] Матеріали текстильні –4 – 3; [**$(C_6H_{10}O_5)_n$** – целюлоза Мінеральні домішки (пісок, глина) –4 – 9 Харчові відходи –37 –44;	Поліетилен – $T_{размяг.} \geq 150°C$ Твердий матеріал рослинного походження, не розчиняється у воді. Целюлоза, лігнін $T_{возг. с обуглив.} \geq 120°C$ Харчові відходи $T_{биоразл.} \geq 4^{o}$ C

Негативний вплив на ОС і людини визначається його хімічним складом.

Ртуть. У природних водах міститься в концентрації 0,00003 ... 0,0028 мг / л. Являючись потужним кумулятивним отрутою, з можливою канцерогенною і мутагенною дією. Процеси самоочищення водойм порушують концентрація ртуті понад 0,018 мг / л, порогова концентрація ртуті за впливом на санітарний режим водойм–0,01 мг / л. Наприкінці концентрація понад 0,03 є токсичною практично для всіх видів водних організмів. Надзвичайно токсична при попаданні з питною водою для теплокровних

організмів, надходження ртуті з питною водою в кількості 75,0 ... 300,0 мг / доб. є смертельним. Відрізняється високою токсичністю для будь–яких форм життя. При отруєнні парами спостерігається слабкість, головний біль, біль в шлунку, роздратування по–чек, навіть нефрит; катаральні явища. Розвивається тремтіння рук, ніг, всього тіла. Виникає стан підвищеної психічної збудливості/ Пари ртуті проявляють нейротоксичність, особливо страждають вищі відділи нервової системи [46].

Скло. Нетоксичні, безпечно в навколишньому середовищу, не шкідлива в нирках і водоймах. Вдихання скляного пилу (волокон) призводить до силікоз в зв'язку з високим вмістом сполук кремнію. Шкідливої дії не робить, але є небезпека механічних пошкоджень (порізи, травми).

Алюміній. Токсичний для водної біоти, теплокровних тварин і людей, в концентрації> 1 мг / л чинить негативний впливав на зростання с /г культур. У концентрації> 1 мг / л гальмує зростання мікрофлори водойм і стримує процеси самоочищення водойм. Рівень токсичності визначається формою, в якій знаходиться елемент. Впливає на обмін речовин і функції нервової системи . При попаданні на ґрунт, в воду і атмосферними повітря надає негативного впливу на НС і здоров'я людини.

Цинк. Малотоксичний для теплокровних тварин при надходженні з їжею і питної водою–концентрація в питній воді 11,2 ... 26,6 мг / л переноситься без будь–яких ознак інтоксикації. Дуже корисний для флори, будучи одним з найважливіших мікроелементів харчування, однак лише в концентрації до 0,2 мг / л, крім того, елемент силяється до кумуляції в грантах. Дуже токсичний для водних організмів, порушуючи процеси самоочищення водойм і стаючи токсичним для іхтіофауни в концентрації 0,15 ... 5,0 мг / л. Мутагенна і онкогенна небезпеку.

Свинець. У природних водах міститься в концентрації 0,001 – 0,023 мг / л. У концентрації 2,0 мг / л надає воді металевий присмак. Можливо має мутагенну і канцерогенну дію, значно збільшує токсичну дію інших металів. В конценрації 1,90 мг / л згубно діє на дафній, концентрація 0,1 мг / л погіршує процеси самоочищення водойм. Свинець токсичний для рослин в концентрації понад 5,0 мг / кг ґрунту.

Помірно токсичний. Викликає хронічне отруєння. Має здатність вражати центральну і периферичну нервову систему, кістковий мозок і кров, судини, синтез білка, генетичний апарат клітини.

Хром. Міститься в природних водах в концентрації 0,001 ... 0,112 мг / л. LK50 Cr (VI) для риб–30,0 ... 50,0 мг / л, LK50 Cr (III) для риб – 117,0 мг / л. Низькі концентрації хрому позитивно впливають на ріст рослин. Володіє канцерогенними властивістю.

Мідь. У природних водах міститься в концентраціях 0,001...0,98 мг/л. У концентрації 0,5 мг/л забарвлює воду, в концентрації> 1,0 мг / л–помітно збільшує мутність води. Дуже токсична як для водних організмів, так і для рослин. У концентрації 0,001 мг / л гальмує розвиток синьо зелених водоростей, LK50 практично для всіх видів риб становить 0,18 ... 1,35 мг / л (короп, карась, окунь, щука, сом). Накопичується ґрунтом і рослинами. У концентрації 0,1 ... 0,2 мг / л надає токсичну дію на ріст рослин. Високотоксичний метал. Викликає гостре отруєння, має широкий спектр токсичної дії).

Целюлоза. Нетоксична. Досить легко піддається біодеструкції лігнін – і целюлозоруйнуючими бактеріями і деякими класами нищих грибів. У зв'язку з нетоксичністю LD50 для тваринах не установлена. Токсичність визначається за вмістом важких металів, здатних мігрувати з неї в навколишнє середовище. При попаданні на ґрунт, в воду і атмосферне повітря чинить негативний вплив на ОС і здоров'я людини.

Поліетилен. Нетоксичний для всіх видів флори і фауни в зв'язку з дуже високою біологічною інертністю. Нерозчинний у водних середовищах і не впливає на санітарний режим водойм. Використання його не вимагає запобіжних заходів. Отруєння можливі при виробництві та переробці плівки, в результаті виділення окису вуглецю, альдегідів, органічних кислот [47]

Деревина. Нетоксична. Досить легко піддається біодеструкції лігнін– і целюлозоруйнуючими бактеріями і деякими класами нижчих грибів. У зв'язку з нетоксичністю LD50 для тварин не встановлена. Деревина нетоксична при використання. Але дія деревного пилу при рубці і переробці деревини викликає захворювання дихальних шляхів і шкіри.

Текстильне волокно. Нетоксична в зв'язку з біогенним походженням, проте для біодеструкції необхідна наявність вологи. Нетоксична при використанні. Токсична дія виникає (як результат механічні дії – наслідок пилу) при виробництві тканів і при переробці вторинних матеріалів; слабкий алерген.

4.7 Висновки до розділу 4

У четвертому розділі магістерської роботи проведений аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в дипломній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо

пожежної та електробезпеки. Наведена схема, розміри приміщення та визначені значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері, визначені основні екологічні аспекти впливу на навколишнє природнє середовище та зазначені заходи щодо поводження з ними.

ВИСНОВКИ

В магістерській роботі виконано дослідження методів пошуку несправностей в комп’ютерних системах та мережах. Розглянуті основні засобів моніторингу й аналізу мережі, фізичні основи діагностики мереж. Запропоновано алгоритм пошуку дефектів в локальній обчислювальній мережі, що базується на представленні об'єкта діагностування як моделі з ранжируваним графом та представленням мережевого сегмента у вигляді матриці досяжності. Проведена модифікація структурного методу пошуку дефектів стосовно локальної мережі. На основі проведених досліджень розроблено програмне забезпечення для проведення діагностики та моделювання комп’ютерної мережі.

В магістерській роботі розглянуті типові несправності комп’ютерної мережі побудованої на кабельних та волоконно-оптичних лініях зв’язку, розподіл несправностей у бездротових мережах, структурний метод пошуку дефектів, опис діагностичного експерименту, ієрархія мережі і вибір типу тесту в залежності від рівня пошуку несправності та алгоритм побудови загальної моделі мережі

Визначено, що в мережі може існувати кілька маршрутів діагностичного трафіку від діагностичного вузла до кінцевого вузла, при побудові моделі мережі необхідно вибрати найкоротший маршрут (за кількістю внутрішніх вершин між вузлом–джерелом і вузлом–приймачем тесту) і будувати дихотомічне дерево з урахуванням цього маршруту, виключаючи з розгляду інші.

ПЕРЕЛІК ПОСИЛАНЬ

1. Г.Г. Раннев, А. П, Тарасенко «Методы и средства измерений» Учебник, Москва, ACADEMA, 2004 г.

2. Бакланов И. Г. « Тестирование и диагностика систем связи», Москва, Изд. ЭКО–Трезд., 2001 г.

3. А. Ю. Гребешков «Стандарты и технологии управления сетями связи», Москва, Изд. ЭКО–Трезд., 1998 г.

4. Бакланов И. Г. «ISDN и FRAME RELAY. Технология и практика измерений», Москва, Изд. ЭКО–Трезд., 1998 г.

5. Бакланов И. Г. « Технологии измерений в первичной сети E1, DH, SDH» Изд. ЭКО–Трезв., 1999 г.

6. Леонов А. И. «Основы технической эксплуатации бытовой и радиоэлектронной аппаратуры». Москва, Легпромбытиздат, 1987 г.

7. Бакланов И. Г. «Технология измерений в современных телекоммутациях», Москва, Изд. ЭКО. Трезд., 1998 г.

8. Байда И. П. «Микропроцессорные системы поэлементного диагностирования радиоэлектронной аппаратуры», Москва, Изд. Радио и связь, 1987 г.

9. «Регламент радиосвязи», Женева,1998 г.

10. Черязданов Е. А. «Контроль работоспособности и диагностика радиоэлектронных средств», Алматы, А Э И С, 1999 г.

11. IEEE Std 802.3, 2000 Edition The Institute of Electrical and Electronics Engineers, Inc.

12. ITU–T Recommendation G.821 Error performance of an international digital connection forming part of an integrated services digital network.

13.

14. ITU–T Recommendation G.826 Error performance parameters and objectives for international, constant bit rate digital paths at or above the primary rate.

15. Recommendation M.2100 Bringing into service international digital paths, sections and transmission systems. ITU–T

16. ITU–T Recommendation I.380 Internet protocol data communication service – IP packet transfer and availability performance parameters

17. ITU–T Recommendation Y.1541 Network performance objectives for IP–based services

18. ITU–T Recommendation Y.1231 IP Access Network Architecture

19. Закон України «Про охорону праці».

20. Кодексу законів України про працю.

21. Закон України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності".

22. НПАОП 0.00–6.03–93 «Порядок опрацювання та затвердження власником нормативних актів про охорону праці, що діють на підприємстві».

23. НПАОП 0.00–4.12–05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці».

24. НАПБ Б.02.005–2003 «Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України».

25. НПАОП 0.00–4.15–98 «Положення про розробку інструкцій з охорони праці».

26. ДСН 3.3.6.042–99 «Санітарні норми мікроклімату виробничих приміщень».

27. ДСанПіН 3.3.2.007–98 «Правила і норми роботи з візуальними дисплейними терміналами електронно–обчислювальних машин».

28. НПАОП 0.00.–1.28–10 «Правил охорони праці під час експлуатації електронно–обчислювальних машин».

29. .НАПБ Б.03.002–2007. «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».

30. ГОСТ 12.1.044–89 ССБТ. «Пожаровзрывоопасность веществ и материалов. Номенклатура показателей и методы их определения».

31. ДСН 3.3.6.042–99. «Санітарні норми мікроклімату виробничих».

32. .ДБН–В.2.5–28–2006. «Природне і штучне освітлення».

33. ДСН 3.3.6.037–99. «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

34. ДБН В.2.5–67:2013 Опалення, вентиляція та кондиціонування.

35. Закон України «Про охорону навколишнього природного середовища».

36. Закон України «Про забезпечення санітарного та епідемічного благополуччя населення».

37. Закон України «Про відходи».

38. Закон України «Про охорону атмосферного повітря».

39. Закон України Закон України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру».

40. ДСанПіН 2.2.7.029. «Гігієнічні вимоги щодо поводження з промисловими відходами та визначення їх класу небезпеки для здоров'я населення».

41. Закон України «Про металобрухт».

42. ДСТУ 3911–99. Охорона природи. Поводження з відходами. Виявлення відходів і подання інформаційних даних про відходи. Загальні вимоги.

43. ДК 005–96. Державний класифікатор України. Класифікатор відходів.