

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проєкту (роботи)

магістра

(ступінь вищої освіти)

на тему СИСТЕМА СЕРВЕРНОГО ОБЛАДНАННЯ ДЛЯ ОБ'ЄКТУ
КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Виконав: студент 2 курсу, групи КНТ-512м
спеціальності _____

123 Комп'ютерна інженерія

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Комп'ютерні системи та мережі

ОСИПЕНКО О. В.

(ПРИЗВИЩЕ та ініціали)

Керівник ЗЕЛЕНЬОВА І.Я.

(ПРИЗВИЩЕ та ініціали)

Рецензент КОЗИНА Г.Л.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій
 Кафедра «Комп'ютерні системи та мережі»
 Ступінь вищої освіти магістерський
 Спеціальність 123 Комп'ютерна інженерія
 (код і найменування)

Освітня програма (спеціалізація) «Комп'ютерні системи та мережі»
 (назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Зав. кафедри Кудерметов Р.К.

“20” 12 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

Осипенко Олександра Вікторовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Система серверного обладнання для об'єкту критичної інфраструктури

керівник проєкту (роботи) к. т. н., доцент, ЗЕЛЕНЬОВА Ірина Яківна

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

затверджені наказом вищого навчального закладу від “24” 10 2023 року №
 400

2. Строк подання студентом проєкту (роботи) 10 грудня 2023 року

3. Вихідні дані до проєкту (роботи) методи оцінювання показників надійності комп'ютерних мереж, засоби підвищення надійності, опис структури підприємства, пакет моделювання Cisco.

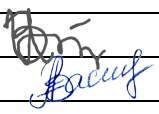
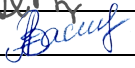
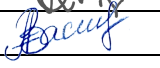
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Ознайомлення із надійністю серверних систем.

2) Дослідження та аналіз структури серверної.

3) Підвищення надійності серверної системи.

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

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	ЗЕЛЕНЬОВА І.Я., доцент		
нормоконтроль	ПОЛЬСЬКА О.В., ст. викл.		

7. Дата видачі завдання 01.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Резервування серверів в системах відповідального призначення	05.10.2023 р.	
2	Програмні та технологічні засоби для розробки резервування серверних систем	10.10.2023 р. 15.10.2023 р.	
3	Розробка обладнання та мереж	20.10.2023 р.	
4	Розробка структури обладнання серверверної	05.10.2023 р.	
5	Підвищення надійності серверної системи	20.11.2023 р.	
6	Оформлення отриманих результатів у ПЗ	25.11.2023 р.	
7	Оформлення допоміжного матеріалу	01.12.2023 р.	

Студент  Олександр ОСИПЕНКО
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник проєкту (роботи)  Ірина ЗЕЛЕНЬОВА
(підпис) (ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

ПЗ: 60 с., 24 рис., 2 табл., 29 джерел.

КОМП'ЮТЕРНА МЕРЕЖА, КОМУТАТОР, МАРШРУТИЗАТОР, СЕРВЕР, ДЖЕРЕЛО БЕСПЕРЕБІЙНОГО ЖИВЛЕННЯ, ПРОГРАМНИЙ МОДУЛЬ ASNA, RAID МАСИВ.

Об'єктом дослідження є система серверного обладнання для об'єкту критичної інфраструктури.

Предметом дослідження є засоби для підвищення надійності серверних установок та технології для створення ефективного резерву.

Метою роботи є підвищення надійності серверної у складі системи відповідального призначення.

Основними задачами розробки є розрахунок і використання резерву для підвищення відмовостійкості серверів; проведення аналізу сучасних технологій резервування серверних систем та систем моделювання та дослідження надійності у вигляді структурно-автоматних моделей; налаштування резерву у системі поєднання великої кількості серверів для постійного контролю відмовостійкості та виводу з ладу.

В першій главі розглядається об'єкт критичної інфраструктури та система серверного обладнання. В другій главі розглядається характеристика об'єкта серверної для об'єкту критичної інфраструктури. В третій главі розглядається структура обладнання серверної а також комп'ютерна і електрична мережа. В четвертій главі розглядається підвищення надійності серверної системи та вибір резерву.

ABSTRACT

Explanatory note to the master's work: 60 p., 24 figures, 2 tables, 29 sources.

COMPUTER NETWORK, SWITCH, ROUTER, SERVER, UNINTERRUPTED POWER SUPPLY, ASNA SOFTWARE MODULE, RAID ARRAY.

The object of the study is a system of server equipment for a critical infrastructure facility.

The subject of research is the means to increase the reliability of server installations and the technology for creating an effective reserve.

The purpose of the work is to increase the reliability of the server as part of the responsible destination system.

The main tasks of the development are the calculation and use of the reserve to increase the fault tolerance of servers; analysis of modern server system backup technologies and modeling systems and reliability research in the form of structural-automatic models; redundancy settings in a system combining a large number of servers for continuous monitoring of fault tolerance and failover.

The first chapter examines the object of critical infrastructure and the system of server equipment. The second chapter considers the characteristics of the server object for the critical infrastructure object. The third chapter examines the structure of server room equipment, as well as the computer and electrical network. The fourth chapter deals with increasing the reliability of the server system and choosing a reserve.

ЗМІСТ

Вступ.....	7
1 Ознайомлення із надійністю серверних систем.....	9
1.1 Об'єкти критичної інфраструктури.....	9
1.2 Резервування серверів в системах відповідального призначення.....	11
1.3 Переваги та недоліки резерву серверів.....	14
1.4 Програмні та технологічні засоби для розробки резервування серверних систем.....	17
1.6 Комплексні показники надійності мереж.....	21
2 Характеристика об'єкта.....	24
2.1 Дослідження та аналіз структури серверної.....	24
2.2 Характеристика наявного об'єкта.....	40
2.3 Постановка задачі розробки.....	41
3 Розробка обладнання та мереж.....	41
3.1 Розробка структури серверверної шафи.....	41
3.2 Розробка електромережі.....	43
3.3 Розробка топології мережі.....	46
4 Підвищення надійності серверної системи.....	47
4.1 Побудова графа надійності.....	47
4.2 Вибір резерву серверної та електрообладнання.....	50
4.3 Дослідження резервованої мережі.....	51
4.4 Тестування резервованої мережі.....	55
Висновки.....	56
Перелік джерел посилання.....	57

ВСТУП

На сьогодні у світі практично не існує радіоелектронних систем без використання керуючих серверних систем, які б в свою чергу повинні були б мати високу надійність. Тому, якщо виходити з практики використання радіоелектронних систем на сьогодні, особливу увагу необхідно приділити надійності таким вузлам, а саме: оперативна пам'ять, блок живлення, дискові масиви пам'яті та підсистеми охолодження.

Для створення моделі серверної, яке буде займатися зберіганням, обробкою та передачею великої кількості даних, крайнє необхідно організувати надійний резерв. При цьому треба забезпечити бесперебійний доступ до електричної та інтернет мережі. Враховуючи всі ці фактори необхідно обрати обладнання, яке зможе забезпечити швидку та бесперебійну роботу усієї серверної системи із використанням резерву та виконуватиме всі свої операції пов'язані з передачею, обробкою та збереженням даних.

Проектування серверних кімнат – важливий етап створення інформаційно-технічної інфраструктури підприємства. Якісне проектування серверних кімнат забезпечує надійну та ефективну роботу серверного обладнання, а також безпеку даних. Розглянемо деякі важливі кроки та аспекти, які слід врахувати під час проектування серверних кімнат.

Вибір розташування для серверної кімнати є важливим аспектом. Вона має бути віддалена від можливих джерел вібрації, вологості, агресивних хімічних речовин та інших факторів, які можуть вплинути на роботу обладнання. Визначення кількості серверів та обладнання, які будуть розміщені в серверній кімнаті, має бути виконано зна етапі проектування. Це дозволить визначити необхідну площу, висоту стель, розподіл розеток та систему кондиціонування. Також потрібно зробити розрахування необхідної потужності для всіх серверів та обладнання, включаючи можливі майбутні розширення, забезпечити наявність

резервного джерела живлення, такого як джерело безперебійного живлення (ДБЖ), щоб запобігти втраті даних при збоях в електропостачанні.

Серверне обладнання генерує значну кількість тепла, тому необхідно забезпечити ефективну систему охолодження. Це може бути система кондиціювання повітря, спеціалізовані охолоджувачі або рідинне охолодження.

Забезпечення фізичної безпеки серверної кімнати є також важливим елементом проектування. Вхід повинен бути обмежений, можливо, за допомогою біометричної ідентифікації або електронних ключів. Також розглядається установка системи відеоспостереження та контролю доступу. Правильне розміщення мережевих та електричних кабелів, а також їх маркування, сприяють порядку та спрощують обслуговування.

Сервери можуть створювати шум, який може бути неприйнятним для навколишніх приміщень. Тому розглядається можливість звукоізоляції серверної кімнати.

Важливо мати можливість моніторингу стану серверів та обладнання у реальному часі. Це дозволить оперативно реагувати на проблеми та збої. При цьому розглядається можливість створення відмовостійкої інфраструктури з дубльованими системами, резервними джерелами електроживлення тощо.

Під час проектування серверної кімнати чи інфраструктури потрібно враховувати можливість розширення. Це дозволить уникнути проблем при додаткових потребах у майбутньому. Важливо також вести докладну документацію про розміщене обладнання, схеми підключення, налаштування систем та іншу інформацію.

Проектування серверних кімнат – це складний процес, який потребує комплексного підходу та врахування багатьох факторів. Важливо працювати з досвідченими фахівцями з інформаційних технологій та інженерії для створення надійної та ефективної інфраструктури.

1 ОЗНАЙОМЛЕННЯ ІЗ НАДІЙНІСТЮ СЕРВЕРНИХ СИСТЕМ

1.1 Об'єкти критичної інфраструктури

Об'єкти критичної інфраструктури – підприємства та установи енергетичної, хімічної, транспортної промислової а також, фінанси, телекомунікації та охорона здоров'я, що відіграє важливу стратегічну роль у функціонуванні економіки і безпеки держави та суспільства країни, руйнування цих об'єктів може призвести до значних втрат як матеріальних фінансових або людських жертв [1].



Рисунок 1.1 – Електрична підстанція [3]

До прикладу можна також віднести станції та підстанції це електроустановка що призначена для вироботку перетворення чи розподілу електричної енергії.

У призначинні можуть бути трансформаторні підстанції або перетворювальні підстанції. Електричний розподільний пристрій який не є у складі підстанції є розподільчим пунктом (рис.1.1) [2].

Теплова електростанція це електростанція в якій первинна енергія генерується шляхом спалювання вугілля, рідкого палива чи газу оскільки має хімічну форму; у парових електростанціях, які мають парові турбіни, топки парового котла перетворюють хімічну енергію палива у тепло газів що являє собою продукт згоряння; тепло яке передається до теплоносія, являє собою пару що надходить з котла до парової турбіни, що призводить до обертання турбогенератора; пара що відпрацьовується в турбіні конденсується і віддає тепло охолоджувальній воді (рис.1.2) [4].



Рисунок 1.2 – Теплова електростанція [5]

До конфігурації відмовостійкості системи на рисунку 1.3 включено основні елементи такі як: 1 – модулі основного пристрою, 2 – модулі ковзного резерву основного пристрою, 3 - резервні пристрої, ЗКД – засоби контролю та діагностики [6].

Для проектування надійності таких відмовостійких систем в терії відсутні формули визначення відповідних показників, але існує технологія розробки їх математичних моделей у вигляді дискретно-неперервної стохастичної системи. Але для використання цієї технології потребує значних затрат часу в процесі проектування при розв'язанні задач багатоваріантного аналізу, що в свою яергу ускладнює роботу при проектуванні. Тому в цьому дослідженні використовується удосконалена технологія аналітичного моделювання дискретно-неперервних стохастичних систем . Це дозволило автоматизувати процес розробки моделі у вигляді графа станів і переходів, що в свою чергу вже зменшує затрати часу на багатоваріантний аналіз відмовостійких систем з комбінованим структурним резервуванням. Реалізація цієї технології в програмному модулі ASNA, призначена для формування надійнісних моделей та розв'язання задач надійнісного проектування відмовостійких систем. Робота з програмним модулем ASNA передбачає розробку структурно-автоматної моделі об'єкту проектування, яка представляє вибрану конфігурацію відмовостійкої системи та її поведінку [6, 7].

Отже, поставленою метою роботи є розробка надійнісних моделей вузла пам'яті сервера, а також джерела безперебійного електроживлення (ДБЕЖ) у системах відповідального призначення у вигляді структурно-автоматних моделей [6].

Для автоматичного резерву невід'ємною частиною у підвищенні надійності є і вузол пам'яті сервера який реалізується на блоках RAID-масиву, пристрою перемикання, засобів контролю та діагностики [6].

Структурна схема вузла пам'яті сервера представлена на рисунку 1.4. Основна вимога до надійності вузла пам'яті є забезпечити безперебійну роботу протягом тривалого часу, а саме від 3 до 5 років, який обумовлений амортизацією

обладнання. Після закінчення терміну експлуатації вузла пам'яті сервера протягом вказаного періоду часу проводиться його заміна на новий (рис.1.4) [6].

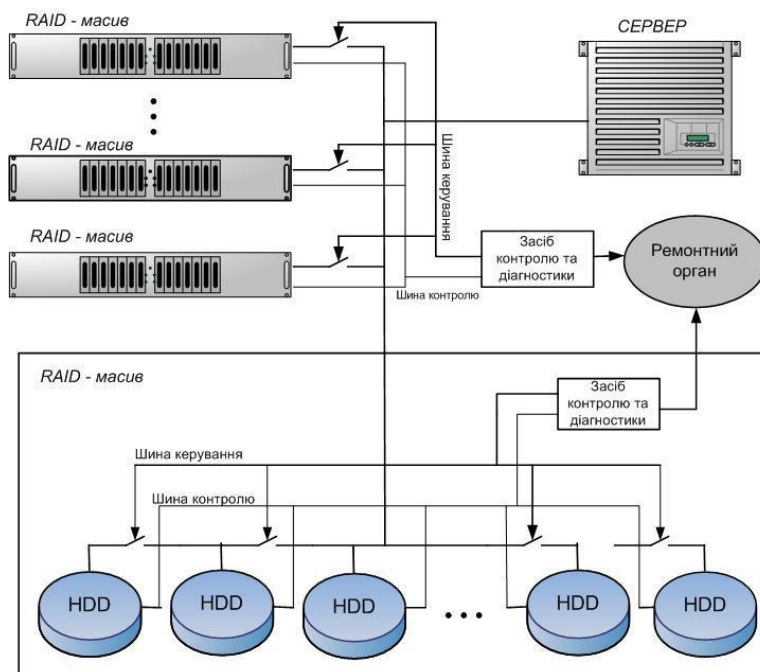


Рисунок 1.4 – Структурна схема вузла пам'яті сервера [6]

Для побудови надійнісної моделі вузла пам'яті сервера мають містити в собі такі параметри як: кількість модулів основного пристрою n , кількість модулів ковзного резерву m , кількість резервних пристроїв L , інтенсивність відмови модулів основного пристрою та резервних модулів λ_m , інтенсивність відмови працюючого резервного пристрою λ_{rpr} , інтенсивність відмови непрацюючого резервного пристрою λ_{npr} , середнє значення часу необхідного для підключення резервного модуля T_{prm} , середнє значення інтервалу часу необхідного на ремонт резервного модуля T_{rnm} , середнє значення часу необхідного для підключення резервного пристрою T_{prp} , середнє значення інтервалу часу, необхідного на ремонт резервного пристрою T_{prp} . Для модулів основного пристрою та резервних пристроїв передбачено технічне обслуговування, яке проводить один ремонтник. При цьому для модулів передбачено $S_{мор}$ відновлень, а для резервних пристроїв – S_{rp} відновлень [6].

До надійності джерела безперебійного електроживлення, що розглядається, ставиться така ж сама вимога забезпечити працездатність протягом тривалого часу. Джерело безперебійного електроживлення складається з блока живлення, у складі якого є однотипні модулі робочої конфігурації і такі ж модулі ковзного резерву. Два акумулятори здійснюють загальне резервування блока живлення і для них передбачено певну кількість заряджань. Засоби контролю та діагностики здійснюють контроль працездатності блока живлення і локалізацію несправного модуля в ньому, а також контроль працездатності акумуляторів. Перший акумулятор підключається до навантаження в момент відмови блока живлення, або при відключенні електромережі. Другий акумулятор підключається тоді, коли перший розрядився або вийшов з ладу. При відсутності електромережі живлення напруга на зарядний пристрій акумулятора подається від генератора. Функцію перемикачання електромережа/генератор здійснює автоматичний перемикач. Все це має забезпечити безперервну роботу серверної системи та підвищити її надійність. При цьому показники надійності будуть залежати від якості проєктування структурно-автоматної моделі системи [6, 7].

1.3 Переваги та недоліки резерву серверів

Обчислювальні прилади поділяються на відновлювальні та невідновлювальні після відказу. Крім того, прилади обчислювальної техніки відрізняються вимогами щодо надійності, умовами експлуатації та інше. Тому на практиці використовуються різні показники надійності [8].

До відновлювальної обчислювальної техніки відноситься сервер, який у свою чергу повинен мати резервування та надійність радіоелементів із коефіцієнтом польових умов $K=2$ [8].

Час до відмови, час між відмовами, час відновлювання та інше є випадкові величини. Тому, усі показники надійності, як для невідновлювальних, так і

відновлювальних приладів, є імовірнісними [8].

Вихідні данні щодо кількісного визначення параметрів надійності є розподіл імовірності відмов у часі. Для оцінки цього розподілу коли якась кількість виробів експлуатується тривалий час, або проводяться спеціальні випробування, доки усі прилади не відмовлять. Час на відмову кожного виробу фіксується. Якщо на початок випробувань усі 100 відсотків виробів працюватимуть, то при якомусь часі ($t \rightarrow \infty$) вони обов'язково вийдуть із ладу - відмовлять. Нормована крива, яка побудована на основі великого числа вимірів часу відмов, характеризує щільність імовірності відмов у часі $f(t)$. За допомогою щільності імовірності відмов у часі $f(t)$ знаходять інші показники надійності приладів обчислювальної техніки [8].

В окремих випадках, коли потрібно підвищити показники надійності радіоелементів, вузлів, приладів тощо, в обчислювальних системах включають паралельно основному обладнанню таке саме резервне обладнання, розташування якого передбачено в конструкції [8].

Якщо, цей спосіб дозволяє конструювати із ненадійних елементів надійну апаратуру, так як, при відмові основних елементів, роботу продовжують резервні [8].

Якщо кількість резервних елементів s менша за основну w , то має місце резервування із дробовою кратністю та навпаки, якщо кількість резервних елементів більша за основну в k разів, то має місце ціле k -кратне резервування. Де $k=0,1,2,3,..$ [8].

Загальне резервування, коли резервують увесь елемент (пристрій, блок, плату, радіоелементів, інше) як і дробове, коли резервують окремі елементи (вузли, блоки, плати) пристрою, або комбіноване, може бути із постійним включенням, або із включенням при заміщенні елемента що відмовив.

При цьому резервні елементи знаходяться в одному з режимів:

- навантажений (гарячий);
- ненавантажений (холодний), коли резерв не підключений до джерел напруги;

– полегшений (теплий), коли резерв підключений до джерел напруги, але відключений від навантаження [8].

До переваг резервування серверів можна віднести наступне.

По-перше, надійний захист даних: захист при кібератаках, стихійного лиха, несправності апаратного забезпечення, випадкових видалень або інші подібні інциденти, що не має призвести до значної втрати даних. За допомогою сервера резервного копіювання завжди створюється дублікат важливих даних, тож навіть якщо є проблема, що може спричинити втрату даних, це рішення для резервного копіювання захистить дані [9].

По-друге, покращений захист важливих даних: на сьогоднішній день збирається безпрецедентна кількість даних, яка включає в себе як життєво важливу інформацію для отримання ділової інформації, так і неважливі дані. Дані, які життєво важливі для бізнесу, мають бути створені резервні копії, щоб мати гарантії їх відновлення у час необхідності. Сервер резервного копіювання це носій резервного копіювання де можна постійно й автоматично зберігати свої дані, важливі для бізнесу та будь чого, а також робити їх зашифрованими для підвищення безпеки. Таким чином, є кілька копій даних, що забезпечують захист і безпеку даних [9].

По-третє, негайне відновлення даних: система миттєвого резервного копіювання даних а також можливість швидкого відновлення цих даних. Тому, якщо втрачено важливі дані, все, що потрібно, це отримати доступ до диска відновлення та відновити дані [9].

До недоліків резервування серверів можна віднести: вартість резерву, оскільки набір усіх компонентів для серверної системи для користувача обходиться до значних витрат як у експлуатації, налаштуванні так і у обслуговуванні усієї системи резерву.

1.4 Програмні та технологічні засоби для розробки резервування серверних систем

Для розробки серверних систем є важливо забезпечити надійність та доступність інформаційних систем. У розробці використовуються різноманітне програмне забезпечення та технологічні засоби. Все це має допомогати у відмовостійкості та дублюванні серверних систем, забезпечити резервне копіювання та відновлення і інше.

До програмних засобів розробки резерву серверних систем можна віднести:

- Cisco Packet Tracer;
- Microsoft Visio;

Cisco Packet Tracer це програма симулятор мережі для підготовки до сертифікаційних іспитів, мережевої академії Cisco для студентів CCNA. Програма допомагає змодельовати комп'ютерну мережу із багатьма технічними елементами (рис.1.5) [10].

Microsoft Visio це програма, яка дозволяє користувачам моделювати процеси за допомогою різних графічних форм, де є можливість створювати різноманітні діаграми і багатими наборами форм та шаблонів (рис.1.6) [11].

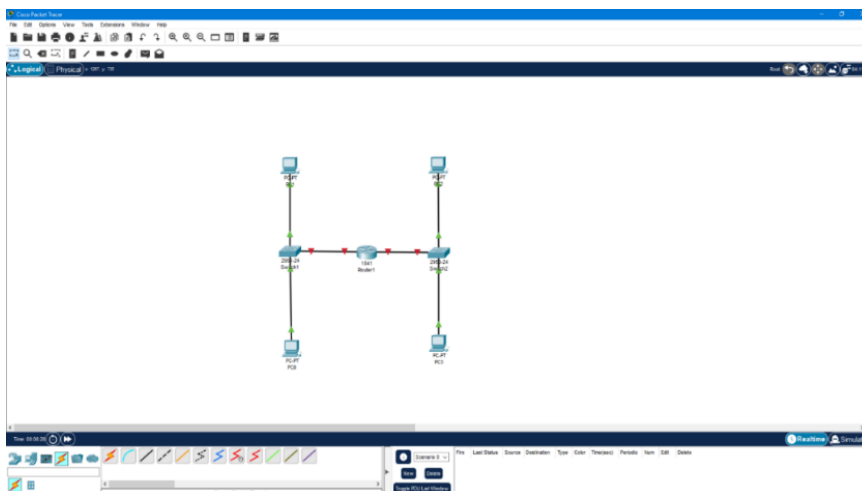


Рисунок 1.5 – Робоче вікно Cisco Packet Tracer

Кластеризація це групи серверів, які працюють синхронно під однією IP-адресою. Кластерні сервери використовуються для серверів, які містять файли, бази даних і повідомлення. Кластери підвищують захист даних та зберігають узгодження конфігурації кластера із часом. Кластеризація забезпечує належне балансування та доступність. Кластерами є Linux High Availability Clusters та Microsoft Failover Clustering [14].

Інструменти автоматизації це інструменти які допомагають налаштувати автоматизацію сервера. Інструменти використовуються у платформах надання серверів як Terraform, так і у контейнеризації, як Kubernetes. Ці інструменти допомагають автоматизувати процеси створення резервних копій та відновлення серверів [15].

Системи моніторингу та сповіщень це процес моніторингу системних ресурсів сервера, робота процесора, запис на диск та інше. Показники моніторингу сервера допомагають у плануванні потужності, знаючи використання ресурсів системи сервера. Інструмент моніторингу допомагає серверу автоматизувати моніторинг [16].

Всі інструменти та технології повинні забезпечити високу надійність серверної системи у випадку виходу її з ладу.

1.5 Апаратні засоби електричної мережі

Електрична мережа відіграє велику роль у надійності серверної системи. Перепад або перенапруга у електричній мережі може призвести до виходу з ладу усієї системи та втрати даних. Для цього існують наступні апаратні засоби електричної мережі(рис.1.7).

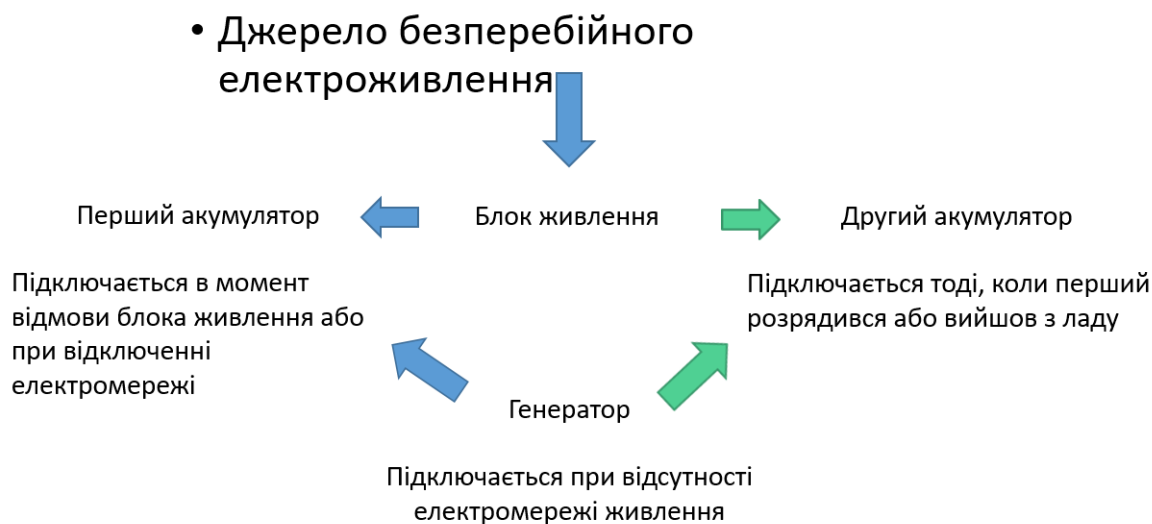


Рисунок 1.7 – Схема джерела безперебійного живлення [7]

До апаратних засобів електричної мережі можна віднести:

- джерела енергії із резервуванням;
- безперебійне живлення;
- генератори резервного живлення;
- моніторинг та управління;
- розподіл електроживлення.

Джерела енергії із резервуванням це обладнання, на якому проводиться обробка даних, вибираються джерела живлення, які мають характеристики надійності та ефективності а також резервування. Тому при обробці великих даних яке ведеться на обладнанні, необхідно використовувати блоки живлення із резервом та функцією гарячої заміни [17].

Безперебійне живлення: сервери та інше мережеве обладнання потребує електричного захисту. Достатньо лише одного стрибка напруги що може вивести із ладу будь яку техніку чи пристрій, та втратити цінні дані. Тому необхідно встановити джерело безперебійного живлення [18].

Генератори резервного живлення: ці генератори забезпечують на виході чистоту напруги із гарантованою безпекою. Тому при відключенні зовнішньої мережі дає забезпечення безпеки електроприладів через проблеми із

електромережею. Але для того щоб запустити генератор необхідний час, та через кілька годин генератор перегрівається та необхідне охолодження [19].

Розподіл електроживлення: блоки розподілу використовуються для підключення комп'ютерного чи мережевого обладнання до електричної мережі, які встановлюються всередині шафи. Також це дає можливість підключити велику кількість комп'ютерного обладнання у шафі [20].

Моніторинг та управління: управління електроживленням підвищує надійність живлення, а також має забезпечити постачання енергії високої якості у будівлях. А також це допомагає забезпечити ефективність і безпеку [21].

Всі апаратні засоби електричної мережі мають забезпечити надійність електроживлення для роботи серверної системи. Якщо забезпечити правильну надійність то це підвищить безвідказну роботу та не дасть системі вийти з ладу.

1.6 Комплексні показники надійності мереж

У випадках для оцінки експлуатаційних якостей об'єкта одних одиничних показників надійності буває недостатньо. З'являється необхідність у більш складних показниках, які б надавали опис відразу декілька властивостей, складових надійності об'єкта. Такі показники є комплексними показниками надійності [22].

До них можна віднести: коефіцієнт готовності, коефіцієнт технічного використання і коефіцієнт оперативної готовності [22].

Процес функціонування відновлюваного об'єкта можна представити як послідовність чергування інтервалів працездатності і відновлення (простою).

Коефіцієнт готовності КГ – ймовірність того, що об'єкт виявиться працездатним в довільний момент часу, крім запланованих періодів, протягом яких використання об'єкта за призначенням не передбачається [22].

До статистичних даних експлуатації коефіцієнт готовності об'єкта

визначається як відношення сумарного часу перебування спостережуваного об'єкта в працездатному стані до всього часу його експлуатації.

Якщо подивитись на найпростішу систему експлуатації об'єкта (робота – відновлення – робота), то для цього визначення значення коефіцієнта готовності можна записати:

$$K_T = \frac{T}{T + T_B}$$

де T – напрацювання на відмову; T_B – середній час відновлення.

Коефіцієнт готовності може бути визначений як для одиночного об'єкта, так і для групи об'єктів.

З наведеного виразу випливає, що збільшити значення коефіцієнта можна, збільшуючи безвідмовність об'єкта або ж якимось скорочуючи час відновлення. Коефіцієнт готовності об'єкта може бути підвищений за рахунок збільшення напрацювання на відмову і зменшення середнього часу відновлення. Для того щоб визначити коефіцієнт готовності необхідний досить тривалий календарний термін функціонування об'єкта.

Коефіцієнт оперативної готовності КОГ визначається як ймовірність того, що об'єкт виявиться в працездатному стані в довільний момент часу (крім планованих періодів, протягом яких застосування об'єкта за призначенням не передбачається) та, починаючи з цього моменту, буде працювати безвідмовно протягом заданого інтервалу часу [22].

З визначення випливає, що

$$K_{OG} = K_T \cdot p(t).$$

Коефіцієнт простою $K_{п}$ – коефіцієнт, що визначає імовірність того, що об'єкт буде непрацездатним у довільно обраний момент часу. Коефіцієнт простою

визначається як:

$$K_{\pi} = \frac{T_B}{T + T_B} \Rightarrow K_p = 1 - K_{\pi}.$$

Коефіцієнт технічного використання – відношення математичного очікування часу перебування об'єкта в працездатному стані T за деякий період експлуатації до суми математичних сподівань часу перебування об'єкта в працездатному стані T , часу простоїв $T_{\text{пр}}$, обумовлені технічним обслуговуванням, і часу ремонтів T_B за той же період експлуатації, визначається як:

$$K_{\text{ТВ}} = \frac{T}{T + T_B + T_{\text{пр}}}.$$

У виразі коефіцієнт технічного використання характеризує частку часу перебування об'єкта в працездатному стані щодо загальної (календарній) тривалості експлуатації.

Середня сумарна трудомісткість технічного обслуговування – математичне сподівання сумарних витрат на проведення технічного обслуговування об'єкта за певний період експлуатації. Відношення цього показника до математичного очікування сумарного напрацювання об'єкта за той же період експлуатації називають питомою сумарною трудомісткістю технічного обслуговування.

Для визначення оцінки трудомісткості ремонтів використовують аналогічний показник – середню сумарну трудомісткість ремонтів, розуміючи під цим математичне сподівання сумарних затрат на всі види ремонтів об'єкта за певний період експлуатації. Відношення цього показника до математичного очікування сумарного напрацювання об'єкта за той же період експлуатації це питома сумарна трудомісткість ремонтів [22].

Для оцінки умов експлуатації об'єкта є коефіцієнт навантаження, що дозволяє враховувати вплив різних факторів на об'єкт у період його експлуатації.

Коефіцієнт навантаження – відношення реального робочого навантаження

НР, що діє на об'єкт (елемент) в даних умовах, до номінального навантаження НН, передбаченого для даного об'єкта (елемента) в заданих умовах експлуатації:

Формула розрахунку коефіцієнта навантаження є наступною:

$$K_H = H_p / H_H.$$

Крім розглянутих показників, у ряді випадків використовуються і інші комплексні показники надійності. Наприклад, для оцінки вартості експлуатації: вартість технічного обслуговування, вартість ремонтів тощо [22].

2 ХАРАКТЕРИСТИКА ОБ'ЄКТА

2.1 Дослідження та аналіз структури серверної

На тепловій електростанції, у якій буде система серверного обладнання як для об'єкту критичної інфраструктури, у якій буде збір, зберігання та аналіз даних.

Серверні приміщення є невід'ємною частиною ІТ-інфраструктури будь-якої організації. У них розміщуються сервери, сховища даних та мережеве обладнання, що забезпечує функціонування сфери діяльності. Кожна галузь має свої особливі вимоги, тому серверні кімнати можуть відрізнятися від організації до організації. Деякі з них можуть бути невеликими із однією шафою, тоді як інші можуть вміщувати кілька стелажів із серверами, розміщеними в одному стелажі. Незалежно від конфігурації, важливість захисту кімнати та збереження даних в ній неможливо переоцінити (рис. 2.1) [26].

На сьогоднішній день існують такі стандарти розробки серверних приміщень: Стандарт TIA/EIA-569. Commercial Building Standard for Telecommunication Pathways and Spaces, Стандарт ANSI/NECA/BICSI 568-2001.

Installing Commercial Building Telecommunication Cabling, Стандарт ANSI/TIA/EIA-607. Commercial Building Grounding and Bonding Requirements for Telecommunications [28].



Рисунок 2.1 – Серверна кімната із серверами [27]

Тому для побудови приміщень із серверами а саме кімнат висуваються наступні вимоги, що викладено нижче.

Серверне приміщення має розміщуватись як ближче до магістральних кабельних каналів.

Для серверної кімнати потрібне відповідне місце, що може вмістити значну кількість обладнання, живлення та системи кондиціювання повітря. Підлога повинна бути стійкою й здатною витримувати великі навантаження від важкого обладнання. Звужені приміщення не є оптимальним вибором, оскільки ефективне охолодження вимагає постійної циркуляції повітря. Також не рекомендується розташовувати серверну кімнату у приміщенні з вікнами або на зовнішній стіні, оскільки це може ускладнити контроль та забезпечення безпеки середовища всередині приміщення [26].

Ідеальною вважається висота приміщення близько 2.8 метрів, з підвісними стелями для забезпечення необхідної роботи повітряних каналів та можливості встановлення систем відведення тепла та іншого обладнання. Використання фальшпідлоги для прокладання кабелів є бажаним, але не є обов'язковим для невеликих серверних кімнат.

В ідеальних випадках, серверне приміщення повинно бути поруч з головним розподільчим пунктом (Main Cross, MC), а якщо є така можливість, то слід організувати головний розподільний пункт аж в самому серверному приміщенні.

Необхідно розміщувати апаратне приміщення недалеко від вантажних або вантажопасажирських ліфтів, використовуваних для транспортування важкого обладнання. У цей час, слід уникати близького розміщення потужних джерел електричних і магнітних полів, а також обладнання, яке може викликати підвищену вібрацію.

Вібрація може негативно впливати на активне обладнання, особливо на його точність та надійність роботи. Частота та амплітуда коливань є важливими параметрами, які необхідно враховувати для запобігання можливих проблем.

Це особливо важливо у випадках, коли обладнання потребує високої точності або працює у чутливих умовах.

Частота та амплітуда вібрацій є ключовими параметрами, які слід враховувати. Вони визначають рівень коливань, які можуть впливати на обладнання. Чим вища частота або амплітуда вібрацій, тим більший потенційний вплив на роботу обладнання.

Для запобігання проблемам, пов'язаним із вібрацією, можуть застосовуватися різноманітні техніки та методи. Це може включати встановлення спеціальних амортизуючих підкладок або систем віброгасіння, розміщення обладнання на спеціально призначених платформах чи у відведених приміщеннях з додатковими заходами для поглинання вібрації.

Урахування параметрів вібрацій та вжиття відповідних заходів для їх контролю та зменшення допомагають забезпечити стабільну та безпечну роботу

активного обладнання, зберігаючи його точність та надійність.

У високотехнологічних приміщеннях, де розташоване активне обладнання, таке як сервери, комп'ютери чи інші пристрої, важливо контролювати рівень вібрації. Недостатня увага до цього може призвести до збоїв обладнання, втрати даних та зниження продуктивності.

Рекомендується дотримуватися конкретних стандартів, наприклад, як у вашому випадку, де вказано, що амплітуда коливань в діапазоні до 25 Гц не повинна перевищувати 0.1 мм. Дотримання цих параметрів допоможе уникнути негативного впливу вібрації на обладнання та забезпечити його нормальну роботу.

Багато джерел розміщує апаратну в геометричному центрі будівлі тому, що дозволяє істотно заощадити на прокладці кабелю.

Розміщення апаратної кімнати у геометричному центрі будівлі може мати свої переваги з точки зору ефективності розташування обладнання та економії на прокладці кабелю.

Центральне розташування апаратної кімнати може дозволити оптимізувати довжину кабельних маршрутів для з'єднання з іншими приміщеннями чи точками доступу. Це може спростити процес прокладки кабелів, оскільки коротші маршрути кабелів можуть заощадити час, кошти та зусилля при встановленні та обслуговуванні мережі.

Однак рішення щодо розташування апаратної кімнати в геометричному центрі будівлі повинно бути узгодженим з рядом інших факторів, таких як доступність, вентиляція, системи безпеки та інші технічні обмеження. Важливо враховувати ці фактори при плануванні розташування апаратної кімнати, щоб забезпечити оптимальну роботу обладнання та забезпечити безпеку його функціонування.

В кінцевому рахунку розташування апаратної кімнати в геометричному центрі може бути раціональним рішенням, але це повинно бути зроблено з урахуванням всіх аспектів ефективності та безпеки роботи системи.

Через апаратну не повинні бути прокладині транзитом трубопроводи

інженерних систем будівлі.

Це правило, яке забороняє прокладку трубопроводів транзитом через апаратну кімнату, часто встановлюється з метою забезпечення безпеки та надійності роботи обладнання в кімнаті. Прокладка транзитних трубопроводів через приміщення з обладнанням може створювати потенційні загрози для роботи цього обладнання та відсутності його нормальної функціональності.

Такі трубопроводи можуть мати ризики, такі як ризик пошкодження обладнання під час проведення робіт з трубопроводами або непередбачувані ситуації, які можуть виникнути у випадку аварійного стану трубопроводу, що може вплинути на роботу обладнання в апаратній кімнаті.

Заборона прокладки трубопроводів транзитом через апаратну кімнату спрямована на збереження безпеки і надійності роботи обладнання, яке зазвичай потребує стабільного і безперебійного живлення та функціонування. Це може також полегшити планування обслуговування та ремонту обладнання, уникнути можливих конфліктів із зонами доступу для технічного обслуговування.

Забороняється розташовувати апаратну кімнату поряд із приміщеннями для зберігання пожежонебезпечних або агресивних хімічних матеріалів.

Це обмеження зазвичай встановлюється з метою забезпечення безпеки та уникнення потенційних небезпек, які можуть виникнути в разі взаємодії апаратної кімнати із пожежонебезпечними або агресивними хімічними речовинами.

Приміщення для зберігання таких матеріалів часто має специфічні умови зберігання, які можуть створювати потенційні ризики для обладнання, яке працює в апаратній кімнаті. Взаємодія з хімічними речовинами може призвести до пошкоджень обладнання, виникнення корозії або навіть до небезпеки виникнення пожежі чи викиду шкідливих речовин.

Такі правила спрямовані на те, щоб максимально уникнути потенційних небезпек, забезпечити безпечну експлуатацію апаратної кімнати та зберегти її працездатність без ризику взаємодії з пожежонебезпечними або агресивними хімічними речовинами.

Забороняється розташовувати апаратну в приміщенні, яка межує

з приміщенням виробництв з мокрими технологічними процесами.

Приміщення невиділяються для апаратної кімнати на верхніх поверхах будівлі, оскільки вони найбільш схильні до пошкоджень та у разі пожежі і можуть заливатися при протіканнях даху.

Забороняється розміщувати серверне приміщення поруч з сходовими прольотами, ліфтовими шахтами, великими вентиляційними каналами, які згідно існуючого планування, можуть обмежити розширення серверного приміщення в майбутньому.

Це правило важливе для забезпечення безпеки та зручності експлуатації серверного приміщення. Розміщення його поруч з сходовими прольотами, ліфтовими шахтами та великими вентиляційними каналами може обмежити можливість розширення приміщення у майбутньому через вже зайняте простір або вплив на існуючу інфраструктуру.

А саме спрямоване на те, щоб забезпечити можливість безперешкодного розширення або модернізації серверного приміщення у майбутньому, не обмежуючи його можливостей через обмежений доступ або вже встановлену інфраструктуру поруч.

Не допускається розміщення апаратної кімнати під приміщеннями, пов'язаними зі використанням води.

Це правило стосується безпеки та запобігання можливим ризикам у випадку витоку води або інших проблем, пов'язаних з водопроводом, які можуть негативно вплинути на апаратну кімнату. Розміщення апаратної кімнати під приміщеннями, де використовується вода (наприклад, ванні кімнати, пральні, кухні), може створити серйозні проблеми у разі витоку або затоплення.

Це правило спрямоване на те, щоб уникнути потенційних негараздів або втрати обладнання в разі водяного лиха у вище зазначених приміщеннях. Розташування апаратної кімнати у безпечному місці, де ризик впливу води буде мінімальним, допомагає забезпечити надійну роботу обладнання та зменшити ймовірність пошкоджень в разі аварій.

Серверні приміщення мають розміщуватись осторонь від джерел

електромагнітних завад на тій відстані, щоб напруженість електричного поля не перевищувала 3 В/м у всьому спектрі частот [28].

Це допомагає запобігти негативному впливу електромагнітних полів на обладнання. Для обмеження напруженості електричного поля до 3 В/м в усьому спектрі частот є досить типовою. Висока напруженість електромагнітного поля може стати причиною перешкод у роботі обладнання, особливо серверів, що може призвести до зниження продуктивності та надійності системи.

Тому важливо ретельно планувати розміщення серверних приміщень, дотримуючись рекомендацій з обмеження електромагнітних завад для забезпечення стабільної та безпечної роботи обладнання.

Серверне приміщення необхідно розміщувати таким чином, щоб була можливість розширити приміщення за рахунок площі приміщення що знаходиться поруч. Також слід враховувати розташування несучих перекриттів, щоб була необхідність за можливості збільшити простір апаратного приміщення шляхом демонтажу суміжних з сусіднім приміщенням стін [28].

Розміри серверного приміщення вибираються виходячи з розміру обслуговуємої робочої області і кількості встановленого обладнання. Необхідно враховувати не тільки розміри самого обладнання, а й способи монтажу, забезпечити доступ та обслуговування обладнання, можливість установки додаткових пристроїв та інше. Необхідно щоб був простір для можливості монтажних маневрів [28].

Параметри для монтажу обладнання у серверному приміщенні включають висоту не менше 2,44 метра для комфортного доступу та обслуговування обладнання, мінімальний розмір приміщення не менше 14 м² для вміщення необхідного обладнання та забезпечення ефективної організації простору, а також виділення 0,09 м² площі на кожні 10 м² робочої зони для спеціального розміщення серверів у великих офісах чи будівлях. Дотримання цих параметрів сприяє оптимальному функціонуванню обладнання та забезпечує належні умови для технічного обслуговування. [28].

При будівництві приміщення для серверної кімнати необхідно враховувати

декілька важливих аспектів. Серед них - ефективне розташування обладнання для забезпечення зручного доступу та обслуговування, захист приміщення від доступу для сторонніх, що може включати системи контролю доступу та безпеки даних, захист обладнання від збоїв живлення шляхом використання безперебійних джерел живлення та стабільного мікроклімату для забезпечення оптимальних умов для роботи серверів і зниження ризику перегріву чи інших проблем, пов'язаних з температурою та вологою. [29].

Гідроізоляція відіграє велику роль, оскільки приміщення має дуже багато електроприладів високої напруги і попадання вологи або води може призвести до виводу з ладу обладнання, пожежі травм або найгірше людських жертв.

Потрапляння вологи або води до цих приміщень може призвести до серйозних наслідків, включаючи виходження з ладу обладнання, коротке

замикання, загрозу пожежі та потенційну загрозу для життя та здоров'я людей.

Гідроізоляція допомагає убезпечити приміщення від проникнення вологи ззовні та мінімізує ризик потрапляння води у приміщення, де розташовані електричні пристрої. Це важливий захист, що забезпечує безпеку обладнання, працівників та користувачів приміщення.

Дотримання відповідних норм гідроізоляції є ключовим для забезпечення безпеки та ефективної роботи електрообладнання в умовах, де є потенційний ризик вологи. Це може включати застосування спеціальних матеріалів, технологій укладання та інших заходів для запобігання проникненню води та забезпечення безпеки в таких приміщеннях.

Необхідно уникати розміщення серверного приміщення нижче рівня поверхні землі, якщо приміщення не забезпечено захистом від проникнення води потрібно враховувати нижчевикладені фактори [28].

У серверній кімнаті не повинно бути розміщених трубопроводів і дренажних систем, якщо вони не призначені для роботи обладнання і спеціальних систем розміщених безпосередньо в ній.

У випадку, якщо існує ризик потрапляння води в серверне приміщення, розумною буде установка системи дренажу. Це може включати в себе встановлення дренажних каналів, водостічних систем або спеціальних насосів для відведення води у разі затоплення чи протікання.

Дренажна система допоможе уникнути негативних наслідків від затоплення, зберігши серверне обладнання та інфраструктуру в безпеці. Це важливий захід безпеки, який може мінімізувати потенційні збитки у разі виникнення проблем із водою.

Установка дренажних каналів під трубопроводами, які приєднані до аварійних розпилювачів води при пожежі (спринклерів), є розумним заходом для захисту серверного обладнання від можливого протікання.

Це важливий захід безпеки, який допоможе уникнути можливих пошкоджень обладнання в разі активації системи спринклерів у випадку пожежі. Дренажні канали допоможуть відведенню води від розпилювачів, запобігаючи потенційному затопленню приміщення та захищаючи сервери й інші компоненти від впливу води.

Це важливий елемент плану безпеки, спрямований на збереження функціональності та надійності серверної інфраструктури в найекстремальніших ситуаціях, таких як пожежа. [28].

Зазвичай серверні приміщення будують без вікон для забезпечення кращих умов для обладнання. Але, якщо вони все ж таки мають вікна, рекомендацією є закладення їх цеглою або іншими матеріалами, що не пропускають світло, для зменшення впливу зовнішнього освітлення на сервери та інші компоненти.

У випадку, коли вікна не можуть бути виключені, розташування апаратної частини на північній або північно-східній стороні будівлі може бути розумним рішенням. Це допоможе зменшити теплове навантаження на приміщення через сонячне випромінювання, оскільки північні або північно-східні стіни отримують менше сонячного світла протягом дня.

Це може сприяти підтримці стабільної температури в приміщенні, що є важливим для оптимальної роботи серверного обладнання, оскільки

температурний режим має велике значення для ефективності та довговічності компонентів. [28].

Так, у багатьох випадках в апаратних кімнатах серверних приміщень використання підвісної фальшстелі може бути не рекомендованою практикою.

Підвісна фальшстеля може створювати простір між підлогою та стелею, що може бути використано для прокладання кабелів, вентиляційних систем, та іншого обладнання. Однак, в умовах серверних приміщень це може створювати певні проблеми.

Фальшстеля може ускладнити рівномірне розподілення тепла в приміщенні, що може призвести до збільшення температурного градієнту та перегріву електронного обладнання.

Використання підвісної стелі може ускладнити налагодження систем вентиляції та охолодження, що є критичними факторами для підтримки оптимальної температури в серверних приміщеннях.

Підвісна фальшстеля може ускладнити доступ до обладнання для технічного обслуговування, ремонту та заміни компонентів.

У більшості випадків, для забезпечення оптимальних умов експлуатації серверного обладнання, розглядають конструкції без підвісної фальшстелі, щоб забезпечити ефективне охолодження, хорошу вентиляцію та легкий доступ для обслуговування. [28].

Оздоблення приміщення має наступні параметри:

Мінімальна висота апаратної стелі має становити 2,44 м.

Поли в апаратній кімнаті повинні бути рівними і мати антистатичне покриття з опором 106 Ом, щоб забезпечити стікання і відведення статичної електрики. Настил підлоги здійснюється на незгораючу підставу. Покриття має дозволяти виконувати очитку пилососом і вологе прибирання.

Максимально допустиме навантаження на підлогу в апаратній кімнаті повинне становити: розподілене навантаження не більше 12 кПа; зосереджене навантаження не більше 4,4 кН [28].

Апаратне оснащення серверної кімнати має включати в себе підсистеми: охоронної сигналізації; пожежної сигналізації; пожежогасіння; контролю доступу; кондиціонування; освітлення; аварійне освітлення (для роботи при відключенні робочого освітлення) [28].

Для забезпечення безпеки важливо встановити систему датчиків, налаштованих на виявлення диму в приміщенні, а також датчики, що реагують на критичне підвищення температури. Датчики протікання води повинні бути розміщені по периметру серверної кімнати, під кожним пристроєм обладнання та під кожною трубою. Важливо мати центр керування, який автоматично активує систему пожежогасіння при отриманні тривожного сигналу від датчиків.

Системи газового пожежогасіння на сьогоднішній день є надійними і безпечними. Це пояснюється їх високою швидкістю розповсюдження газу та здатністю проникнення у важкодоступні ділянки приміщення. Ці властивості роблять системи газового пожежогасіння практично необхідними для приміщень, що мають велике значення, включаючи серверні кімнати [26].

Правильне заземлення є критичним для безпеки та надійності серверної інфраструктури. У серверних кімнатах дійсно повинно бути захисне і телекомунікаційне заземлення для всього апаратного оснащення.

Захисне заземлення призначене для відводу електричного струму, що може виникнути внаслідок перенапруги чи короткого замикання. Таке заземлення допомагає запобігти пошкодженню обладнання та забезпечує безпеку приміщення від електричних небезпек.

Телекомунікаційне заземлення, у свою чергу, забезпечує ефективну передачу даних і сигналів без шумів або перешкод. Це важливо для забезпечення стабільної та надійної роботи мережевого обладнання.

Також, можливість підключення безпосередньо до головної пластини заземлення для апаратної частини є важливим аспектом. Це забезпечує найкоротший можливий шлях для відводу електричного струму в разі потреби, що є важливим для попередження пошкоджень обладнання та забезпечення безпеки всієї інфраструктури. [28].

Серверне приміщення має свій рівень температури вологості, вентиляції тому є певні вимоги та рекомендації щодо підтримки мікроклімату у серверній кімнаті а саме:

Система контролю і управління мікрокліматом має забезпечити заданий рівень вологості і температури який необхідний для нормального функціонування активного обладнання.

Система мікроклімату повинна забезпечити підтримку температурного режиму як влітку так і взимку, яка розрахована до цілодобової безперервної роботи.

У випадку коли централізована система мікроклімату в будівлі не може забезпечити безперервну роботу і заданий рівень температури і вологості, то є необхідність встановити автономну систему у кімнаті.

При повітряному охолодженні вимір температури і вологості повинен здійснюватися при працюючому активному обладнанні на висоті 1.5 метра від рівня підлоги в зоні подачі холодного потоку повітря.

Якщо є водяне охолодження вимір температури і вологості має здійснюватися при працюючому активному обладнанні в монтажному конструктиві.

Необхідно забезпечити повітряний тиск більше а ніж в прилеглих приміщеннях.

Повинна бути повна зміна повітря не рідше 1 разу на годину, якщо в приміщенні постійно працює обслуговуючий персонал.

Необхідно використовувати систему очищення і фільтрації повітря, що поступає до апаратного приміщення.

Якщо в будинку є система резервного електроживлення, то тоді система підтримки мікроклімату повинна бути до неї підключена [28].

Сервери виробляють значну кількість тепла, і висока температура в серверній кімнаті може призвести до перегріву компонентів, що спричинить їх виход з ладу та значні фінансові втрати від простоїв. Рекомендована температура в серверних кімнатах зазвичай становить близько 22°C. Сучасні сервери можуть

працювати при більш високих температурах, але це збільшує ризик відмови компонентів.

Для підтримання стійкої температури в серверній кімнаті використовуються спеціальні кондиціонери і системи вентиляції. Зазвичай встановлюють по два кондиціонери для підвищення надійності - як основний, так і резервний. Датчики температури/повітряного потоку розміщують біля кожного кондиціонера для попереднього виявлення можливих несправностей.

Контроль вологості також важливий у серверних кімнатах. Оптимальний рівень вологості зазвичай знаходиться між 40% і 60%. Надто сухе повітря може спричинити накопичення статичної електрики, тоді як занадто вологе може викликати корозію, що призведе до поступового пошкодження обладнання та його несправностей [26].

Таблиця 2.1 - Рекомендована температура і вологість в серверному приміщенні

Рекомендована температура, С °	Рекомендована відносна вологість, %
18-27	40-55

Серверне приміщення повинне бути добре захищене від пилу та шкідливих речовин, що можуть негативно впливати на функціонування обладнання. Для цього можна застосовувати різноманітні заходи, такі як використання спеціальних систем фільтрації повітря, контроль вологості та температури, герметизація приміщення та систематичне прибирання для зменшення накопичення пилу та забруднень на обладнанні.

Ці заходи є важливими для забезпечення надійності та тривалого функціонування серверного обладнання. Дотримання високих стандартів чистоти й утримання оптимальних умов у середовищі, де знаходяться сервери, не лише запобігає можливим поломкам та збоям обладнання, але й сприяє підвищенню продуктивності і зменшенню витрат на його обслуговування. Додатковою перевагою є збереження безперебійності роботи серверів, що є критично

важливим для багатьох організацій та підприємств, особливо у сфері інформаційних технологій та обробки даних.

Таблиця 2.2 - Гранично допустима норма шкідливих речовин в серверному приміщенні

Шкідлива речовина	Гранично допустима норма
Хлор	0.01 ppm (проміле)
Пил	100 мг/м ³ / на добу
Вуглеводороди	4 мг/м ³ / на добу
Сероводород	0.05 ppm (проміле)
Оксид азоту	0.1 ppm (проміле)
Діоксид сірки	0.3 ppm (проміле)

Якщо є необхідність для очіщення і фільтрації повітря що поступає до серверної, використовуються система для її очіщення. Застосування масляних фільтрів в апаратних не допускається [28].

Однак, у багатьох випадках застосування масляних фільтрів у системах очищення повітря в апаратних не рекомендується чи навіть забороняється.

Масляні фільтри можуть бути несприятливими для середовища серверної кімнати, оскільки масло може вилитися з фільтрів і потрапляти на обладнання, що призводить до забруднення та пошкодження компонентів. Крім того, масляні фільтри можуть стати джерелом викидів органічних речовин або парів, які можуть утворювати плівку або осідати на елементах обладнання, що також може вплинути на його ефективність та надійність.

Зазвичай у серверних кімнатах використовуються спеціальні системи фільтрації, такі як HEPA-фільтри або інші технології, які ефективно очищають повітря від пилу, частинок та інших забруднень без ризику витоку масла чи інших шкідливих речовин на обладнання.

Приміщення серверної повинно мати освітлення тому для цього є наступні вимоги: необхідність забезпечення освітлення не менше 500 люкс; рівень освітленості вимірюється на висоті 1 метра від рівня підлоги; електроживлення освітлення серверного приміщення та електроживлення телекомунікаційного

обладнання, яке встановлено в ньому має подаватися від різних розподільних електричних щитів; світильники мають бути розміщені на стелі; для управління освітленням використовується один або декілька вимикачів і розташовується поряд з дверима на висоті 1.5м від рівня підлоги; у серверних приміщеннях забороняється використовувати пристрої плавного регулювання освітлення [28].

Серверна кімната має електроживлення тому для приміщення висуваються описані нижче вимоги.

Необхідно як мінімум, два окремі блоки подвійних електричних розеток. Блоки електричних розеток мають жити від різних живильних кабелів, електричні розетки повинні бути розраховані на змінний струм до 16А. Додатково необхідно встановити блоки з подвійними електричними розетками з інтервалом 1,8 метра уздовж стіни на висоті не нижче 0,15 метра від рівня підлоги.

Подача електроживлення в серверне приміщення має здійснюватися по виділеному силовому кабелю, рекомендовано безпосередньо від головного розподільного щита.

Якщо є встановлена система резервного електроживлення, то серверне приміщення має бути до неї підключена.

Необхідно встановити окремий електричний розподільний щит.

Дозволяється установка джерел безперебійного живлення (ДБЖ) до 100 кВА. ДБЖ потужністю понад 100 кВА мають бути встановлені в окремому приміщенні [28].

В апаратному приміщенні встановлюється магістральна телекомунікаційна заземлювальна шина, до якої підключаються заземлюючі і сполучні провідники від монтажних конструктивів, телекомунікаційних обладнень та металевих кабелепроводів [28].

Засоби розподілу кабелів і організації кабельних потоків у серверних кімнатах:

Розподіл кабелів і організація кабельних потоків в телекомунікаційному приміщенні використовуються кабелепроводи і організатори.

Засоби розподілу і організації кабельних потоків мають бути надійно закріплені, витримувати вагу кабелю, мають забезпечити захист і розподіл кабелів з мінімально допустимим радіусом вигину всього кабелю.

Кабелепроводи встановлюються від кабельного вводу в телекомунікаційне приміщення до телекомунікаційних шаф.

Кабелепроводи які розташовуються під стелею, мають бути відкриті і доступні для проведення подальших робіт з прокладання кабелів, шнурів або перемичок.

Необхідно розміщувати кабельні вводи в апаратне приміщення поруч з дверима [28].

У кімнаті де буде розташовуватися уся апаратура необхідно мінімізувати шум від того коли вона буде у роботі, який може досягати значного рівня у великих серверних і заважати роботі інших співробітників. Кімната має бути добре ізольована і забезпечена щільно закривається дверима з електромагнітним замком, підключеним до локальної системи контролю і управління доступом [29].

Важливе обладнання з якого складається кожна серверна це стійки та шафи, при виборі спеціального оснащення для організації, яке необхідно розмістити і зафіксувати робоче обладнання. Тому для цього використовуються збірні металеві конструкції – шафи і стійки із стандартизованими габаритами, вимірюваними юнітами (1 юніт = 44,45 мм). Вони можуть бути навісними або підлоговими. Найбільш поширеним варіантом є стійка на 4-х опорах шириною 19" з різною глибиною (до 1,2 м). Які бувають закритого і відкритого типу. До вибору, де розміщувати та обслуговувати таке обладнання також існують специфічні вимоги, які надають фахівці. Розміщувати робочу апаратуру в стійках є зручним, та безпечним як для апаратури так і для персоналу [29].

Системи життєзабезпечення серверної у будь якій серверній кімнаті вимагається якісного і періодичного обслуговування та захисту від різних факторів. Скоротити витрати на обслуговування, ремонт і усунення наслідків різного роду аварій допоможуть додаткові системи життєзабезпечення:

безперебійного і резервного живлення; освітлення; вентиляції; пожежогасіння; система контролю та управління доступом.

Необхідно враховувати про державні і галузеві норми безпеки праці, експлуатації електроустановок та електрообладнання, відповідних будівельно-монтажних норм. Все це мають врахувати фахівці при проектуванні серверної кімнати [29].

Для забезпечення безпеки використовуються системи доступу через ключ-картку або біометричні дані. Ці системи гарантують, що лише авторизований персонал може отримати доступ до серверної кімнати. Це виключає можливість несанкціонованого доступу до конфіденційної інформації та обладнання, тим самим забезпечуючи безпеку. Крім того, ці системи допомагають забезпечити, що всі відвідувачі реєструються та відстежуються для подальшого аудиту [26].

2.2 Характеристика наявного об'єкта

Теплова електростанція яка є об'єктом критичної інфраструктури оскільки генерує електричну енергію яку невід'ємно споживають ті чи інші споживачі. Яка також являє собою доволі складну конструкцію для виробництва електроенергії, тому необхідно забезпечити її нормальне функціонування яке буде більш менш автоматизоване. Тому для такого об'єкту необхідна серверна система у відділі автоматизації, де будуть зберігатися: звіти, накази, данні про ремонт чи експлуатацію обладнання, диспетчеризація на щиті управління, та в цілому данні про роботу та спроможність електростанції.

Серверна система та її приміщення буде розроблятися по чинним стандартам які є на сьогоднішній день.

Апаратне устаткування серверної складається: сервери; маршрутизатори; комутатори; комп'ютери.

Електрична частина серверної складається: джерело змінного струму 220V, електрощитової; генераторів; джерела бесперебійного живлення; акумуляторні батареї.

2.3 Постановка задачі розробки

Для створення моделі серверної, яке буде займатися зберіганням, обробкою та передачею великої кількості даних, необхідно організувати надійний резерв. При цьому треба забезпечити бесперебійний доступ до електричної та інтернет мережі. Враховуючи всі ці фактори, необхідно обрати обладнання, яке зможе забезпечити швидку та бесперебійну роботу усієї серверної системи із використанням резерву та виконуватиме всі свої операції пов'язані з передачею, обробкою та збереженням даних.

3 РОЗРОБКА ОБЛАДНЕННЯ ТА МЕРЕЖ

3.1 Розробка структури серверверної шафи

У проєктуванні є необхідність мінімізувати витрати на розробку серверної шафи, включення лише необхідних компонентів у базовий варіант буде найкращим підходом. Це може включати в себе самі сервери або обладнання для зберігання даних, основні системи охолодження та живлення, необхідні мережеві з'єднання і системи безпеки.

Проте важливо також враховувати масштабованість та можливість майбутнього розширення. Навіть у базовому варіанті слід урахувати певний резерв для можливого збільшення місткості чи функціональності серверної шафи в майбутньому без значного перепланування або модернізації.

Часто вибір компонентів є мінімалістичний, щоб оптимізувати витрати відповідно до поточних потреб проекту, але з врахуванням можливості додаткового розвитку в майбутньому за потреби.

При розробці серверної шафи потрібно враховувати економічні вимоги, зокрема не витрачати зайві кошти. Тому базовий варіант обладнання серверної шафи включає тільки необхідні компоненти (рис.3.1):

- блоки розеток;
- органайзери;
- патч панелі;
- маршрутизатори;
- комутатори;
- сервер;
- RAID-масив;
- джерело живлення.

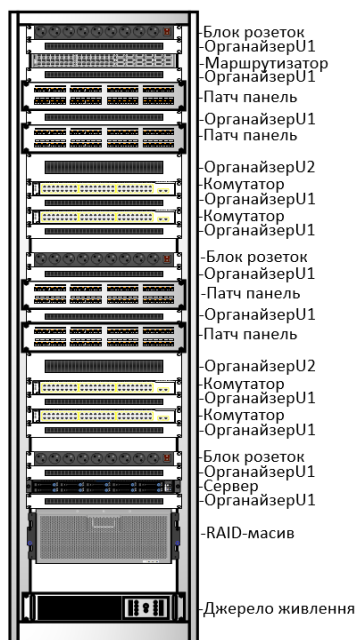


Рисунок 3.1 – Схема сервера із обладнанням

Обладнання що вибране та підключене у серверній показане на схемі (рис.3.2).

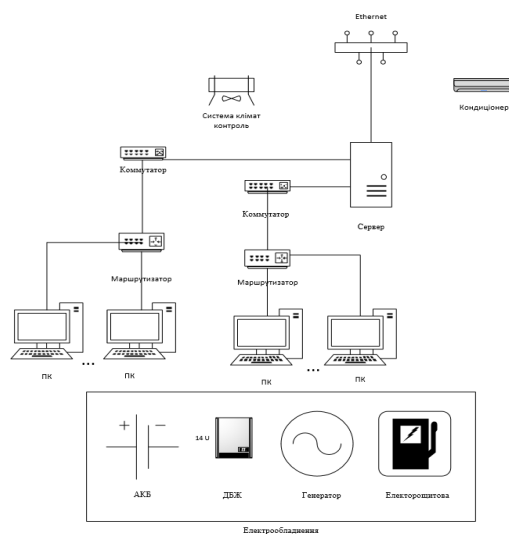


Рисунок 3.2 – Схема серверної кімнати, базове обладнання

Базове обладнання серверної кімнати включає в себе: сервер із виходом до ethernet, коммутатори, маршрутизатори, ПК. Охолодження у кімнаті проводиться із застосуванням: системи клімат контроль та кондиціонеру. Система живлення у кімнаті: Джерело змінного струму 220V, акумуляторна батарея, джерело бесперебійного живлення, генератор, електрощитова.

3.2 Розробка електромережі

Електромережа у серверній кімнаті є критично важливою для неперервної роботи обладнання. Вона зазвичай складається з основних джерел живлення, резервних джерел живлення, систем бесперебійного живлення (UPS), аварійних генераторів та блоків розподілу напруги.

Основні джерела живлення - це електромережі, які постачають стандартне електричне живлення в приміщення, включаючи сервери та інше обладнання. Резервні джерела живлення використовуються у випадку відмови основних джерел, забезпечуючи бесперебійність електропостачання.

Системи безперебійного живлення (UPS) є іншим важливим компонентом, які забезпечують постійну подачу електроенергії у випадку відключення основного джерела живлення. Вони дають короточасну можливість продовжувати роботу обладнання або запускати аварійний генератор.

Аварійні генератори є резервними джерелами електроживлення та активуються у випадку тривалого відключення основних джерел електроенергії.

Блоки розподілу напруги забезпечують зручний доступ та підключення обладнання до електромережі.

Ці компоненти разом створюють ефективну та надійну електромережу для серверної кімнати, що дозволяє підтримувати безперебійну роботу серверів та іншого обладнання, навіть у непередбачуваних ситуаціях.

Для серверних кімнат, як і для будь-яких приміщень важливого значення, критично важливо мати захист від надзвичайних ситуацій. Для забезпечення безперебійного живлення, необхідно використовувати систему резервного живлення, яка автоматично перемикає живлення з одного джерела на інше у випадку несправності основного джерела. Наявність аварійного генератора у випадку відключення електроенергії на обох джерелах забезпечує неперервну роботу систем.

Це забезпечує захист обладнання від пошкоджень та надалі дозволяє системам працювати. Важливо мати на увазі, що час, необхідний для запуску генератора, становить від 1 до 4 хвилин, і в цей час слід забезпечити безперебійне живлення від джерела безперебійного живлення (UPS). UPS забезпечує електроживлення під час коротких перерв у подачі електроенергії та є тимчасовим рішенням.

Також важливо мати блоки розподілу напруги у стійках, які спрощують підключення обладнання до живлення та дозволяють зручний доступ.

Відмова електромережі у серверній кімнаті може призвести до серйозних простоїв в роботі систем, порушення роботи комп'ютерів та іншого обладнання, що може спричинити втрату даних та завдати значних фінансових збитків компанії. Тому важливо мати надійну та дубльовану електромережу, яка

забезпечує стабільну роботу серверів навіть у випадку виникнення проблем з основним живленням [26].

Електромережа серверної кімнати до якої будуть під'єднані наступні пристрої зображені на схемі: сервер, коммутатор, маршрутизатор, ПК, система клімат контроль, кондиціонер, джерело змінного струму, електрощитова, 2 генератори, заземлення, акумуляторна батарея, джерело безперебійного живлення (рис.3.3).

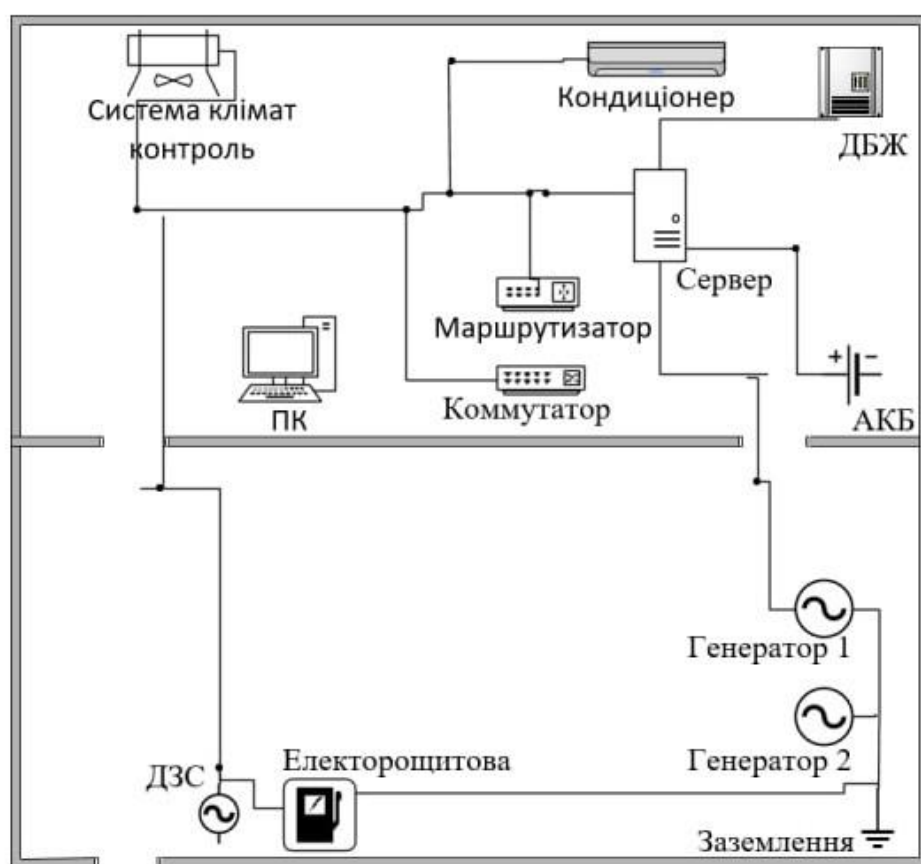


Рисунок 3.3 – Схема електромережі серверної кімнати

Виходячи зі схеми можна сказати, що всі пристрої знаходяться на своїх місцях та мають резервне живлення у разі непередбачених випадках із електроживленням.

3.3 Розробка топології мережі

Схема топології мережі відділу автоматизації, буде розроблена та змодельована у Cisco Packet Tracer.

Топологія комп'ютерної мережі відділу автоматизації включає в себе: 1 сервер, 2 комутатори Cisco 2960-24TT, 3 маршрутизатори Cisco 1941 та 15 комп'ютерів (рис.3.3).

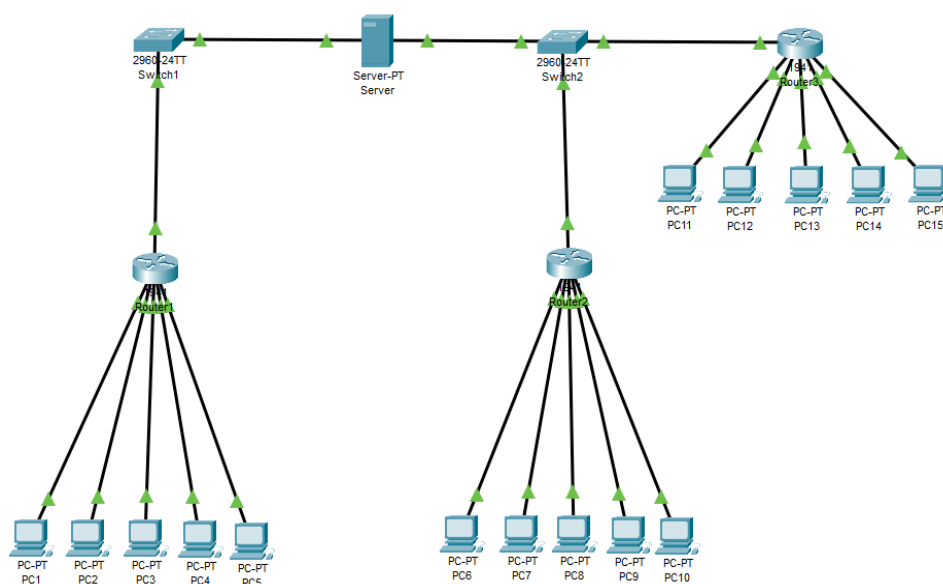


Рисунок 3.4 – Схема топології мережі відділу автоматизації

Серверна яка має мережеве обладнання буде мати наступну базову модель OSI по рівням:

- фізичний рівень (Physical Layer): комп'ютер, комутатор;
- канальний рівень (Data Link Layer): комп'ютер, Комутатор;
- мережевий рівень (Network Layer): маршрутизатор, комп'ютер;
- транспортний рівень (Transport Layer): комп'ютер, сервер;
- рівень сеансів (Session Layer): сервер;
- рівень представлення (Presentation Layer)

- рівень додатків (Application Layer): сервер, комп'ютер.

4 ПІДВИЩЕННЯ НАДІЙНОСТІ СЕРВЕРНОЇ СИСТЕМИ

4.1 Побудова графа надійності

Для оцінки показників надійності в даній роботі використовується метод мінімальних шляхів і мінімальних перетинів (МШ\МП). Цей метод дає можливість оцінити верхню і нижню межу показника вірогідності безвідмовної роботи системи:

$$P_H < P_C < P_B$$

Цей метод є простим у порівнянні з точними методами, тому багато де широко застосовується для оцінки складних обчислювальних систем.

По графу надійності спочатку знаходяться "мінімальні перетини" та "мінімальні шляхи", потім будуються еквівалентні графи для "мінімальних перетинів" та "мінімальних шляхів" для розрахунку P_H та P_B .

Мінімальний шлях має складатися із мінімальної послідовності підсистем, які входять до графу (P_B) які необхідні для передачі даних від початкового до кінцевого пристрою, від вершини А до вершини В. У складних резервованих системах, є декілька мінімальних шляхів і кожен наступний приймається за новий мінімальний, якщо вважати, що попередні відказали. До множини мінімальних шляхів входять усі можливі комбінації напрямків передачі даних.

Мінімальний перетин має складатися з мінімальної кількості підсистем графа (P_H), відмова яких веде до відмови системи, незалежно від стану інших підсистем. До множини мінімальних перетинів входять усі можливі комбінації перетинів, які приводять до відмови системи.

Імовірність P_H знаходять через еквівалентний граф перетинів, складений з послідовно ввімкнених груп підсистем усіх мінімальних перетинів, де в кожній

групі підсистеми включені паралельно.

Імовірність P_v знаходять через еквівалентний граф шляхів, складений з груп послідовно включених підсистем кожного мінімального шляху; групи усіх мінімальних шляхів системи включені паралельно.

Щоб застосувати МШ\МП, побудуємо граф надійності мережі (рис.4.2), використовуючи перехідний граф (рис.4.1), побудований на підставі схеми мережі (рис. 3.4).

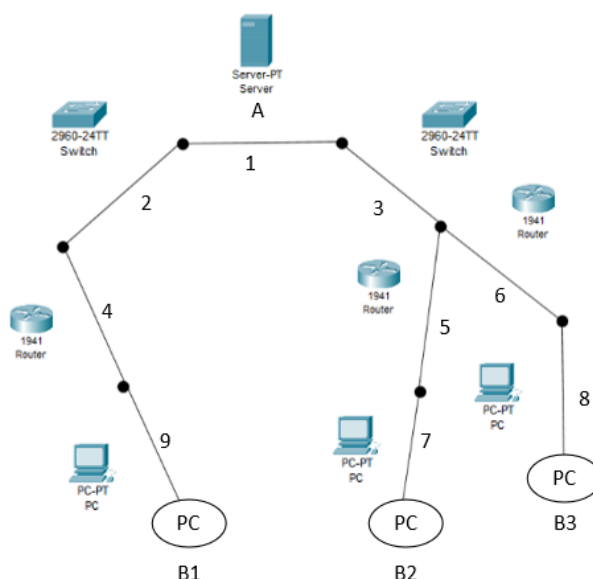


Рисунок 4.1 – Перехідний граф

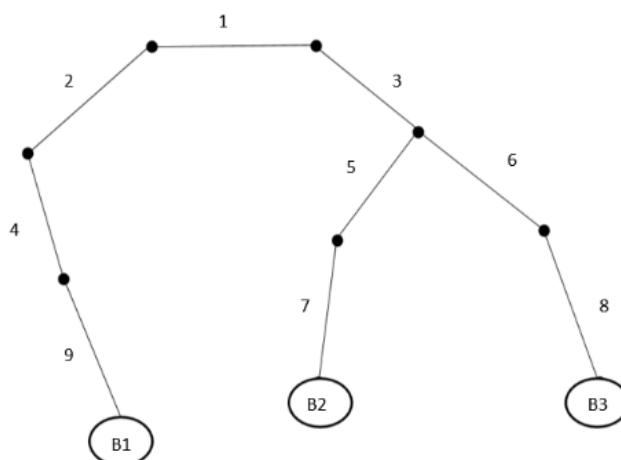


Рисунок 4.2 – Граф надійності мережі

По графу надійності визначимо мінімальні перетини 1-2-4-9, 1-3-5-7, 1-3-6-8, а також мінімальні шляхи – А-В1: 1249, А-В2: 1357, А-В3: 1368. Оскільки граф відображує найпростішу, нерезервовану базову схему мережі з топологією «дерево», то ці множини співпадають.

Для нижньої оцінки P_n потрібно розрахувати показник ВБР для послідовно включених груп мінімальних перетинів.

Для верхньої оцінки P_v потрібно розрахувати показник ВБР для паралельно включених груп мінімальних шляхів.

Припустимо, що імовірності відмови приладів однакові і дорівнюють 0,9, тоді імовірність безвідмовної роботи визначається як $q=1-p=1-0.9=0.1$.

Імовірність безвідмовної роботи для мінімальних шляхів знаходимо, як добуток часткових значень P для кожного ребра на одному мінімальному шляху:

$$P_{\text{посл}} = \prod_{i=1}^n p_i ;$$

$$P_v(A, B1) = p1 * p2 * p4 * p9 = 0,9 * 0,9 * 0,9 * 0,9 = 0,6561$$

$$P_v(A, B2) = p1 * p3 * p5 * p7 = 0,9 * 0,9 * 0,9 * 0,9 = 0,6561$$

$$P_v(A, B3) = p1 * p3 * p6 * p8 = 0,9 * 0,9 * 0,9 * 0,9 = 0,6561$$

Після перетворення для трьох та чотирьох послідовно включених ребер для імовірностей безвідмовної роботи по графу мінімальних шляхів, визначимо їх загальну верхню імовірність P_v при паралельній структурі за формулою:

$$P_{\text{парал}} = 1 - \prod_{i=1}^n (1 - p_i), \text{ де } p_i = 1 - q$$

Тоді отримаємо значення P_n , яке для даного випадку дорівнює P_v . Це відбувається тому, що в даній структурі мережі граф мінімальних шляхів співпадає з графом мінімальних перетинів. Таким чином, для найпростішої конфігурації базової мережі $P_c = P_n = P_v = 0,6561$.

Таке значення ВБР не може задовольняти вимоги до надійності мережі на підприємстві критичної інфраструктури. Тому необхідно вживати заходи з поліпшення показника вірогідності безвідмовної роботи. При цьому необхідно враховувати не тільки електронне обладнання мережі і серверної кімнати, а також пристрої електроживлення і клімат-контроля.

4.2 Вибір резерву серверної та електрообладнання

Підвищити показники вірогідності безвідмовної роботи сервера і мережі загалом в даному випадку можна або зміною топології мережі, тобто обрати більш надійну ніж дерево, або способом резервування. Зміна топології мережі не передбачена технічним завданням, оскільки вимагає організаційних заходів з боку підприємства. Тоді розглядаємо підвищення надійності мережі із застосуванням резервування – це найпростіший і найпоширеніший спосіб (рис.4.3).

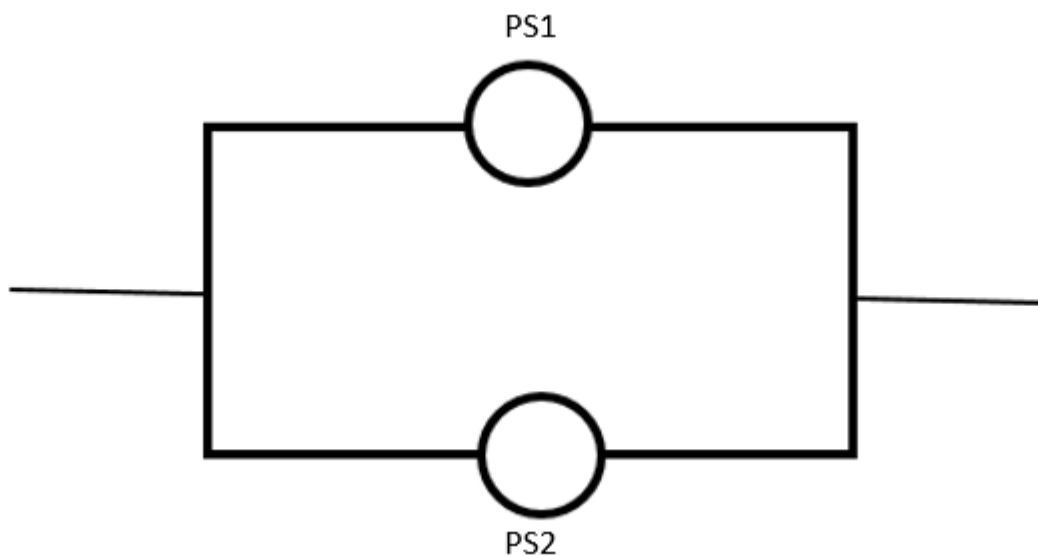


Рисунок 4.3 – Граф надійності резервованого елемента

Резервування PS1 PS2, а саме резерв таких елементів як: сервер1 та сервер2, зображені на рис. 4.3.

Розрахуємо вірогідність безвідмовної роботи PS1- для Server 1, ВБР PS2- для Server 2:

$$P_{serv}=1-(1-P_{s1})(1-P_{s2})=1-(1-0,9)*(1-0,9)=0,99$$

Аналогічно для для комутаторів Sw1, Sw2, Sw3 при дублюванні отримаємо $P_{sw}=0,99$.

Аналогічно для резерву $P_r=0,99$.

Таким чином $P_H=P_V=0,99*0,99*0,99*0,99=0,96$, тобто верхня ті нижня оцінки вірогідності безвідмовної роботи рівні між собою.

4.3 Дослідження резервованої мережі

Для перевірки попередніх результатів обчислень побудуємо перехідний граф резервованої мережі (рис.4.4) на основі графа нерезервованої мережі (рис. 4.4).

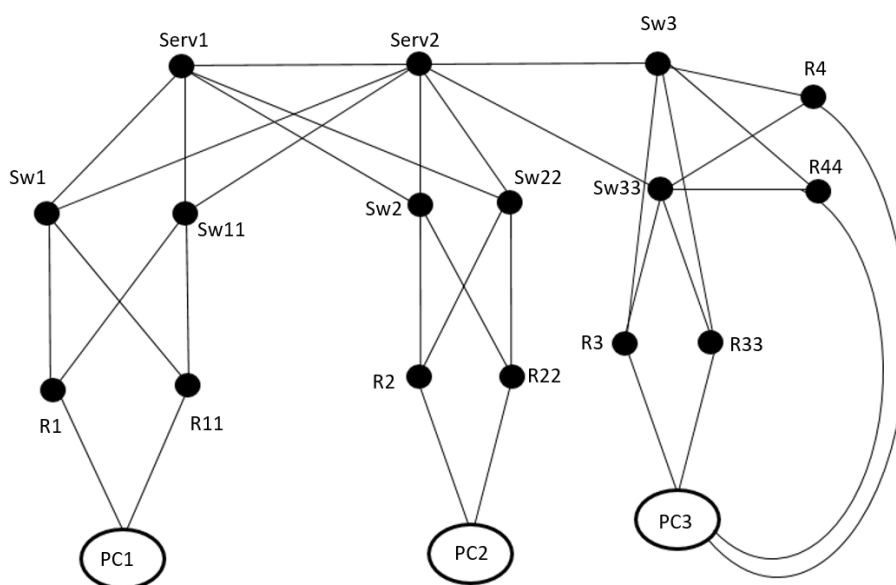


Рисунок 4.4 – Перехідний граф резервовної мережі

Виконаємо розрахунки мінімальних шляхів та мінімальних перетинів для резервованого графа надійності.

Мінімальний шлях:

AB1: 1-3-5-7, 1-4-6-8, 1-3-6-8, 1-3-6-7, 1-3-5-8, 1-3-5-7, 2-4-6-8, 2-3-6-8, 2-3-5-7, 2-3-6-7, 2-4-6-8.

AB2: 1-10-12-14, 1-9-12-13, 1-10-11-13, 2-9-11-13, 2-10-12-14, 2-9-12-13, 2-9-11-14, 2-10-11-14, 2-10-11-13, 1-9-12-14, 1-9-11-14.

AB3: 1-10-15-17, 2-9-16-18, 1-9-15-17, 1-10-16-18, 1-9-15-17, 2-10-15-17, 2-9-15-17, 2-10-16-18, 2-9-15-17,

Мінімальний перетин:

AB1: 1-2, 3-4, 5-6, 7-8.

AB2: 1-2, 9-10, 11-12, 13-14.

AB3: 1-2, 9-10, 15-16, 17-18.

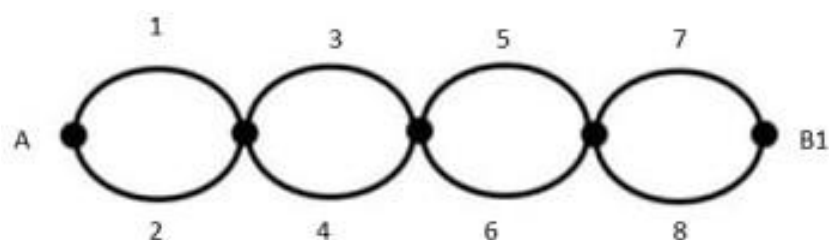


Рисунок 4.6 – Еквівалентний граф мінімальних перетинів AB1

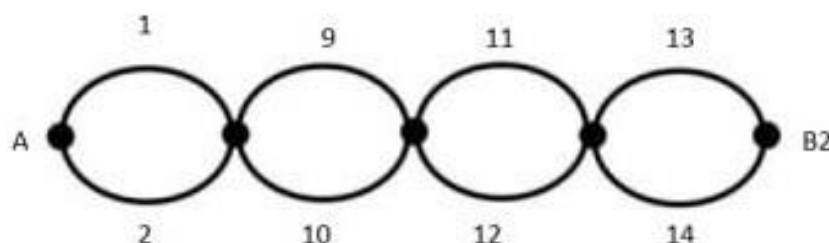


Рисунок 4.7 – Еквівалентний граф мінімальних перетинів AB2

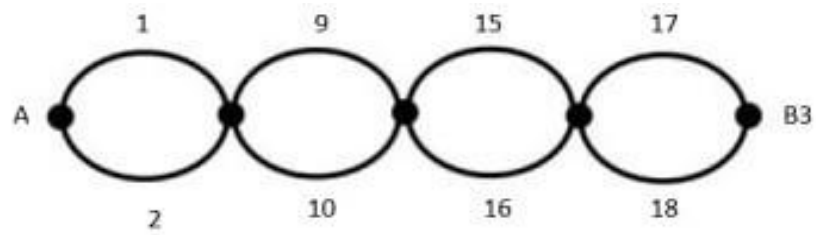


Рисунок 4.8 – Еквівалентний граф мінімальних перетинів АВЗ

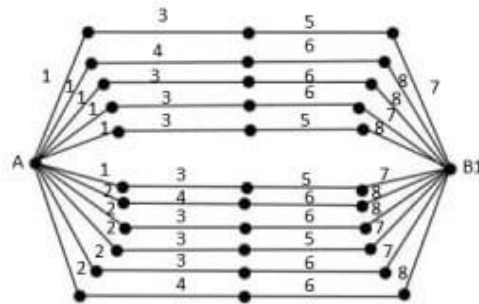


Рисунок 4.9 – Еквівалентний граф мінімальних шляхів А-В1

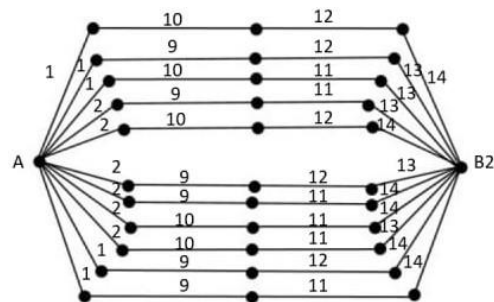


Рисунок 4.10 – Еквівалентний граф мінімальних шляхів А-В2

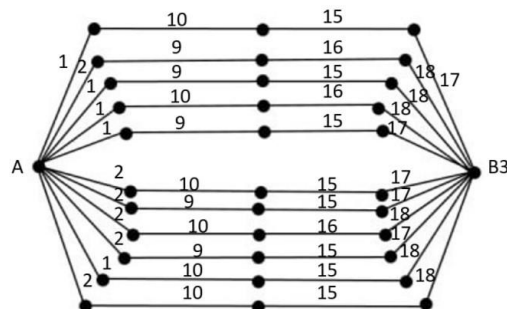


Рисунок 4.11 – Еквівалентний граф мінімальних шляхів А-В3

Кожен ланцюжок містить 4 сегменти, тобто шляхи АВ1, АВ2, АВ3 мають однакову довжину. Тому всі три графа шляхів мають бути однакового розміру.

Розрахунок оцінки ВБР для мінімальних перетинів:

$$P_H = [1-(1-P_2)(1-P_1)] * [1-(1-P_3)(1-P_4)] * [1-(1-P_5)(1-P_6)] * [1-(P_7)(1-P_8)] = (1-0,1*0,1) = 0,99 = 0,9606.$$

Отже, доведено, що показник вірогідності безвідмовної роботи мережі покращений на 48% за рахунок резервування основних елементів.

4.4 Тестування резервованої мережі

Топологія мережі зі своїх технічних можливостей зарезервована у холодний резерв, зображена на рисунку 4. До топології додано: А - Сервер 2, В1 – коммутатор 11, маршрутизатор 11, В2 – коммутатор 22, маршрутизатор 22, В1 – коммутатор 33, маршрутизатор 33 а також маршрутизатори 4 та 44 (рис.4.12).

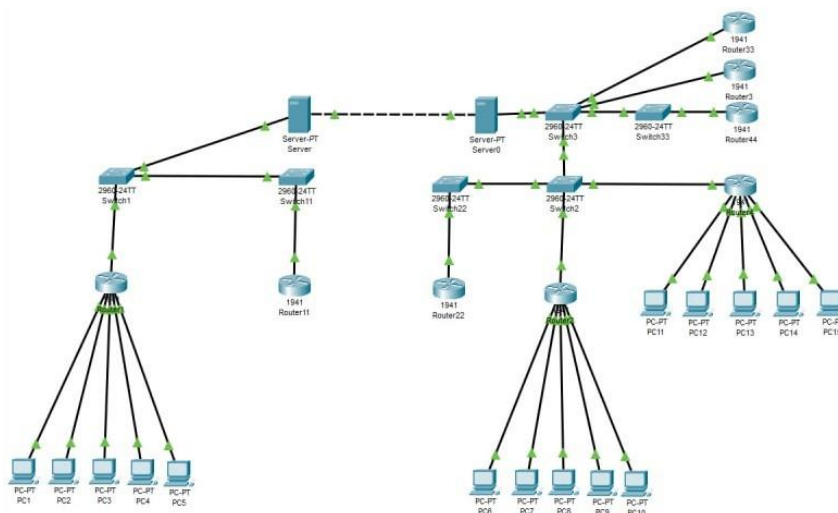


Рисунок 4.12 – Тестування топології резервованої мережі

Як видно на рисунку 4.12 мережа, що протестована у Packet Tracer, є роботоспроможною із урахуванням резерву.

ВИСНОВКИ

В межах розробки системи серверного обладнання для об'єкту критичної інфраструктури з використанням технології резерву, вирішені всі задачі, поставлені в технічному завданні.

Розроблено серверне обладнання та мережі для серверної кімнати.

Розроблено електрично мережу із резервним обладнанням для серверної кімнати.

Створено топологію мережі об'єкту критичної інфраструктури, котра забезпечить нормальну роботу спроможність відділу автоматизації.

Проведено аналіз підвищення надійності серверної системи, мережевого обладнання, із побудовою графа надійності мережі.

Обраний резерв серверної та електрообладнання.

Досліджено резервовану мережу та побудован граф надійності.

У пакеті моделювання Cisco Packet Tracer, створено віртуальну модель, яка повністю відповідатиме реальній мережі із застосуванням холодного та гарячого резерву.

В результаті проведеного аналізу визначено, що мета роботи досягнута в повному обсязі.

Головним результатом моделювання є доказ працездатності запропонованої моделі та її функціональності у відповідності з поставленими вимогами.

Таким чином, в результаті виконання магістерської роботи було вирішено актуальну інженерно-наукову задачу: дослідження засобів для підвищення надійності серверних установок та технології для створення ефективного резерву.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Офіційний вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/laws/show/563-2016-п/paran17#n17> (дата звернення: 21.11.2023).

2 Шмиг Р. А. Боярчук В. М. Добрянський І. М. Барабаш. В. М. Термінологічний словник-довідник з будівництва та архітектури : Словник-довідник. Львів : Львів. нац. аграр. ун-т, 2010. 222 с.

3 Інженерні рішення для енергетики. Промислова автоматизація. URL: https://svitovyr.ua/upload/landing/631/DSC_0393@1x.jpg (дата звернення: 01.11.2023).

4 Різниця між ТЕС і ТЕЦ - Dovidka.biz.ua. Dovidka.biz.ua. URL: <https://dovidka.biz.ua/riznitsya-mizh-tes-i-tets/> (дата звернення: 21.11.2023).

5 Новини Запоріжжя та області, Україна та Світ. Усі події дня, архів новин. - Газета МИГ. URL: <https://mig.com.ua/wp-content/uploads/2019/11/ja-t.jpg> (дата звернення: 21.11.2023).

6 Волочій Б.Ю. Моделі для надійнісного проектування вузла пам'яті сервера та джерела безперебійного електроживлення / Б.Ю. Волочій, Л.Д. Озірковський, О.В. Муляк, В. Гиля // Вісник НУ «Львівська політехніка». Радіотехніка та телекомунікації, 2011. №680, С. 206 -214

7 Осипенко О.В., Резервування серверів в системах відповідального призначення / О.В. Осипенко, І.Я. Зеленцова, Т.В. Голуб // Тиждень науки-2023. Факультет комп'ютерних наук і технологій : наук.-техн. конф., 24-28 квітня 2023 р. : тези доп. – / Редкол. : Вадим ШАЛОМЄЄВ (відпов. ред.) Електрон. дані. Запоріжжя : НУ «Запорізька політехніка», 2023. С. 38-40 1 електрон. опт. диск (DVD-ROM); 12 см. – назва з тит. екрана.

8 Салогуб М. В. Електронний підручник з дисципліни: Надійність, діагностика та експлуатація комп'ютерних систем та мереж : підручник. ДКІТІ, 2016. 151 с.

9 What are the Advantages of Backup Server? - Backup Everything. Backup Everything. URL: <https://backupeverything.co.uk/what-are-the-advantages-of-backup-server/> (date of access: 01.11.2023).

10 Cisco Learning Network. Cisco Learning Network. URL: <https://learningnetwork.cisco.com/s/packet-tracer-alternative-lab-solutions> (date of access: 21.11.2023).

11 Visio. IT Connect. URL: <https://itconnect.uw.edu/tools-services-support/software-computers/productivity-platforms/microsoft-productivity-platform/visio/> (date of access: 21.11.2023).

12 What is Virtualization? | IBM. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: <https://www.ibm.com/topics/virtualization> (date of access: 21.11.2023).

13 Containerization Explained | IBM. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: <https://www.ibm.com/topics/containerization> (date of access: 21.11.2023).

14 Server Clustering and How It Works URL: <https://www.racksolutions.com/news/blog/server-cluster-how-it-works/> (дата звернення: 01.11.2023).

15 Server Automation Guide | phoenixNAP KB. Knowledge Base by phoenixNAP. URL: <https://phoenixnap.com/kb/server-automation> (date of access: 01.11.2023).

16 Network Monitoring Software by ManageEngine OpManager. ManageEngine OpManager. URL: <https://www.manageengine.com/network-monitoring/server-monitoring.html> (date of access: 21.11.2023).

17 Ідеальне джерело живлення стандарту ATX PS2 для серверів, робочих станцій й інших систем автоматизації - EServer. Мережеве обладнання. Купити серверне обладнання в Києві, Дніпрі - EServer. URL: <https://e->

server.com.ua/uk/poradi/idealne-dzherelo-zhivlennja-standartu-atx-ps2-dlja-serveriv-robochih-stancij-j-inshih-sistem-avtomatizacii (дата звернення: 01.11.2023).

18 Джерела безперебійного живлення для серверних стійок. ITbox - інтернет-магазин електроніки та комп'ютерної техніки. URL: https://www.itbox.ua/ua/category/Usi_DBZh-c3164/filter=101746-86000002700/ (дата звернення: 01.11.2023).

19 5 причин, чому для бізнесу система резервного живлення краща за генератор – AIN.UA. URL: <https://ain.ua/2023/03/24/5-prychyn-chomu-dlya-biznesu-systema-rezervnogo-zhyvlennya-krashha-za-generator/> (дата звернення: 01.11.2023).

20 Амайнд – Системи розподілу електроживлення. Amind – Головна сторінка (Amind). URL: <https://amind.ua/systemy-rozpodilu-electrozhyvlenня> (дата звернення: 01.11.2023).

21 Управління живленням і електроенергією рішення для будівель. Schneider Electric. URL: <https://www.se.com/ua/uk/work/solutions/power-management/> (дата звернення: 01.11.2023).

22 С.О Волкова О.М Труханов. Дослідження існуючих підходів підвищення якості програмного забезпечення критичного застосування. 2008. С. 7.

23 Martin L. Shooman. Reliability of computer systems and networks. John Wiley & Sons, Inc, 2002. 546 p.

24 Зенів І.О, Жураковський Б. Ю. Комп'ютерні мережі частина 1 навчальний посібник. КИЇВ : КПІ ім. Ігоря Сікорського, 2020. 328 с.

25 Тиш Є.В Литвиненко Я.В. Конспект лекцій з дисципліни „Надійність, контроль, діагностика та експлуатація ЕОМ” для студентів спеціальності 123 „Комп'ютерна інженерія”. Тернопіль, 2020. 150 с.

26 Як правильно облаштувати серверну кімнату. SVA - СПЕЦВУЗАВТОМАТИКА. URL: <https://sva.ua/yak-pravylyno-oblashtuvaty-servernu-kimnatu/> (дата звернення: 14.12.2023).

27 Купити мережеве обладнання від виробника недорого у Києві, Харкові, Одесі | Hypernet. URL: <https://shop.hypernet.com.ua/content/uploads/images/novosti-i-statyi/steny-v-servernoy.jpg>

28 Вимоги до серверної | Серверних приміщень, апаратним в Україні. Hypernet - магазин мережевого обладнання в Києві та Україні. URL: <https://shop.hypernet.com.ua/trebovaniya-k-servernoy-komnate/> (дата звернення: 04.11.2023).

29 Як зробити серверну для офісу?. Системний інтегратор України, інженерні системи та мережі: Кластер. URL: <https://klaster.ua/ua/stati-i-obzory/kak-sdelat-servernuyu-dlya-ofisa/> (дата звернення: 10.11.2023).