ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО – НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«Система забезпечення високої автономності та відмовостійкості обчислювальних систем»**

на здобуття освітнього ступеня магістр
за спеціальності 123 Комп'ютерна інженерія_____
(код ,найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ _____Роман БОБКОВ_____
(підпис) (ім'я, ПРІЗВИЩЕ здобувача)

Виконав: здобувач вищої освіти гр.КСДМ-61
_____Роман БОБКОВ_____
(ім'я, ПРІЗВИЩЕ)
Керівник: _____Наталія ЛАЩЕВСЬКА_____
к.т.н,доцент, (ім'я, ПРІЗВИЩЕ)

Рецензент:_____
(ім'я, ПРІЗВИЩЕ)

Київ – 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра Комп'ютерної інженерії
Ступінь вищої освіти «Магістр»
Напрям підготовки 123 «Комп'ютерна інженерія»
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерної інженерії
Наталія ЛАЩЕВСЬКА
(ім'я, ПРІЗВИЩЕ)
"____"_____20___ року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Бобкову Роману Анатолійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи: «Система забезпечення високої автономності та відмовостійкості обчислювальних систем»

Керівник роботи Лащевська Наталія Олександрівна – доцент кафедри комп'ютерної інженерії
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від _15.10.2024_року №__320__.

2. Строк подання студентом роботи 29.12.2024

3. Вхідні дані до роботи:
   3.1. Вимоги до кваліфікаційної роботи магістра з актуальних завдань.
   3.2 Нормативні матеріали (стандарти).
   3.3 Технічні вимоги.
   3.4 Науково-технічна література з питань, пов'язаних з темою роботи.

Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити):
4.1. Огляд існуючих рішень для забезпечення автономності та відмовостійкості;
4.2 Вплив зовнішніх факторів на обчислювальні системи;
4.3 Методи підвищення автономності комп'ютерних систем;
4.4. Засоби забезпечення відмовостійкості обчислювальних систем;
4.6. Практична реалізація методів забезпечення автономності

відмовостійкості.

5. Графічні матеріали.
   1. Презентація

6. Дата видачі завдання ____01.09.2024_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	10.10-12.10.2024	Виконано
2	Аналіз понять та характеристик відмовостійкої та автономної комп’ютерної системи	12.10-15.10.2024	Виконано
3	Огляд технологій та методів підвищення відмовостійкості та автономності комп'ютерних систем	15.10-18.10.2024	Виконано
4	Аналіз проблематики підвищення відмовостійкості та автономності комп’ютерних систем	18.10-22.10.2024	Виконано
5	Практична реалізація методів та засобів підвищення автономності та відмовостійкості у вигляді системи	22.10-26.10.2024	Виконано
7	Вступ, висновки, реферат	26.10-30.11.2024	Виконано
8	Попередній захист роботи	09.12-11.12.2024	Виконано
9	Подання роботи в деканат	20.12-29.12.2024	Виконано

Студент _____ _____Бобков Р.А_____
(підпис) (прізвище та ініціали)

Керівник роботи _____ ____Лащевська. Н.О_
(підпис) (прізвище та ініціали)

Реферат

Текстова частина дипломної роботи містить: 71 сторінку, 31 рисунок, 7 таблиць, 15 джерел.

Ключові слова: автономність, відмовостійкість, обчислювальні системи, хмарні технології, контейнеризація, кластеризація, резервування, кіберзахист, штучний інтелект, моніторинг.

Актуальність теми. В сучасних умовах інтенсивного розвитку інформаційних технологій надійність і безперебійність обчислювальних систем набуває особливої важливості для роботи підприємств та організацій. Забезпечення високої автономності та відмовостійкості є необхідною умовою для стабільного функціонування компаній, мінімізації ризиків збоїв та втрати даних, а також захисту від зовнішніх загроз. Розробка методів, які дозволяють досягати максимального рівня автономності та безвідмовної роботи систем, сприятиме покращенню ефективності бізнес-процесів та забезпеченню надійності обчислювальної інфраструктури. Наявні системи забезпечення високої автономності та відмовостійкості обчислювальних систем, які використовуються у роботі критичних підприємств або компаній, у більшості випадків розраховані на епізодичні, несистематичні відмови. Тому дана тема є актуальною і була обрана для створення більш оптимізованої системи підвищеної автономності та відмовостійкості в умовах сьогодення України.

Мета роботи: розробка системи забезпечення високої автономності та відмовостійкості обчислювальних систем.

Завдання:

- проаналізувати і впровадити методи підвищення автономності та відмовостійкості обчислювальних систем під впливом різних чинників;

- побудувати модель архітектури приватного підприємства з високим рівнем автономності та відмовостійкості обчислювальних систем;
- здійснити тестування запропонованих рішень для оцінки ефективності моделі архітектури з високим рівнем автономності та відмовостійкості обчислювальних систем.

ABSTRACT

The text part of the thesis contains: 71 pages, 31 figures, 7 tables, 15 sources.

Keywords: autonomy, fault tolerance, computer systems, cloud technologies, containerization, clustering, redundancy, cyber defense, artificial intelligence, monitoring.

Relevance of the topic. In today's conditions of intensive development of information technology, the reliability and uninterrupted operation of computer systems is of particular importance for the operation of enterprises and organizations. Ensuring high autonomy and fault tolerance is a prerequisite for the stable operation of companies, minimizing the risks of failures and data loss, and protecting against external threats. Developing methods that maximize the level of autonomy and fault tolerance of systems will help improve the efficiency of business processes and ensure the reliability of the computing infrastructure. Existing systems for ensuring high autonomy and fault tolerance of computing systems used in the operation of critical enterprises or companies are in most cases designed for episodic, non-systematic failures. Therefore, this topic is relevant and was chosen to create a more optimized system of increased autonomy and fault tolerance in the current conditions of Ukraine.

Purpose: to develop a system to ensure high autonomy and fault tolerance of computer systems.

Objectives:

- to analyze and implement methods for increasing the autonomy and fault tolerance of computer systems under the influence of various factors;
- to build a model of the architecture of a private enterprise with a high level of autonomy and fault tolerance of computer systems;
- to test the proposed solutions to evaluate the effectiveness of the architecture model with a high level of autonomy and fault tolerance of computer systems.

ЗМІСТ

РОЗДІЛ 1. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ АВТОНОМНОСТІ ТА ВІДМОВОСТІЙКОСТІ.....15

1.1. Поняття автономності та відмовостійкості в обчислювальних системах..15

1.2. Огляд сучасних технологій забезпечення автономності та відмовостійкості..... 17

1.2.1. Кластеризація обчислювальних систем..... 17

1.2.2. Віртуалізація..... 18

1.2.3. Резервування..... 19

1.2.4. Моніторинг і віддалене управління.....20

1.3. Аналіз переваг і недоліків існуючих рішень.....21

РОЗДІЛ 2. ВПЛИВ ЗОВНІШНІХ ФАКТОРІВ НА ОБЧИСЛЮВАЛЬНІ СИСТЕМИ.....……...24

2.1. Класифікація зовнішніх факторів..... 24

2.2. Фізичні фактори.....25

2.2.1. Коливання напруги.....25

2.2.2. Температура і вологість..... 27

2.3. Програмні фактори.....28

2.3.1. Програмні помилки.....28

2.3.2. Шкідливе програмне забезпечення..... 29

2.4. Мережеві фактори..... 29

2.4.1. Втрата пакетів і нестабільність мережі.....29

2.4.2. Мережеві атаки.....30

2.5. Людський фактор.....31

2.5.1. Некоректна експлуатація..... 31

2.5.2. Зловмисні дії..... 32
2.6. Аналіз впливу зовнішніх факторів на стабільність та продуктивність систем..... 32
2.6.1 Фізичні фактори..... 32
2.6.2. Програмні фактори.....33
2.6.3. Людський фактор.....34
2.6.4. Комплексний вплив.....34
2.6.5. Оцінка впливу.....34
2.6.6. Висновки з аналізу впливу зовнішніх факторів на систему.....35
РОЗДІЛ 3. МЕТОДИ ПІДВИЩЕННЯ АВТОНОМНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ..... 36
3.1. Методи оптимізації ресурсів..... 36
3.1.1 Динамічне балансування навантаження..... 36
3.1.2. Енергозбереження..... 38
3.1.3. Оптимізація зберігання даних.....38
3.2. Автоматизовані системи резервного копіювання та відновлення..... 39
3.2.1. Резервне копіювання в режимі реального часу..... 39
3.2.2. Системи, що самовідновлюються.....39
3.3. Використання штучного інтелекту для підвищення автономності..... 40
3.3.1. Автоматичне виявлення аномалій.....40
3.3.2. Оцінка стану системи.....40
3.3.3. Автоматична оптимізація процесів..... 41
3.4. Оцінка ефективності методів підвищення автономності..... 41
РОЗДІЛ 4. ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ.....42
4.1. Поняття відмовостійкості.....42

4.2. Резервування компонентів....42
4.2.1. Апаратне резервування....42
4.2.2. Програмне резервування.... 47
4.2.3. Гаряче, тепле та холодне резервування....48
4.3. Методи забезпечення безперервної роботи.... 55
4.3.1. Дублювання операцій.... 55
4.3.2. Автоматичне відновлення процесів....55
4.3.3. Реплікація даних....55
4.4. Тестування на відмовостійкість....56
4.4.1. Тестування сценаріїв відмови....56
4.4.2. Регулярні стрес-тести.... 57
4.5. Відповідність стандартам відмовостійкості.... 57
4.6. Висновки щодо забезпечення відмовостійкості....57
РОЗДІЛ 5. ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ АВТОНОМНОСТІ І ВІДМОВОСТІЙКОСТІ.... 58
5.1. Критичні температури та вологість....60
5.2. Шкідливе програмне забезпечення.... 64
5.3. Мережеві чинники.... 67
5.4. Резервування та відновлення після збоїв....70
5.5. Коливання напруги та відсутність електроживлення.... 72
5.6. Людські фактори.... 86
Висновки.... 87
Електронні ресурси.... 89
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 91

Вступ

З розвитком сучасних технологій обчислювальні системи стали невід’ємною частиною практично всіх аспектів людського життя. Всюди потрібні комп’ютерні системи з високою надійністю та продуктивністю, від промисловості, магазинів, медицини, фінансових установ і до національної безпеки. У зв'язку з цим забезпечення відмовостійкості та автономності роботи комп’ютерних систем стає дедалі більш актуальним завданням.

Сучасні обчислювальні системи не лише мають функціонувати надійно, але і повинні залишатися продуктивними та стабільними під час виникнення збоїв, викликані різними факторами. Серед таких факторів є: фізичні загрози (перепади напруги, екстремальні температури); програмні та мережеві атаки. Дані загрози можуть призводити до втрати даних, зниження продуктивності або повної відмови роботи системи. В сучасних умовах, де комп’ютерні системи широко використовуються, навіть короткочасні збої можуть спричинити значні фінансові збитки або навіть загрожувати життю людей, якщо йдеться про роботу медичних чи транспортних систем.

Таким чином, дослідження ефективних методів підвищення автономності та відмовостійкості обчислювальних систем є надзвичайно актуальним. Досягнення цієї мети дозволить розробити систему, яка здатна витримувати різні види загроз, адаптуватися до змінних умов та забезпечувати високу якість обслуговування, незалежно від зовнішніх обставин.

Метою цієї дипломної роботи є розробка та аналіз методів і засобів, які забезпечують високий рівень автономності та відмовостійкості обчислювальних систем в умовах сьогодення України під впливом різних зовнішніх факторів.

Для досягнення поставленої мети були визначені наступні основні завдання дослідження:

- провести аналіз існуючих методів та підходів забезпечення автономності та відмовостійкості обчислювальних систем, з метою виявлення їхніх переваг і недоліків;

- дослідити класифікацію та характерні особливості зовнішніх факторів, які можуть спричинити збої в обчислювальних системах;

- розробити методи та засоби для підвищення автономності обчислювальних систем, включаючи оптимізацію ресурсів та впровадження самооновлювальних алгоритмів;

- запропонувати практичні засоби для забезпечення відмовостійкості систем, які враховують різні рівні захисту, зокрема, методи реплікації даних та резервування;

- провести експериментальний аналіз розроблених методів і засобів, оцінити їх ефективність та зробити висновки щодо якості їх придатності в різних сценаріях.

Об'єктом дослідження є процес забезпечення автономності та відмовостійкості обчислювальних систем у середовищах із зовнішніми впливами. Такі системи можуть бути представлені як серверні обчислювальні комплекси, так і розподілені мережеві інфраструктури.

Предметом дослідження є методи та засоби, які забезпечують автономність та відмовостійкість обчислювальних систем шляхом впровадження інноваційних технологій, адаптивних алгоритмів, інструментів моніторингу та резервування.

Дослідження зосереджено на розробці рішень, які сприяють зниженню впливу зовнішніх факторів на працездатність систем та підвищують їхню здатність з адаптації до умов навколишнього середовища.

Для досягнення поставлених цілей та вирішення визначених завдань у цій роботі використовувалися такі методи дослідження:

- Теоретичний аналіз: вивчення наукової літератури та існуючих досліджень у сфері автономності та відмовостійкості обчислювальних систем, аналіз існуючих

підходів та технологій;

- Моделювання: створення моделей, що дозволяють відтворити вплив зовнішніх факторів на обчислювальні системи та оцінити ефективність різних методів захисту;

- Експериментальне тестування: практична перевірка розроблених методів і засобів, що забезпечують автономність і відмовостійкість, на тестовому середовищі, з метою визначення ефективності та надійності;

- Порівняльний аналіз: проведення аналізу ефективності запропонованих рішень у порівнянні з традиційними методами для оцінки їхньої результативності у різних сценаріях.

РОЗДІЛ 1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ АВТОНОМНОСТІ ТА ВІДМОВОСТІЙКОСТІ

1.1. Поняття автономності та відмовостійкості в обчислювальних системах

Автономність обчислювальних систем визначається як здатність системи функціонувати без втручання людини протягом тривалого часу, приймати самостійні рішення на основі доступних даних і адаптуватися до змін середовища. Прикладом таких систем є автоматичні системи управління виробничими процесами або автономні транспортні засоби. Важливим аспектом автономності є адаптація до змін та виправлення помилок у разі їх виникнення.

Відмовостійкість характеризується здатністю системи виявляти помилки, локалізувати їх і забезпечувати безперервну роботу навіть за умов збоїв окремих компонентів. Прикладом відмовостійких систем є RAID-масиви для зберігання даних або кластерні обчислення, де вихід з ладу одного вузла не впливає на функціонування системи в цілому.

Відмова - це подія в роботі комп’ютерних систем, коли техніка втрачає здатність до виконання її основної функції внаслідок різних несправностей.

Автономність обчислювальної системи передбачає декілька ключових аспектів:

- **Адаптація**: Система повинна мати здатність адаптуватися до різних умов. Це може бути адаптація, наприклад, до збільшення або зменшення навантаження, обмеження доступних ресурсів або зміну конфігурації обладнання;

- **Виявлення та виправлення помилок**: Автономна система має бути здатною автоматично виявляти збої та помилки, а також самостійно приймати рішення щодо їх виправлення. Це може включати механізми самооновлення програмного

забезпечення, перезапуск сервісів;

- Прогнозування та попереджувальне обслуговування: Завдяки аналізу даних, отриманих у процесі роботи, обчислювальна система може прогнозувати потенційні проблеми та вживати заходів для їх запобігання. Наприклад, система може виявити, що певний компонент наближається до кінця свого життєвого циклу і заздалегідь замінити його або перемістити робоче навантаження на інші компоненти;

Відмовостійкість - це здатність системи продовжувати свою роботу або швидко відновлюватися після збою. Система з високою відмовостійкістю має бути здатною виявляти помилки, ізолювати проблемні ділянки, а також забезпечувати резервне копіювання важливих компонентів.

Відмовостійкість залежить від таких характеристик системи:

- Резервування компонентів: Система повинна мати резервні компоненти, які можуть замінити основні у випадку їх відмови. Це включає як апаратні засоби (наприклад, резервні жорсткі диски або процесори), так і програмні рішення (резервні копії даних, реплікація сервісів);

- Дублювання та реплікація: У відмовостійких системах часто застосовуються механізми дублювання або реплікації даних та процесів, що дозволяє зберігати критичну інформацію в кількох копіях. Це забезпечує можливість швидкого відновлення після збою або атаки;

- Швидке відновлення: Система з високою відмовостійкістю повинна мати можливість швидко відновлювати роботу після збоїв. Це може включати відновлення з резервних копій, перезапуск зупинених процесів або перемикання на резервні компоненти. Час відновлення є важливим параметром, оскільки від нього залежить, як довго система залишатиметься недоступною після збою;

- Терпимість до збоїв: Це характеристика, яка дозволяє системі продовжувати

функціонування з обмеженою продуктивністю навіть у випадку виходу з ладу деяких компонентів. Наприклад, якщо один із серверів у кластері виходить з ладу, інші сервери можуть продовжувати обробку запитів, хоча загальна продуктивність системи може знизитися.

Таблиця 1.1 - Порівняння автономності та відмовостійкості

Характеристика	Автономність	Відмовостійкість
Основна мета	Мінімізувати втручання людини	Забезпечити безперервну роботу
Реалізація	Автоматизація процесів, ШІ	Резервування, реплікація
Приклади	Розумні системи моніторингу	RAID, кластери

Ці характеристики є критичними для обчислювальних систем, що працюють у реальному часі, особливо в умовах важливих завдань, таких як управління технологічними процесами або забезпечення безперервності фінансових операцій.

1.2. Огляд сучасних технологій забезпечення автономності та відмовостійкості

1.2.1. Кластеризація обчислювальних систем

Кластеризація передбачає об’єднання декількох обчислювальних пристроїв або серверів у єдину систему для підвищення продуктивності та відмовостійкості. У разі відмови одного з компонентів системи, його функції автоматично

передаються на інші вузли кластеру, що мінімізує втрати даних і збої. Різноманітні технології кластеризації, такі як Hadoop або Kubernetes, активно використовуються для розподілених обчислень і управління контейнеризованими додатками.

1.2.2. Віртуалізація

Віртуалізація забезпечує можливість створення декількох віртуальних машин на одному фізичному сервері. Це дозволяє розподіляти ресурси між віртуальними машинами так, щоб можна було забезпечити резервування системи під час різних факторів. У разі збою однієї з віртуальної машини, її функції можуть бути швидко перенесені на іншу, не перериваючи процесу роботи. Віртуалізація також дає змогу динамічно керувати ресурсами системи, покращуючи її автономність [13].

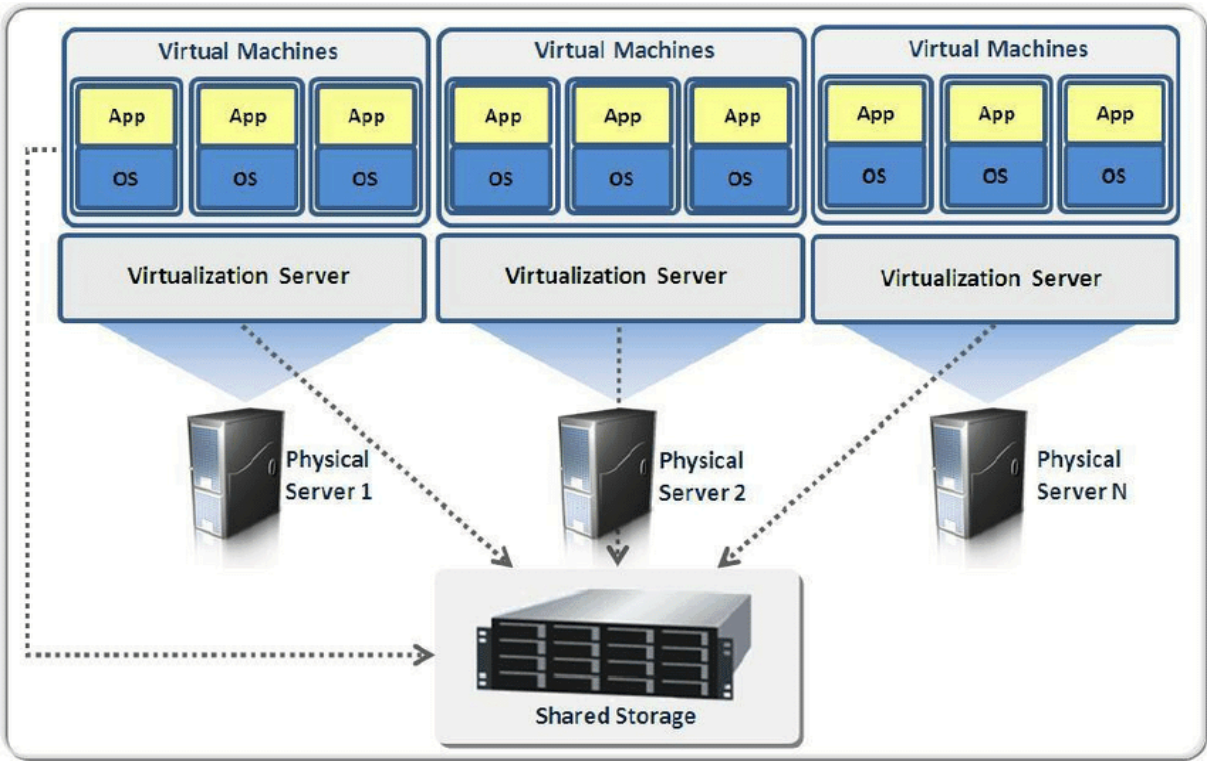


Рисунок 1.1 - Приклад схеми віртуалізації

1.2.3. Резервування

Резервування - це основний метод забезпечення відмовостійкості систем. Суть підходу полягає в тому, що критичні компоненти комп'ютерної системи мають свої копії або резервні варіанти, які можуть бути активновані чи замінені у разі збою основного обладнання. Це може бути реалізовано на рівні апаратних засобів, програмного забезпечення або навіть на рівні мережі [14].

Для зберігання даних активно використовуються RAID-масиви. Наприклад, RAID 1 забезпечує дзеркальне копіювання даних, що гарантує їх збереження навіть у разі виходу з ладу одного з дисків.

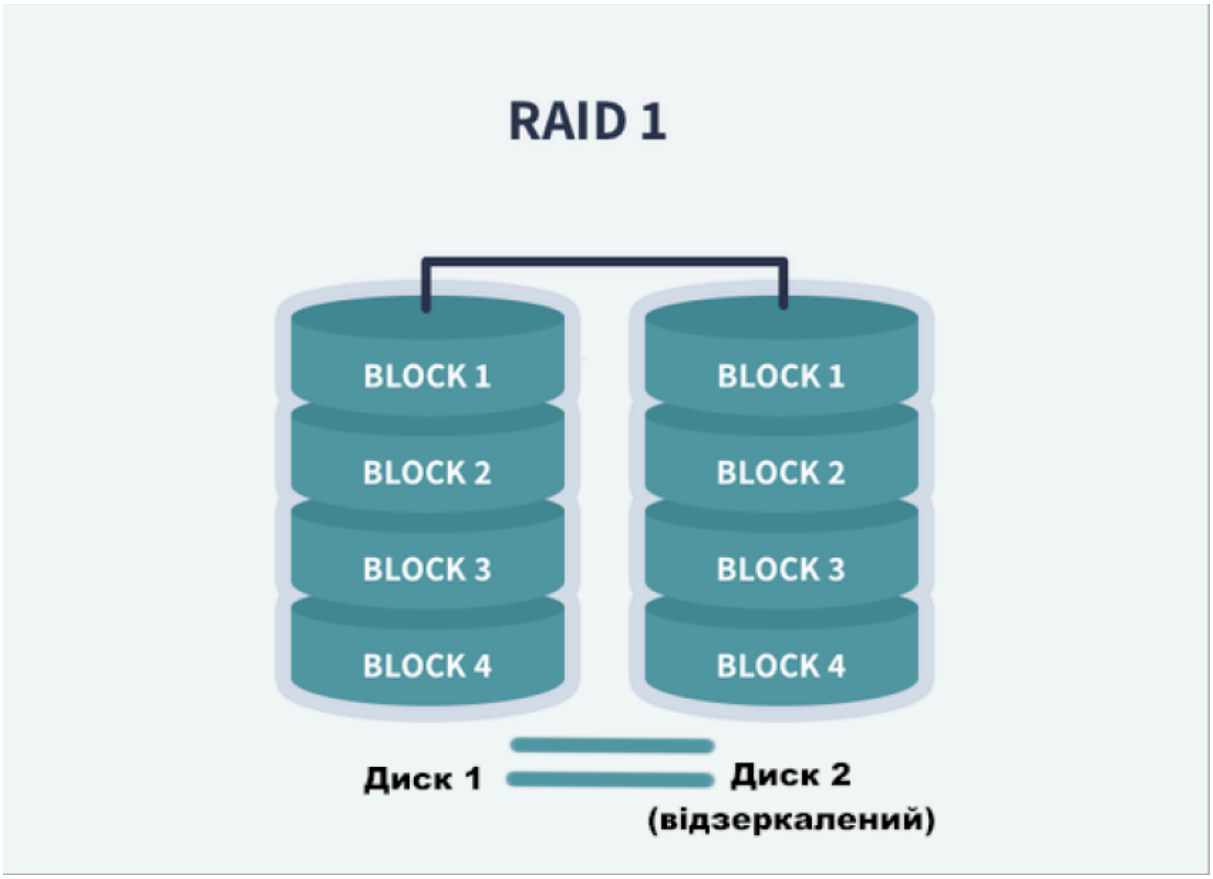


Рисунок 1.2 - Резервування компонентів на прикладі роботи RAID 1

1.2.4. Моніторинг і віддалене управління

Для забезпечення автономності системи необхідний постійний моніторинг її стану. Сучасні системи моніторингу, такі як, наприклад, Nagios або Zabbix, дозволяють контролювати роботу всіх компонентів, виявляти збої на ранніх етапах і запускати механізми самовідновлення системи [6].

Віддалене управління та автоматичне оновлення компонентів забезпечують автономність навіть у разі обмеженого доступу до фізичної інфраструктури.

Рисунок 1.3 - Моніторинг системи Nagios

Суть моніторингу полягає у безперервному спостереженні за станом апаратного і програмного забезпечення, мережі та інших компонентів системи.

Він дозволяє:

- відслідковувати продуктивність систем у реальному часі;
- аналізувати історичні дані для виявлення тенденцій або вузьких місць;

- генерувати автоматичні сповіщення про критичні ситуації.

Основними параметрами, які контролюються під час моніторингу, є:

- завантаження процесора, оперативної пам’яті та дискових ресурсів;
- пропускна здатність та затримки в мережі;
- статус серверів, баз даних і додатків.

Сучасні системи моніторингу надають широкий функціонал для збору, обробки та візуалізації даних.

Найпоширеніші з них:

- Zabbix. Відкрите рішення для моніторингу інфраструктури, що дозволяє стежити за станом серверів, мережевих пристроїв і додатків;
- Nagios. Інструмент для моніторингу мереж та серверів, який забезпечує гнучку систему оповіщень;
- Prometheus. Використовується для моніторингу контейнеризованих додатків і хмарних систем;
- Grafana. Система для візуалізації даних, яка часто інтегрується з іншими інструментами моніторингу.

Віддалене управління дозволяє адміністраторам отримувати доступ до систем із будь-якої точки світу. Це забезпечує оперативне усунення несправностей, оновлення програмного забезпечення та виконання інших задач без необхідності фізичної присутності.

1.3. Аналіз переваг і недоліків існуючих рішень

Сучасні технології забезпечення автономності та відмовостійкості обчислювальних систем пропонують широкий спектр рішень, кожне з яких має свої переваги та обмеження. Розуміння цих аспектів дозволяє обрати найбільш

відповідний та якісний підхід до впровадження в конкретній інфраструктурі.

Переваги існуючих рішень.

Кластеризація є одним із ключових підходів до створення відмовостійких систем. Завдяки об’єднанню кількох вузлів у єдину систему кластеризація забезпечує гнучкість та масштабованість. Вона дозволяє уникнути єдиного пункту відмови, оскільки вихід з ладу одного вузла не впливає на загальну працездатність системи. Це особливо важливо для великих організацій, де доступність сервісів є критичною.

Віртуалізація оптимізує використання фізичних ресурсів, дозволяючи на одному сервері запускати кілька віртуальних машин. Це не лише підвищує ефективність використання обладнання, а й забезпечує можливість швидкого переміщення навантаження між вузлами у разі збою, мінімізуючи час простою.

Резервування гарантує наявність запасних ресурсів, які можуть бути активовані у разі виходу з ладу основних. Це забезпечує безперервність роботи критично важливих процесів, таких як обробка транзакцій чи управління базами даних. Резервування є невід’ємною частиною відмовостійких систем у сферах, де ризик простою є неприйнятним.

Моніторинг дозволяє постійно контролювати стан системи, своєчасно виявляти аномалії та вживати заходів до виникнення серйозних проблем. Завдяки використанню сучасних інструментів моніторинг забезпечує автоматизацію процесу виявлення збоїв і генерує сповіщення для адміністратора у режимі реального часу.

Недоліки існуючих рішень.

Хоча кластеризація є потужним інструментом для забезпечення відмовостійкості, вона потребує значних фінансових витрат на впровадження та підтримку. Крім того, налаштування кластерів є складним завданням, яке вимагає високої кваліфікації спеціалістів. Без належного управління можливі збої у синхронізації вузлів або неефективне розподілення ресурсів.

Віртуалізація може створювати додаткове навантаження на фізичні сервери, оскільки кілька віртуальних машин конкурують за доступ до ресурсів. Це може призводити до зниження загальної продуктивності, особливо у випадках неправильної конфігурації або недостатнього обсягу фізичних ресурсів.

Резервування, хоча і підвищує надійність системи, потребує значних ресурсів для підтримки надлишкових компонентів. Це може бути економічно невиправдано для невеликих компаній чи систем із обмеженими обчислювальними потребами. Крім того, для збереження актуальності резервних копій потрібне регулярне тестування, що збільшує витрати на адміністрування.

Моніторинг, попри свої переваги, вимагає правильної конфігурації та інтеграції з іншими системами. Якщо цей процес виконано некоректно, моніторинг може виявитися неефективним. До того ж, надмірна залежність від ручного налаштування й аналізу даних може уповільнювати реакцію на критичні ситуації.

Висновок.

Кожне з описаних рішень має як переваги, так і обмеження, що впливають на ефективність їх використання в реальних умовах. Для досягнення високого рівня автономності та відмовостійкості доцільно застосовувати комплексний підхід, який поєднує декілька методів. Наприклад, використання кластеризації у поєднанні з резервуванням і моніторингом дозволяє створити надійну систему, здатну ефективно функціонувати, навіть у випадку несподіваних збоїв. Таким чином, гнучка інтеграція існуючих рішень, з урахуванням специфіки завдань організації, в комплексну модель комп’ютерної системи з високим рівнем автономності та відмовостійкості - є найкращим шляхом до забезпечення стабільної та безпечної роботи обчислювальних систем.

РОЗДІЛ 2 ВПЛИВ ЗОВНІШНІХ ФАКТОРІВ НА ОБЧИСЛЮВАЛЬНІ СИСТЕМИ

2.1. Класифікація зовнішніх факторів

Зовнішні фактори - це будь-які умови або події, що можуть впливати на функціонування обчислювальних систем, зокрема на їхню продуктивність, відмовостійкість і автономність. Вони можуть бути природного, техногенного або людського походження. Коротко розглянемо основні види зовнішніх факторів, які можуть впливати на роботу систем у вигляді таблиці:

Таблиця 2.1 - Вплив коливань напруги на стабільність системи

Категорія	Типи факторів	Приклади	Потенційний вплив
Фізичні	Коливання напруги, температура	Перепади електрики, перегрів процесорів	Втрата даних, пошкодження апаратного обладнання
Програмні	Збої, помилки в коді	Переповнення буфера, шкідливе ПЗ	Програмні збої, витік даних
Мережеві	Затримка передачі, мережеві атаки	DDoS, втрати пакетів	Недоступність мережі, втрата даних
Людський фактор	Некоректна експлуатація, помилки	Видалення файлів, неправильне налаштування	Втрати даних, збої в системі

Зовнішні фактори, що можуть впливати на стабільність і продуктивність обчислювальних систем, поділяються на декілька категорій:

- Фізичні фактори: фактори, що пов'язані з апаратним середовищем системи, такі як коливання напруги, температурні зміни, вологість, пил та інші умови навколишнього середовища;

- Програмні фактори: включають у себе збої у програмному забезпеченні, помилки в коді, неочікувані конфлікти між різними програмами та компоненти шкідливого програмного забезпечення;

- Мережеві фактори: пов'язані з доступом до мережі, включаючи втрати пакетів, нестабільність мережі, атаки на мережу, відмову маршрутизаторів і мережевих комутаторів;

- Людський фактор: вплив людської помилки, некоректної експлуатації системи або зловмисних дій.

2.2. Фізичні фактори

Обчислювальні системи часто піддаються дії зовнішніх умов, таких як коливання температури і вологості, які можуть призвести до перегріву компонентів або корозії контактів на електронних платах. Зокрема, сервери та інші критично важливі системи, повинні бути розміщені в спеціально обладнаних серверних приміщеннях з контролем температури та вологості, щоб уникнути фізичних пошкоджень.

2.2.1. Коливання напруги

Коливання напруги є поширеною проблемою, що призводить до збоїв в

роботі обчислювальних систем, особливо в регіонах із нестабільним електропостачанням. Стрибки напруги можуть пошкодити компоненти системи, такі як блок живлення, жорсткі диски, оперативну пам’ять тощо.

Наприклад: у дата-центрі великої компанії зафіксували стрибок напруги, який призвів до пошкодження кількох серверів. В результаті роботи з відновлення даних та заміни обладнання компанія втратила кілька годин часу, що призвело до значних фінансових втрат.

Для запобігання подібним випадкам, зазвичай, встановлюють джерела безперебійного живлення (ДБЖ) з функцією стабілізації напруги [15].

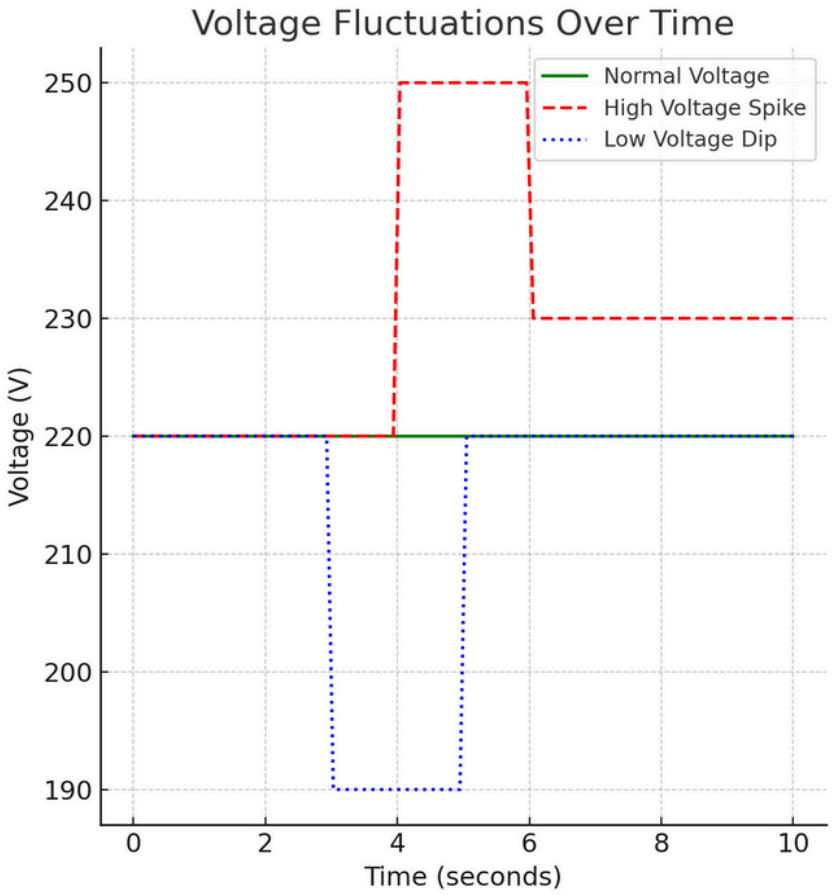


Рисунок 2.1 - Коливання напруги протягом часу

2.2.2. Температура і вологість

Критичні температури, особливо перегрів процесорів та оперативної пам’яті, відеочіпів та інших ключових компонентів, можуть спричинити раптову відмову системи або навіть фізичне пошкодження обладнання.

Далі наведено таблицю та графік залежності тривалості роботи від температур:

Таблиця 2.2 - Вплив температури на стабільність серверів

Температура (°C)	Тривалість роботи без збоїв (години)	Ймовірність збою (%)
20	48	0
40	24	5
60	12	15
80	4	50

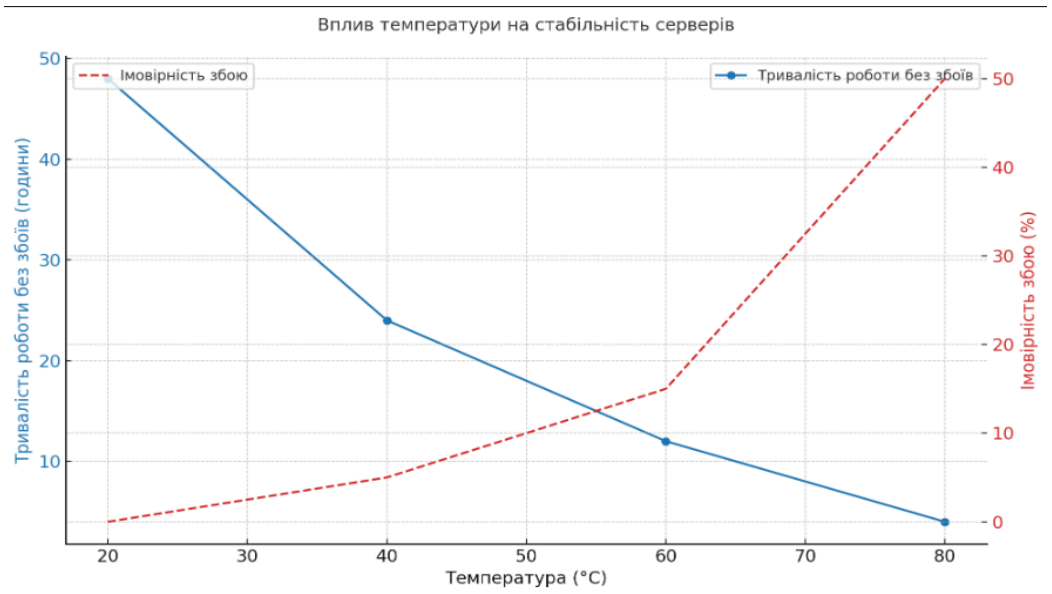


Рисунок 2.2 - Залежність роботи серверів від їх температури

По таблиці та графіку можна зрозуміти, що крива яка відображає ймовірність збою дуже різко зростає при навіть помірному зростанні температури, що відрізняється від рекомендованих для роботи техніки.

Вологість також впливає на працездатність системи: занадто висока вологість може призвести до корозії компонентів, тоді як низька - до утворення статичної електрики, що може пошкодити чутливу електроніку.

Рисунок 2.3 - Корозія компонентів

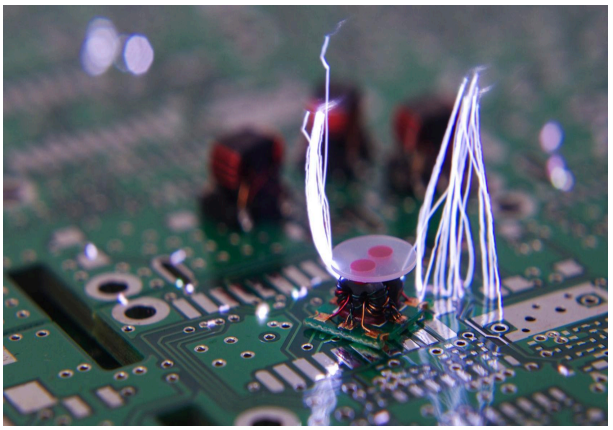


Рисунок 2.4 - Статична електрика

2.3. Програмні фактори

Програмне забезпечення є критично важливою частиною будь-якої обчислювальної системи, тому збої або помилки в програмному коді можуть спричинити серйозні збої в роботі системи.

Програмні помилки можуть виникати через різні причини: помилки в алгоритмах, несумісність версій програмного забезпечення або конфлікти між різними програмами.

2.3.1. Програмні помилки

Програмні помилки, такі як буферний переповнення, непередбачені цикли або помилки логіки, можуть спричинити збої в роботі програм або призвести до

некоректної роботи системи.

Відмовостійкі системи повинні включати механізми для автоматичного виявлення та виправлення помилок у реальному часі, такі як перевірка станів або контроль за цілісністю даних.

2.3.2. Шкідливе програмне забезпечення

Віруси, трояни, шкідливі скрипти можуть призвести до втрати даних, уповільнення роботи системи або навіть повного її збоїв. Щоб мінімізувати ризики, важливо застосовувати антивірусне ПЗ, системи виявлення загроз і постійне оновлення безпеки.

2.4. Мережеві фактори

Обчислювальні системи часто інтегровані у глобальні або локальні мережі, де мережеві збої можуть мати серйозні наслідки для доступності даних і безперервності процесів.

Мережеві фактори є одним з ключових аспектів, що впливають на стабільність та продуктивність обчислювальних систем. З розвитком технологій зростає ризик порушення їхньої роботи через збої, нестабільність або атаки. Вони можуть бути викликані як технічними проблемами, так і зовнішніми діями, такими як кібератаки.

2.4.1. Втрата пакетів і нестабільність мережі

Одним із найпоширеніших мережевих факторів є втрата пакетів. Втрата пакетів може виникати через перевантаження мережевих пристроїв, фізичні

пошкодження кабелів, застаріле обладнання або некоректну конфігурацію мережевих пристроїв.

Втрата мережевих пакетів або затримки передачі даних призводять до збоїв в обчислювальних процесах або до порушення роботи систем, що працюють у реальному часі. Такі проблеми часто виникають через низьку якість з'єднання або перевантаження мережі.

Для запобігання цьому використовують:

- використання протоколів, таких як TCP, з вбудованими механізмами повторної передачі пакетів;
- застосування технології Quality of Service (QoS) для управління пріоритетами мережевого трафіку;
- впровадження дублювання трафіку (Traffic Duplication) у критичних системах.

2.4.2. Мережеві атаки

Мережеві атаки становлять серйозну загрозу для обчислювальних систем та можуть паралізувати роботу всього підприємства.

Найпоширеніші типи атак:

- DDoS-атаки (Distributed Denial of Service): Мета таких атак - вичерпати ресурси системи, зробивши її недоступною для користувачів;
- Man-in-the-Middle (MITM): Цей тип атак передбачає перехоплення трафіку між двома сторонами. Для запобігання MITM-атакам активно використовуються методи шифрування, такі як TLS;
- Phishing та DNS-спуфінг: Направлені на перенаправлення трафіку на підробні сайти для збору конфіденційних даних.

Сучасні підходи до захисту від таких атак:

- Фільтрація трафіку за допомогою фаєрволів. Сучасні рішення, такі як Fortigate або Cisco ASA, забезпечують як базову фільтрацію, так і виявлення аномалій на рівні мережевого трафіку;
- Інтеграція систем IDS/IPS (Intrusion Detection and Prevention Systems). Такі системи, як Snort або Suricata, дозволяють виявляти підозрілу активність у мережі та блокувати її;
- Сегментація мережі. Розділення мережі на ізольовані зони (VLAN) обмежує розповсюдження атак у межах однієї мережі;
- Шифрування трафіку. Використання протоколів HTTPS та VPN забезпечує захист даних під час передачі.

2.5. Людський фактор

Людські помилки також є важливим чинником, який може призвести до збоїв у роботі обчислювальних систем. Найчастіше це стосується некоректного налаштування систем, неправильного управління даними або несвоєчасного оновлення програмного забезпечення.

2.5.1. Некоректна експлуатація

Неправильне використання систем або недотримання протоколів безпеки може призвести до серйозних проблем, таких як видалення важливих даних, налаштування, що не відповідають вимогам безпеки, або неповний моніторинг системи. Навчання персоналу є важливим елементом для зниження ризиків від людського фактора.

2.5.2. Зловмисні дії

Інсайдерські загрози, такі як зловмисні дії співробітників, також можуть суттєво вплинути на безпеку та стабільність систем. Це можуть бути навмисні атаки на систему або несанкціонований доступ до даних. Для запобігання цьому застосовуються системи контролю доступу та аудиту.

2.6. Аналіз впливу зовнішніх факторів на стабільність та продуктивність систем

Зовнішні фактори можуть мати значний вплив на стабільність та продуктивність обчислювальних систем, що проявляється у вигляді збоїв, втрати даних чи навіть повного виходу системи з ладу. Їхній вплив залежить від природи факторів, таких як фізичні умови, програмні помилки, мережеві збої чи людський фактор.

2.6.1 Фізичні фактори.

Стабільність обчислювальних систем багато в чому залежить від фізичних умов, в яких вони працюють. Коливання температури чи вологості, а також перепади напруги можуть пошкодити апаратні компоненти. Наприклад, перегрів процесора через недостатню вентиляцію призводить до втрати його продуктивності, а перепади напруги — до збоїв в роботі жорстких дисків чи серверів. Для забезпечення захисту від таких загроз використовуються джерела безперебійного живлення, системи стабілізації напруги та охолодження серверних приміщень. Такі рішення дозволяють значно знизити ризики простоїв через

несприятливі умови.

2.6.2. Програмні фактори.

Програмні помилки або конфлікти між різними компонентами системи часто стають причиною нестабільності. Це може бути результатом як помилок у коді, так і використання несумісного програмного забезпечення. Наприклад, несвоєчасне оновлення базових компонентів операційної системи може зробити її вразливою до шкідливих програм. Відповідно, для уникнення таких проблем важливо регулярно оновлювати програмне забезпечення, а також тестувати нові функції перед їх впровадженням у виробниче середовище. Крім того, використання методів автоматичного відновлення дозволяє мінімізувати вплив таких факторів на продуктивність.

2.6.3. Мережеві фактори.

Нестабільність у роботі мережі часто впливає на системи, які залежать від постійного обміну даними. Наприклад, втрата пакетів через перевантаження мережі може призводити до уповільнення роботи або навіть до припинення обслуговування клієнтів. Подібні проблеми виникають і під час кібератак, таких як DDoS, коли система не здатна обробити великий обсяг шкідливого трафіку.

Для вирішення цих проблем застосовуються методи сегментації мережі, дублювання каналів передачі даних, а також системи виявлення та запобігання вторгнень, які дозволяють оперативно реагувати на загрози.

2.6.3. Людський фактор

Людський фактор є однією з найчастіших причин нестабільності обчислювальних систем. Помилки в налаштуванні, випадкове видалення даних чи некоректне управління ресурсами можуть суттєво впливати на роботу систем. Наприклад, відсутність регулярного резервного копіювання через недбалість адміністратора може призвести до втрати важливих даних у разі збою. Для мінімізації впливу людського фактору важливо впроваджувати автоматизацію повторюваних задач, використовувати системи моніторингу дій персоналу та проводити регулярні навчання щодо роботи з сучасними технологіями.

2.6.4. Комплексний вплив

Фізичні, програмні, мережеві та людські фактори часто взаємодіють, посилюючи один одного. Наприклад, фізичне пошкодження сервера через перепад напруги може спричинити програмні збої, а неправильне відновлення резервних копій адміністратором лише погіршить ситуацію. У таких випадках ключовим завданням є запровадження комплексних заходів, які включають захист як на фізичному рівні, так і на рівні програмного забезпечення.

2.6.5. Оцінка впливу

Оцінка стабільності та продуктивності систем здійснюється через вимірювання часу відновлення після збоїв, рівня доступності системи та її продуктивності під навантаженням. Наприклад, час відновлення (RTO) показує, наскільки швидко система повертається до нормальної роботи після збоїв, тоді як рівень доступності (Uptime) вказує на стабільність роботи системи протягом тривалого часу.

2.6.6. Висновки з аналізу впливу зовнішніх факторів на систему

Аналіз впливу зовнішніх факторів дозволяє виявити найвразливіші місця обчислювальних систем та розробити ефективні стратегії їх захисту. Завдяки поєднанню превентивних заходів, таких як впровадження резервування та моніторингу, з регулярними оцінками стабільності можна досягти значного підвищення надійності та продуктивності сучасних обчислювальних систем.

Усі зовнішні фактори, перелічені вище, можуть впливати на стабільність і продуктивність обчислювальних систем. Для кожного з цих факторів необхідно впроваджувати відповідні механізми захисту або компенсації. Наприклад, фізичні фактори можна мінімізувати за допомогою належної інфраструктури та обладнання, програмні помилки - через регулярні оновлення та виправлення, мережеві збої - через дублювання каналів і захист трафіку, а людські помилки - через навчання персоналу та жорсткий контроль доступу.

РОЗДІЛ 3 МЕТОДИ ПІДВИЩЕННЯ АВТОНОМНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ

3.1. Методи оптимізації ресурсів

Важливим фактором забезпечення автономності комп'ютерної системи є ефективне використання наявних ресурсів (наприклад, обчислювальної потужності, пам'яті, енергоспоживання тощо). Оптимізація ресурсів мінімізує залежність системи від зовнішніх втручань і підвищує її автономність.

3.1.1 Динамічне балансування навантаження

Одним з основних методів оптимізації ресурсів є динамічне балансування навантаження між компонентами системи. Системи повинні мати можливість перерозподіляти обчислювальні завдання між різними процесорами або серверами залежно від робочого навантаження.

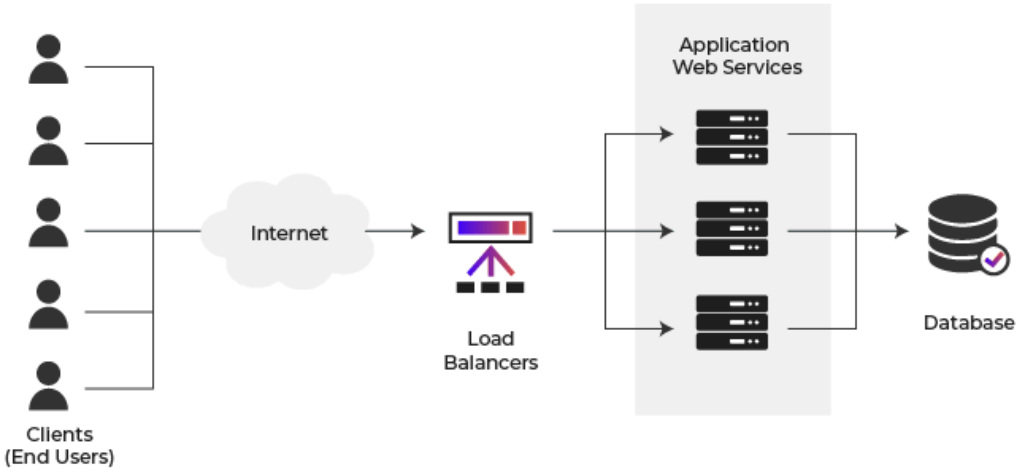


Рисунок 3.1 - Приклад роботи балансувальника навантаження

У випадку кластерних систем або хмарних обчислень це можна зробити автоматично за допомогою інструментів балансування навантаження.

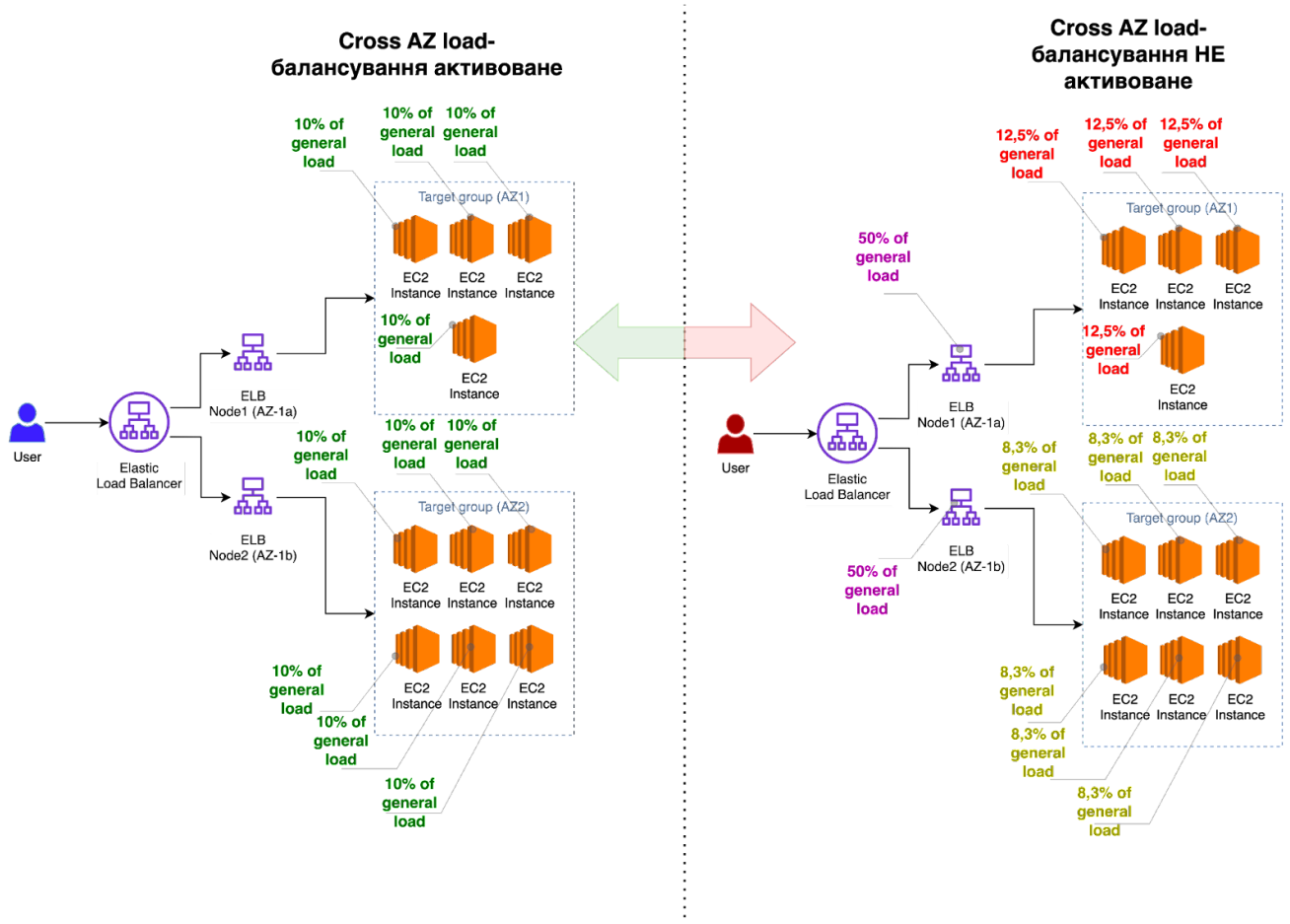


Рис 3.2 - Приклад роботи AWS Elastic LoadBalancer.

Балансувальники навантаження можна використовувати для рівномірного розподілу потоків запитів між серверами. Такі рішення використовуються багатьма інтернет-сервісами, зокрема такими платформами, як Amazon Web Services (AWS) та Google Cloud Platform.

3.1.2. Енергозбереження

Для продовження терміну служби батареї важливо досягти ефективного енергозбереження, особливо в мобільних і віддалених системах. Цього можна досягти шляхом оптимізації програмного забезпечення та обчислювальних процесів:

- переведення компонентів системи в режим низького енергоспоживання під час простою;
- використання енергоефективних алгоритмів для обробки даних;
- процесор динамічно підлаштовує тактову частоту відповідно до навантаження.

Такий підхід не тільки економить енергію, але й подовжує час автономної роботи системи за відсутності електрики.

3.1.3. Оптимізація зберігання даних

Оптимізація зберігання та обробки даних - ще один важливий аспект збільшення часу автономної роботи. Відповідні методи включають:

- стиснення даних для зменшення розміру збережених файлів;
- кешування для прискорення доступу до часто використовуваних даних;
- автоматичне архівування старих даних для звільнення системних ресурсів.

Це допомагає мінімізувати витрати на обробку та зберігання даних і є особливо важливим у великих інформаційних системах з постійно зростаючими обсягами інформації.

3.2. Автоматизовані системи резервного копіювання та відновлення

Автономність системи також залежить від її здатності швидко відновлюватися після збоїв, і тут важливу роль відіграють автоматичні системи резервного копіювання та відновлення. Такі системи мінімізують втрату даних і забезпечують швидке повернення до нормальної роботи.

3.2.1. Резервне копіювання в режимі реального часу

Важливим способом забезпечення автономності є резервне копіювання в режимі реального часу. Це процес постійного зберігання даних на окремому сервері або хмарному сховищі для мінімізації ризику втрати критично важливої інформації. У разі збою або надзвичайної ситуації система може автоматично відновити втрачені дані з резервної копії, що значно зменшує залежність від людського втручання.

Такі рішення, як RAID-масиви та системи зберігання даних на віддалених серверах, мінімізують час простою резервних копій, а також комп’ютерних систем.

3.2.2. Системи, що самовідновлюються

Сучасні комп'ютерні системи можуть містити механізми самовідновлення. Це програми або скрипти, які автоматично виявляють збій, аналізують його причину та ініціюють процес відновлення. Наприклад, якщо один з компонентів системи виходить з ладу, система може перезапустити цей компонент або перенести робочий процес на інший компонент.

Інструменти самовідновлення включають моніторинг та аналіз системних журналів, автоматичне відновлення програмного забезпечення та перенесення на резервний сервер або віртуальну машину в разі виходу з ладу основного сервера.

3.3. Використання штучного інтелекту для підвищення автономності

Сучасні обчислювальні системи все частіше інтегрують штучний інтелект (ШІ) для забезпечення автономності та адаптивності в складних середовищах. Штучний інтелект дозволяє системі вчитися на власному досвіді та самостійно приймати рішення в умовах непередбачених змін.

3.3.1. Автоматичне виявлення аномалій

Одним з найефективніших способів використання штучного інтелекту є автоматичне виявлення аномалій. Системи, що використовують методи машинного навчання, можуть виявляти відхилення в роботі, які можуть свідчити про несправність або зовнішню атаку, і ініціювати відповідні заходи для вирішення проблеми. Наприклад, у фінансових системах ШІ може виявляти підозрілі транзакції та автоматично блокувати їх до з'ясування ситуації.

3.3.2. Оцінка стану системи

Ще однією сферою застосування штучного інтелекту є прогнозування стану системи на основі зібраних даних. Аналізуючи історичні дані, можна передбачити

можливі апаратні збої та помилки програмного забезпечення і заздалегідь вжити контрзаходів. Такі системи прогнозування можуть запобігти надзвичайним ситуаціям і забезпечити автономну роботу без постійного втручання людини.

3.3.3. Автоматична оптимізація процесів

Штучний інтелект також можна використовувати для автоматичної оптимізації обчислювальних процесів, адаптуючи системні ресурси до поточних потреб. Це дозволяє автоматично змінювати конфігурацію системи у відповідь на зміни навантаження і своєчасно вивільняти або розгортати додаткові ресурси для більш ефективної роботи.

3.4. Оцінка ефективності методів підвищення автономності

Ефективність кожного методу підвищення автономності можна оцінити за допомогою наступних показників:

- Час простою системи - тривалість часу, протягом якого система недоступна для користувачів або не може виконувати свої функції. Система з мінімальним часом простою вважається оптимальною;

- Ефективність використання ресурсів: ступінь використання обчислювальних потужностей, енергоефективність та обсяг пам'яті, що використовується;

- Швидкість відновлення після помилок: час, необхідний для повного відновлення роботи після помилки або збою в будь-якому з компонентів.

РОЗДІЛ 4. ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

4.1. Поняття відмовостійкості

Відмовостійкість обчислювальних систем - це здатність системи продовжувати функціонувати навіть у випадку відмови одного або кількох її компонентів. Відмовостійкі системи здатні автоматично відновлювати свою працездатність або виконувати завдання без втрати продуктивності, що особливо важливо для критично важливих систем, таких як банківські, медичні, військові та інші.

4.2. Резервування компонентів

Одним із ключових методів забезпечення відмовостійкості є **резервування компонентів**. Це може бути резервування як апаратного, так і програмного забезпечення.

4.2.1. Апаратне резервування

Апаратне резервування полягає в тому, що критично важливі компоненти системи (блоки живлення, мережеві інтерфейси, сховища даних) дублюються. У разі відмови одного з компонентів система автоматично перемикається на резервний без значних збоїв у роботі.

RAID-масиви: для забезпечення відмовостійкості на рівні зберігання даних використовуються різні рівні RAID (Redundant Array of Independent Disks). Найбільш поширені — RAID 1 (віддзеркалення) та RAID 5 (з розподіленою парністю), які дозволяють зберігати дані навіть у випадку відмови одного з жорстких дисків.

RAID (Redundant Array of Independent Disks) — це технологія організації дискових накопичувачів, що забезпечує підвищення продуктивності, відмовостійкості або обох цих показників одночасно. Рівні RAID визначають спосіб розподілення даних між дисками. Нижче описані основні рівні RAID.

RAID 0 (Striping)

Принцип роботи: Дані розподіляються блоками між кількома дисками, без дублювання.

Переваги:

- максимальна швидкість запису та читання;

- використовується весь обсяг накопичувачів.

Недоліки:

- відсутність відмовостійкості: вихід з ладу одного диска спричиняє втрату всіх даних.

RAID 1 (Mirroring)

Принцип роботи: Дані дублюються на кожному з дисків.

Переваги:

- висока відмовостійкість: вихід з ладу одного диска не впливає на доступність даних;

- проста реалізація.

Недоліки:

- ефективний обсяг зберігання становить лише 50% від загального.

RAID 5 (Striping with Parity)

Принцип роботи: Дані розподіляються між усіма дисками з додаванням контрольних блоків (паритету), які дозволяють відновлювати інформацію у разі відмови одного диска.

Переваги:

- компроміс між продуктивністю, відмовостійкістю та ефективністю обсягу;
- втрата одного диска не впливає на доступність даних.

Недоліки:

- зниження продуктивності під час запису через обчислення паритету;
- мінімальна кількість дисків: 3.

RAID 6 (Striping with Double Parity)

Принцип роботи: Схожий на RAID 5, але додається ще один контрольний блок (подвійний паритет), що забезпечує відновлення даних навіть за виходу з ладу двох дисків.

Переваги:

- висока відмовостійкість: можливість роботи при відмові до двох дисків;
- підходить для великих систем.

Недоліки:

- складність у реалізації;
- більше дисків використовується для зберігання паритету.

RAID 10 (1+0)

Принцип роботи: Поєднання RAID 1 (дзеркалення) і RAID 0 (розподіл). Дані дзеркалюються, а потім розподіляються між кількома дисками.

Переваги:

- висока швидкість читання і запису;
- висока відмовостійкість.

Недоліки:

- ефективний обсяг зберігання становить 50% від загального;
- мінімальна кількість дисків: 4.

RAID 50 (5+0)

Принцип роботи: Поєднання RAID 5 і RAID 0. Дані розподіляються між декількома групами RAID 5, які потім об'єднуються за принципом RAID 0.

Переваги:

- вища продуктивність порівняно з RAID 5;
- висока відмовостійкість при використанні великих систем.

Недоліки:

- складність конфігурації;
- мінімальна кількість дисків: 6.

RAID 60 (6+0)

Принцип роботи: Поєднання RAID 6 і RAID 0. Дані розподіляються між групами RAID 6 з додатковим дублюванням паритету.

Переваги:

- відмінна відмовостійкість: система витримує вихід з ладу до 4 дисків.
- висока продуктивність для читання.

Недоліки:

- дуже складна реалізація.

- потребує великої кількості дисків.

Таблиця 3.1 - Переваги та недоліки рівнів RAID

RAID рівень	Відмовостійкість	Продуктивність	Обсяг пам’яті	Недоліки
RAID 0	Відсутня	Максимальна	100%	Втрата даних при відмові одного диска
RAID 1	Висока	Висока	50%	Використовується лише половина загального обсягу
RAID 5	Середня (1 диск)	Середня	67–80%	Зниження швидкості запису через обчислення паритету
RAID 6	Висока (2 диски)	Середня	50–70%	Складна реалізація
RAID 10	Дуже висока	Висока	50%	Мінімальна кількість дисків: 4
RAID 50	Висока	Вища, ніж RAID 5	67–80%	Потребує багато дисків для реалізації
RAID 60	Дуже висока	Висока	50–70%	Складність у налаштуванні та висока вартість

Резервне живлення: сервери та дата-центри часто використовують резервні джерела живлення (ДБЖ або генератори), щоб забезпечити безперервну роботу систем у разі перебоїв з електропостачанням.

Рисунок 4.1 - Два блоки живлення у сервері

4.2.2. Програмне резервування

Програмне резервування передбачає дублювання або резервне копіювання програмного забезпечення та даних. Системи можуть автоматично запускати резервні копії програм після виявлення збою або використовувати **віртуальні машини** для резервування процесів.

Кластери з відмовостійкістю: у кластерних системах резервування досягається шляхом створення кількох вузлів, що виконують однакові задачі. Якщо один вузол виходить з ладу, інший автоматично бере на себе його функції.

Автоматичне перемикання на резервні сервери: програмне забезпечення

також може бути налаштоване для автоматичного перемикання на резервні сервери в разі відмови основного.

4.2.3. Гаряче, тепле та холодне резервування

Одним із важливих аспектів відмовостійкості є резервування, яке забезпечує наявність запасних ресурсів для швидкого відновлення роботи системи.

Гаряче резервування (Hot Standby) передбачає постійну готовність резервного обладнання до використання.

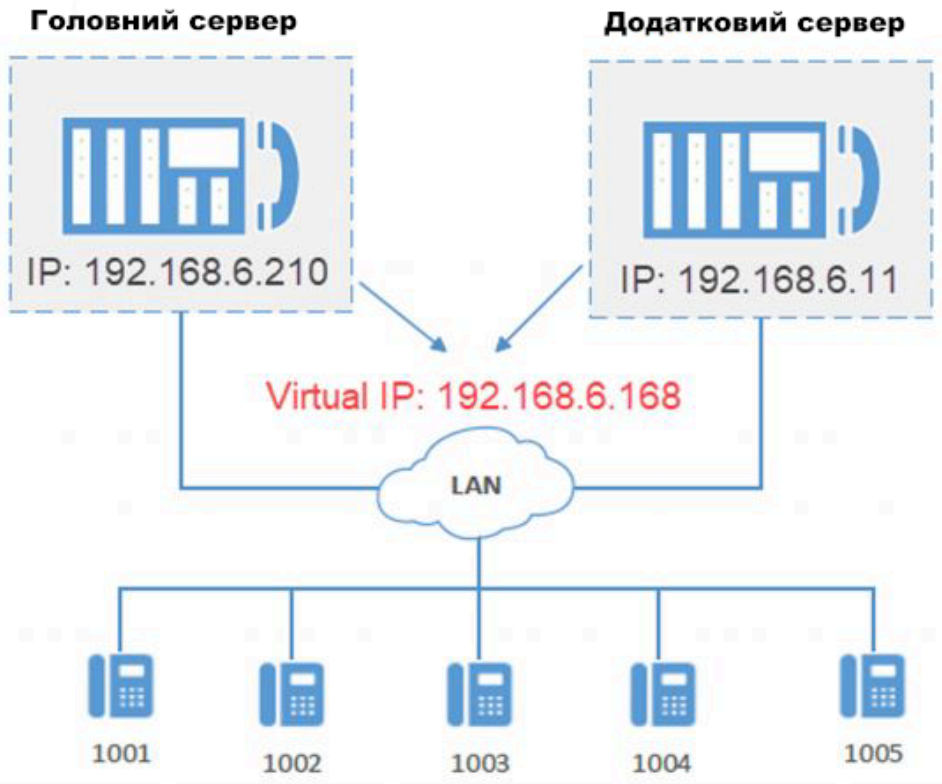


Рисунок 4.2 - Приклад роботи гарячого резервування

Гаряче резервування передбачає наявність резервного обладнання чи програмного забезпечення, яке завжди знаходиться в активному стані або готове до негайного використання [7]. Така система автоматично або з мінімальними затримками переходить на резервний компонент у разі відмови основного.

Основні характеристики гарячого резервування:

- Мінімальний час відновлення: система переходить на резервний компонент практично миттєво;

- Паралельна робота: резервні компоненти можуть працювати паралельно з основними, постійно синхронізуючи дані;

- Висока вартість: через необхідність постійної роботи резервного обладнання.

Реалізація гарячого резервування:

1. **Кластер високої доступності (HA Clustering):**

У кластерах високої доступності кілька серверів працюють разом, забезпечуючи безперервну роботу. Прикладом є *Failover Clusters* у Windows Server. У разі збою одного з вузлів його завдання автоматично беруть на себе інші вузли;

2. **Реплікація баз даних у режимі реального часу:**

У базах даних, наприклад PostgreSQL, функція *Hot Standby* дозволяє створити резервний сервер, який постійно синхронізує дані з основним сервером. У разі відмови основного серверу резервний відразу переходить в активний стан;

3. **Мережеве обладнання з гарячим резервуванням:**

У мережевих маршрутизаторах і комутаторах технології *HSRP* (Hot Standby Router Protocol) або *VRRP* (Virtual Router Redundancy Protocol) забезпечують автоматичний перехід на резервний маршрутизатор без переривання трафіку [8].

Таблиця 3.2 - Приклад таблиці для гарячого резервування

Система	**Тип резервування**	**Час переключення**	**Типи завдань**
Кластер баз даних	Hot Standby	< 1 сек	Зберігання даних
Мережеві маршрутизатори	HSRP/VRRP	< 1 сек	Маршрутизація
Серверні кластери	HA Clustering	Миттєво	Обчислювальні задачі

Тепле резервування (warm standby) — це метод резервування, при якому резервний (запасний) сервер або система знаходиться у стані готовності до використання з мінімальними затримками. Цей підхід забезпечує баланс між швидкістю відновлення (RTO) і витратами. У теплій резервній конфігурації резервний сервер підтримується в активному стані, але не використовується для обробки поточного робочого навантаження до моменту збою основної системи.

Як це працює:

- основна система виконує всі операції та обробляє запити;

- резервна система синхронізується з основною, зберігаючи копію даних або налаштувань, але не бере участі у поточній роботі;

- у разі збою основної системи резервна система активується, стаючи основною.

Приклад: компанія використовує вебдодаток для обслуговування клієнтів:

Основний сервер знаходиться в дата-центрі "A". Він обробляє всі запити клієнтів і постійно оновлює базу даних.

Резервний сервер розташований у дата-центрі "Б". Цей сервер підтримується в активному стані та періодично отримує копії даних з основного сервера через реплікацію бази даних.

Якщо основний сервер виходить з ладу (наприклад, через апаратний збій або мережеві проблеми), система автоматично перенаправляє запити клієнтів на резервний сервер.

Резервний сервер швидко починає обслуговувати запити, оскільки він уже налаштований і має актуальні дані.

Переваги теплового резервування:

- швидке відновлення - мінімізує час простою;

- зменшені витрати у порівнянні з гарячим резервуванням (hot standby), де резервний сервер працює на повну потужність.

Недоліки:

- ризик втрати деяких даних між моментами реплікації, якщо процес не є безперервним;

- резервний сервер використовує ресурси, але не обробляє запити, що може бути неефективним у деяких сценаріях;

- тепле резервування є популярним підходом для систем, де швидкість відновлення важлива, але витрати на гаряче резервування занадто високі.

Холодне резервування (Cold Standby) активується лише у разі виходу з ладу основного обладнання.

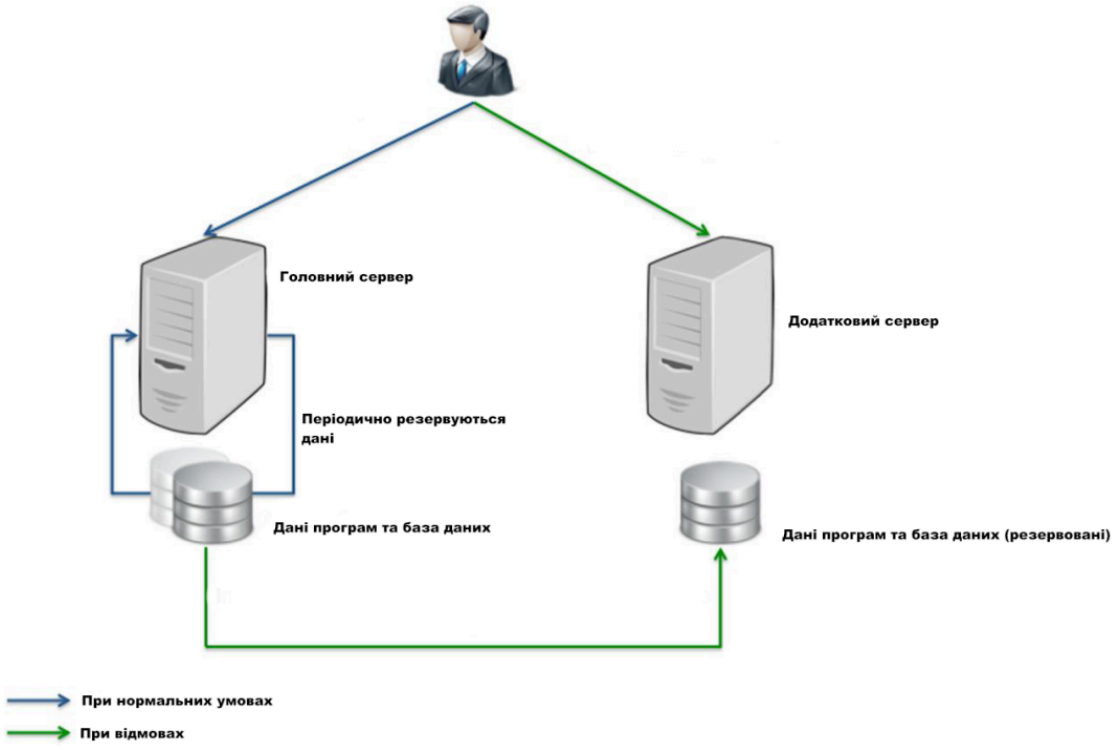


Рисунок 4.3 - Приклад роботи холодного резервування

Холодне резервування передбачає наявність резервного обладнання або системи, які неактивні до моменту відмови основного компонента. У разі збою активується резервний компонент, але це може зайняти більше часу, оскільки необхідно виконати запуск і налаштування.

Основні характеристики холодного резервування:

- довший час відновлення: потрібен додатковий час для запуску резервного компонента;

- менші витрати: резервне обладнання не споживає ресурси під час роботи основної системи;

- простота реалізації: не вимагає складної синхронізації в реальному часі.

Реалізація холодного резервування:

1. **Резервні сервери:**

У великих організаціях резервні сервери знаходяться в режимі очікування. У разі збою основного сервера адміністратор вручну запускає резервний;

2. **Резервні копії даних:**

Системи зберігання резервних копій, такі як *Veeam Backup* або *Acronis*, дозволяють створити копії важливих даних і відновити їх на резервному обладнанні в разі відмови основного;

3. **Резервування електроживлення:**

У разі збою основного джерела живлення активується резервний генератор або джерело безперебійного живлення (UPS), що запускається вручну.

Таблиця 3.3 Приклад таблиці для холодного резервування

Система	**Тип резервування**	**Час переключення**	**Типи завдань**
Резервний сервер	Cold Standby	5-10 хв	Зберігання даних
Система резервного живлення	UPS, генератор	1-5 хв	Електроживлення
Резервна копія бази даних	Backup System	10-30 хв	Відновлення даних

Практичне застосування гарячого та холодного резервування:

1. **Критичні системи:** У банківських системах, авіації та медицині використовують гаряче резервування, через високі вимоги до безперервності роботи;
2. **Системи з меншими вимогами:** У менших бізнесах або системах, де допустимі короткі простої, часто використовується холодне резервування для зниження витрат.

Хоча такий метод резервування і є більш вигідним по витратам на обладнання, але не є цілком зручним та надійним для більшості випадків, крім тих випадків, коли користувачам такої системи не критично почекати поки холодним методом резервуванням відновиться доступ до системи.

Таблиця 3.4 - Порівняння гарячого та холодного резервування

Параметр	Гаряче резервування	Холодне резервування
Час відновлення	Миттєвий (< 1 сек)	Від кількох хвилин
Синхронізація даних	Постійна, у реальному часі	Не потрібна
Вартість	Висока	Низька
Використання ресурсів	Постійно використовується	Використовується при відмові
Складність реалізації	Висока	Низька

Таким чином, вибір між гарячим та холодним резервуванням залежить від критичності системи, доступних ресурсів та бюджету організації.

4.3. Методи забезпечення безперервної роботи

Одним із ключових елементів відмовостійкості є здатність забезпечити **безперервну роботу** системи, навіть у випадку серйозних збоїв. Для цього використовуються різні методи.

4.3.1. Дублювання операцій

Один із методів забезпечення безперервної роботи - це дублювання операцій, коли ті самі обчислювальні процеси виконуються на кількох серверах або процесорах одночасно. Якщо один з компонентів виходить з ладу, інші можуть завершити роботу без перерви.

4.3.2. Автоматичне відновлення процесів

У випадку збоїв обчислювальні системи повинні мати здатність автоматично відновлювати процеси або операції з останньої збереженої точки. Це забезпечує мінімальні втрати даних і часу, необхідного для відновлення функцій системи.

4.3.3. Реплікація даних

Ще один важливий аспект безперервної роботи - **реплікація даних** у реальному часі між різними серверами або центрами обробки даних. Реплікація дозволяє автоматично синхронізувати дані між кількома вузлами, забезпечуючи

доступність інформації у разі відмови основного сервера.

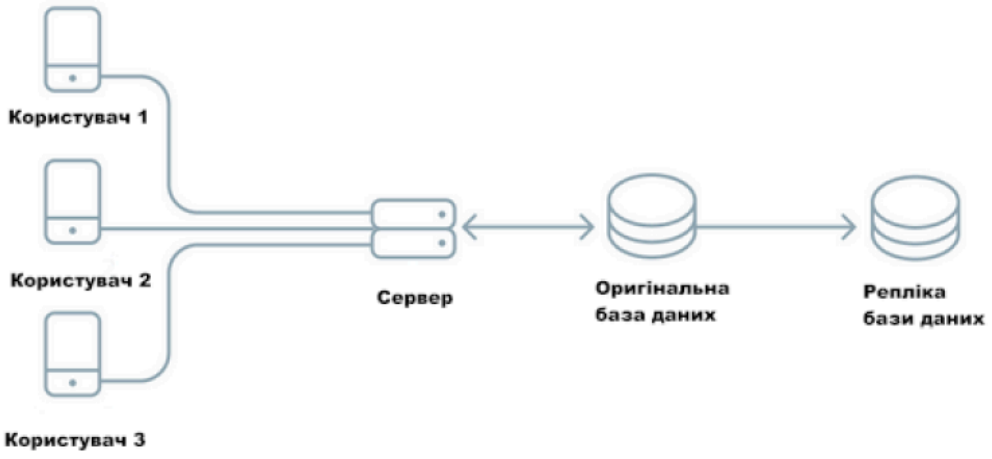


Рисунок 4.4 - Приклад робити реплікації бази даних сервера

4.4. Тестування на відмовостійкість

Для того щоб система дійсно була відмовостійкою, необхідно проводити регулярне **тестування** на різні сценарії збоїв і аварійних ситуацій. Це дозволяє виявляти вразливості і вдосконалювати механізми захисту та відновлення.

4.4.1. Тестування сценаріїв відмови

Тестування відмов включає симуляцію збоїв ключових компонентів системи для оцінки її здатності до автоматичного відновлення. Наприклад, це може бути відключення одного з серверів або вимкнення джерела живлення для оцінки роботи резервного обладнання.

4.4.2. Регулярні стрес-тести

Стрес-тести системи дозволяють визначити її здатність до роботи у критичних умовах, таких як максимальне навантаження або перевищення ресурсів. Такі тести допомагають підготувати систему до пікових ситуацій і виявити потенційні «вузькі місця» в її архітектурі.

4.5. Відповідність стандартам відмовостійкості

Для забезпечення високого рівня відмовостійкості існують міжнародні стандарти, такі як **ISO/IEC 27001** [9] для інформаційної безпеки або **ISO/IEC 24762** для відновлення після аварій. Дотримання цих стандартів допомагає організаціям підвищити відмовостійкість своїх систем та забезпечити належний рівень захисту.

4.6. Висновки щодо забезпечення відмовостійкості

Забезпечення відмовостійкості обчислювальних систем включає використання різноманітних методів та технологій, що дозволяють мінімізувати простої, втрати даних та збої. Ключові підходи включають резервування компонентів, моніторинг, дублювання операцій та тестування систем.

РОЗДІЛ 5. ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ АВТОНОМНОСТІ І ВІДМОВОСТІЙКОСТІ

В сучасному світі, особливо, якщо брати сьогодення, питання автономності та відмовостійкості обчислювальних систем стає дуже актуальним. Тому, зазначаючи досвід вже існуючих автономних та відмовостійких систем, в цій роботі буде побудовано схему приватної компанії, в якій було спроектовано та застосовано новітні методи та засоби, які підвищують працездатність, автономність та відмовостійкість обчислювальних систем.

Допустимо, що є нагальна потреба забезпечити високу автономність та відмовостійкість офісу на 40 кабінетів, один з яких є серверною кімнатою, по 2 офісних комп’ютери кожний з периферійною технікою типу сканерів, принтерів, багатофункційних пристроїв та телефонії для зв’язку між кабінетами.

Згідно з проведеним аналізом та вищезазначеними розрахунками окреслимо причини, через які виникають помилки та затримки в роботі обчислювальних систем:

- коливання напруги та відсутність електроживлення;
- критичні температури та вологість;
- шкідливе програмне забезпечення;
- мережеві фактори;
- резервування та відновлення після збоїв;
- людські фактори.

Отже, дивлячись на зазначені чинники, виділимо етапи впровадження покращень.

Для вирішення проблеми коливань напруги та відсутність електроживлення використаємо стабілізатори або джерела безперебійного живлення та додаткові

джерела живлення.

Для запобігання статичній електриці, корозії компонентів та перегріву будемо використовувати системи вентиляції та кондиціонування.

Щоб протидіяти можливим кібер атакам та шкідливому програмному забезпеченню встановимо мережевий екран (Firewall) та антивірус.

Мережеві проблеми можна вирішити встановленням оптоволоконного інтернет підключення та додатковим джерелом інтернет зв'язку, який майже залежить від зовнішніх факторів - супутниковим інтернет зв'язком.

Проблеми резервування та відновлення роботи серверу після збоїв вирішуються гарячим резервуванням елементів мережі.

Людські фактори вирішуються застосуванням систем контролю доступу та навчання персоналу.

Далі представлено схему роботи даного об'єкту:

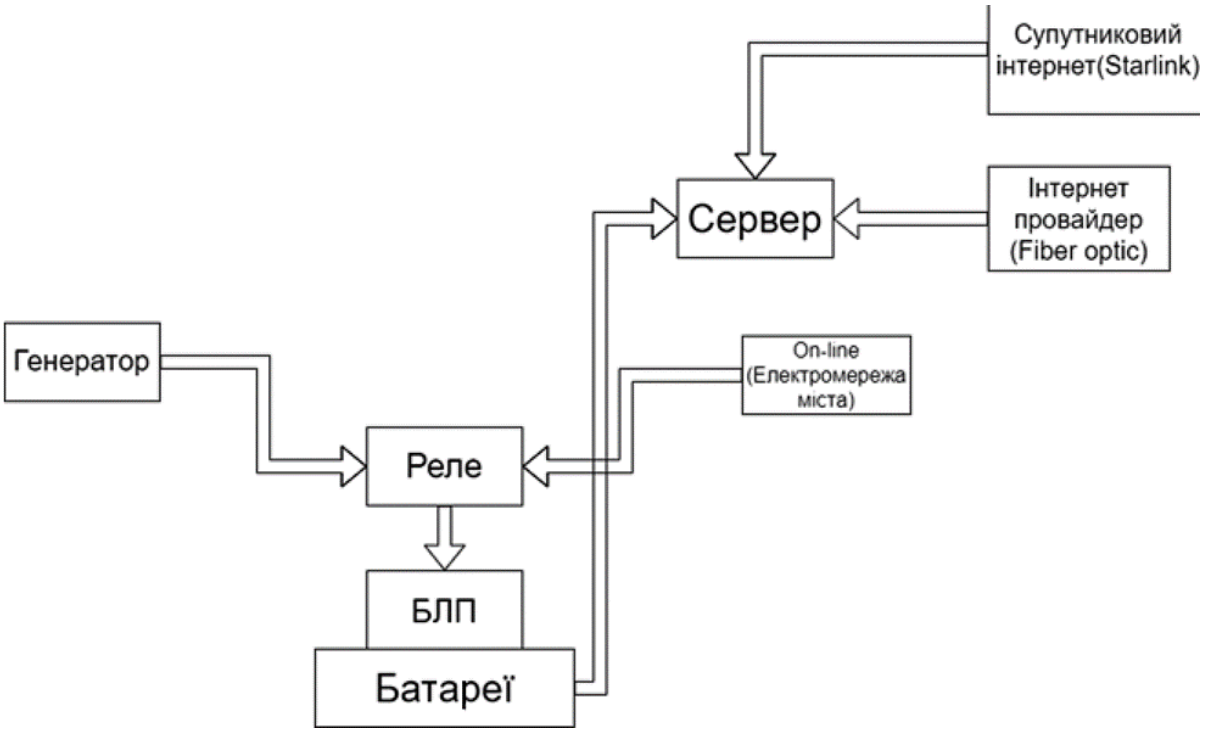


Рисунок 5.1 - Загальна схема роботи підприємства

5.1. Критичні температури та вологість

Серед чинників які можуть шкодити автономності та відмовостійкості обчислювальних систем йдуть критичні температури та вологість.

Найефективніший спосіб контролювати температуру в серверних приміщеннях - це використання сучасних систем охолодження:

Інсталяція потужних кондиціонерів з регуляцією температури забезпечує підтримання оптимальної температури у серверній, що збільшує автономність, ефективність серверного обладнання.

Для дата-центрів використовуються спеціалізовані кондиціонери, які мають високу потужність та точний контроль температури та вологість - прецизійні.

Прецизійні кондиціонери - це системи кондиціонування, які забезпечують постійний мікроклімат у приміщенні, регулюючі температуру і вологість.

У деяких випадках кондиціонування повітря в приміщенні повинно забезпечувати надточні параметри повітря з мінімальним відхиленням, наприклад в серверних, як в нашому випадку. Коли звичайні кондиціонери не можуть впоратися з цим завданням, використовуються прецизійні кондиціонери. Назва цього обладнання походить від слова «precision», що в перекладі означає «точний». Прецизійні кондиціонери використовуються для забезпечення не тільки точних температурних параметрів, але й рівня вологості та руху повітря в приміщенні.

Кожна система прецизійного кондиціонування розроблена з урахуванням параметрів повітря, які необхідно забезпечити в приміщенні. Системи кондиціонування включають в себе теплообмінники, вентилятори, компресори, повітроводи, зволожувачі, блоки управління системою і різні датчики. У більшості випадків прецизійні кондиціонери монтуються в шафу, але також доступні настінні, які є незамінними для приміщень з обмеженим вільним

простором. Прецизійні кондиціонери можуть бути фреоновими, з водяним охолодженням або змішаними [2].

Фреонові кондиціонери охолоджують повітря за допомогою холодильного контуру з фреоном і двома теплообмінниками; випарник і конденсатор можуть бути встановлені в одному корпусі або в окремих блоках (внутрішньому і зовнішньому). Кондиціонери з водяним охолодженням охолоджуються за допомогою води або гліколевого розчину і зовнішньої системи (чиллера). Кондиціонери змішаного типу працюють на фреоні та воді.

Слід зазначити, що прецизійні кондиціонери оснащені енергозберігаючою системою природного охолодження. Коли температура зовнішнього повітря знижується, воно забирається кондиціонером і використовується для охолодження повітря в приміщенні. При цьому компресор може бути переведений в економний режим роботи або повністю вимкнений. Це знижує енергоспоживання кондиціонера, що збільшить час автономності системи.

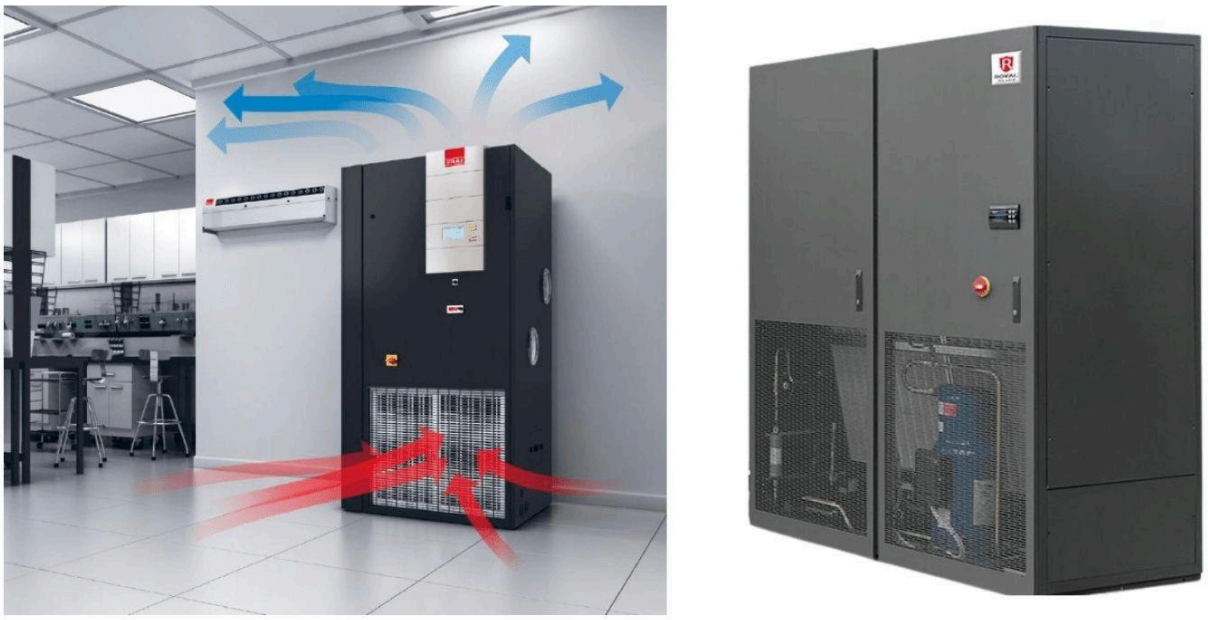


Рисунок 5.1.1 - Прецизійний кондиціонер типу шафи

Крім самого охолодження, регулярний моніторинг та автоматизація дозволяють уникнути перегріву або високої вологості.

Встановлення датчиків температури та вологості у критичних точках серверної дозволяє в реальному часі слідкувати за параметрами навколишнього середовища.

Автоматизовані системи повідомлятимуть персонал про перевищення допустимих значень та можуть автоматично налаштувати системи охолодження.

Також, циркуляція повітря відіграє велику роль в боротьбі з виникненням статичної електрики та зайвої вологості. Використання спеціальних підлог з отворами для циркуляції холодного повітря знизу приміщення та відведення теплого повітря зверху.

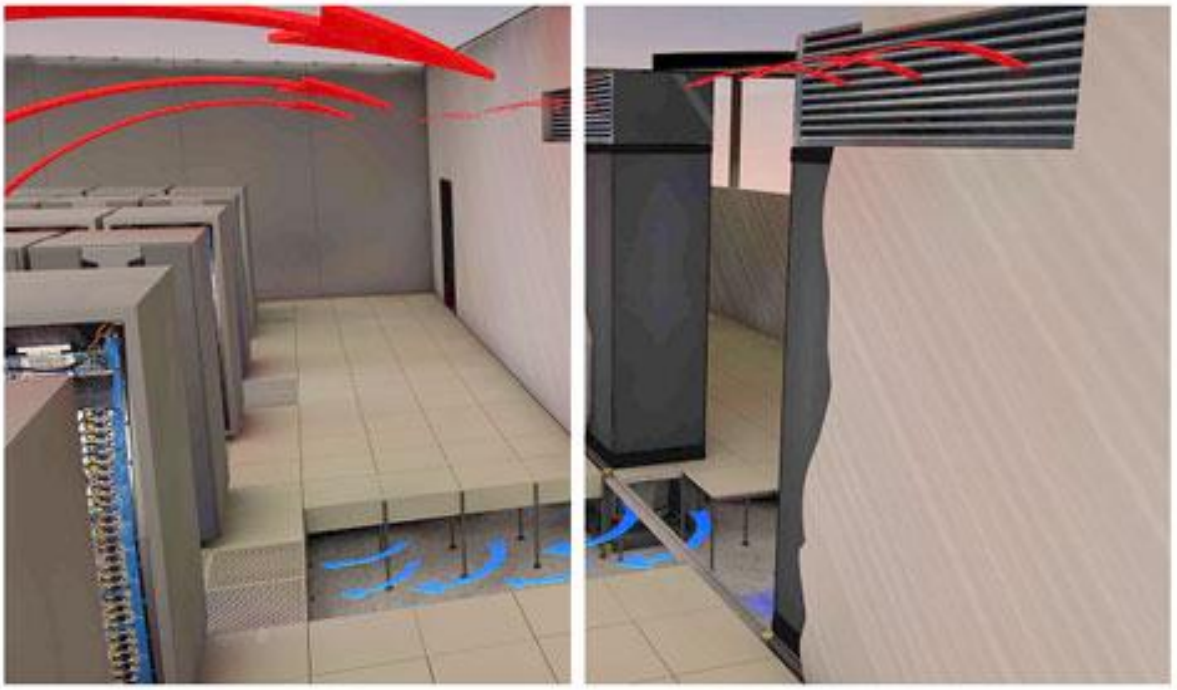


Рисунок 5.1.2 - Додаткова вентиляція в серверній

Забезпечення правильного розподілу повітря через вентиляційні канали та фільтри дозволяє уникнути перегріву певних зон.

Сервери розташовують таким чином, щоб утворювались “гарячі” та “холодні” коридори: в одному ряду забір холодного повітря, а в іншому - вихід теплого.

Це запобігає змішуванню холодного та теплого повітря і підвищує ефективність охолодження.

Використання осушувачів повітря допомагає підтримувати необхідний рівень вологості (30-50%) та запобігає надмірній вологості, що може спричинити корозію та короткі замикання.

Якщо в серверній приміщенні повітря занадто сухе, це може призвести до статичної електрики, що небезпечно для обладнання. У таких випадках можна використовувати зволожувачі для підтримки потрібного рівня вологості.

Сервери з великим тепловиділенням варто розміщувати рівномірно в серверній, щоб уникнути перегріву локальних зон.

Найбільш “гарячі” сервери рекомендується встановлювати ближче до джерел охолодження або створювати окремі зони для серверів з інтенсивним охолодженням.

Отже, контроль температури та вологості в серверних приміщеннях є критично важливим для забезпечення стабільної роботи обчислювальних систем.

Поєднання охолоджувальних систем, вентиляції, моніторингу та правильної організації простору допомагає мінімізувати ризики, пов'язані з перегрівом і підвищеною вологістю.

Кожен з цих заходів може суттєво підвищити надійність роботи серверного обладнання та збільшити його тривалість експлуатації.

5.2. Шкідливе програмне забезпечення

Наступною причиною, що може нашкодити автономності та відмовостійкості обчислювальних систем - це шкідливе програмне забезпечення та хакерські атаки.

Для захисту обчислювальних систем від шкідливого програмного забезпечення та кібератак важливо використовувати багаторівневий підхід до безпеки, що включає кілька методів для запобігання, виявлення і реагування на загрози.

В серверній потрібно встановити міжмережевий екран (firewall), для контролю за трафіком, захисту мережі та протидії можливим кібератакам. Для захисту та контролю мережі можна використовувати звичайний програмний міжмережевий екран, але вони не завжди дають необхідний рівень захисту, що може призвести до відмов або зараженню всієї системи та викрадення даних.

Тому, краще використовувати firewall сервери, наприклад від компанії Fortinet, які одразу йдуть з антивірусним забезпеченням на обчислювальні системи користувачів.

Рисунок 5.2.1 - Мережевий екран FortiGate 900G

Даний мережевий екран має 2 блоки живлення, що збільшує його відмовостійкість під час можливих змін напруги, що може призвести до відмови одного з них без впливу на роботу системи, штучний інтелект, що в режимі реального часу сканує мережу на підозрілий трафік, хакерські атаки та має віртуальну середу, де можна слідкувати за ресурсами, що використовуються та керувати мережевими додатками [4].

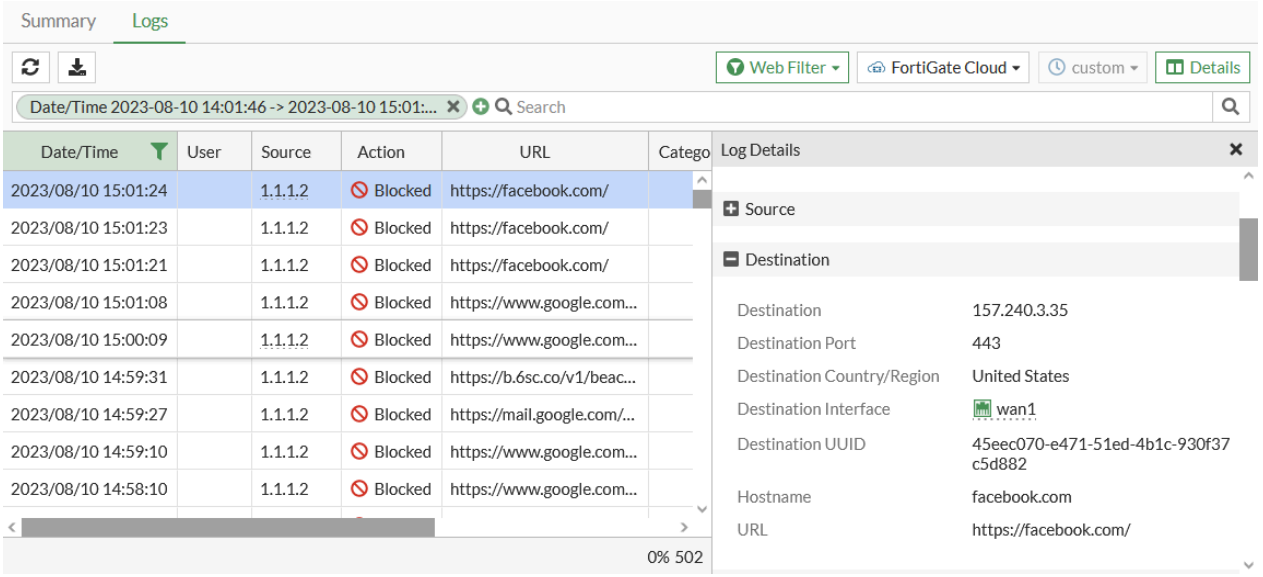


Рисунок 5.2.2 - Приклад функції фільтру мережі через фаервол Fortigate

Також, цей мережевий екран має системи виявлення та запобігання вторгненням (IDS/IPS) - що моніторять трафік і поведінку в мережі для виявлення підозрілих дій і можуть автоматично блокувати їх, функцію шифрування даних: яке шифрує крізними методами всі важливі дані під час зберігання і передачі, щоб у випадку викрадення інформації вона залишилася недоступною зловмисникам та функцію анти-DDoS, що відслідковує з’єднання сервера на можливі DDoS атаки і запобігає перевантаженню сервера.

Даний мережевий екран робить віртуальну середу підключених користувачів та відслідковує їх дії, якщо дії перестають збігатися з тими, що на

сервері даний мережевий екран блокує даний комп’ютер та видаляє його з мережі, щоб не заражати інші ділянки мережі. В цей самий час, антивірусне програмне забезпечення, що встановлене на персональних комп’ютерах користувачів, перевіряє систему на можливі мережеві атаки, підозрілі дії або шкідливе програмне забезпечення та відправляє відгуки про роботу на основний сервер.

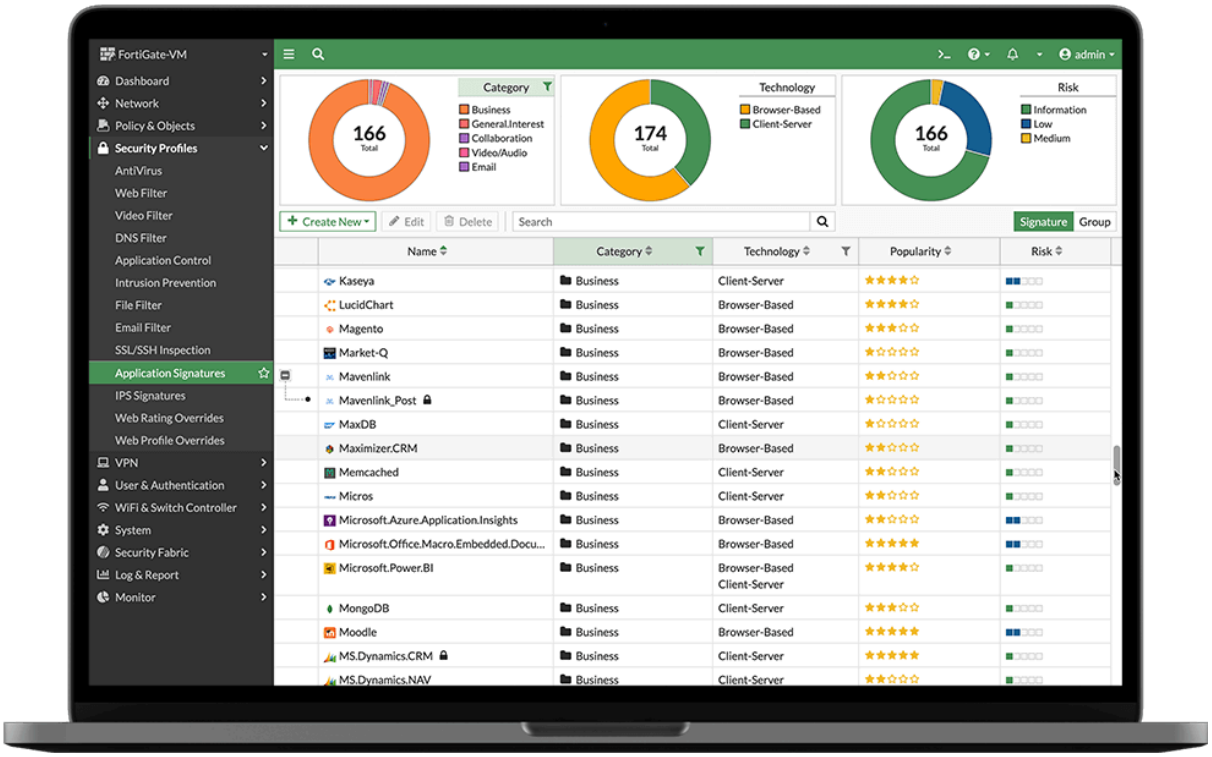


Рисунок 5.2.3 - Веб інтерфейс фаервола Fortigate

Проведені заходи підвищать відмовостійкість системи через унеможливлення хакерських атак та шкідливого програмного забезпечення. Також, штучний інтелект зменшує можливість того, що сервер потребує дії зі сторони. Здібності до адаптації, відслідковування патернів, які можуть вказувати на можливі атаки на мережу та можливість самостійно приймати рішення зменшує необхідність взаємодії з фаерволом.

5.3. Мережеві чинники

Четвертим чинником, який може призвести до відмов та затримок і пов’язаний з попередніми чинниками - це мережеві фактори. Втрата пакетів, відсутнє з’єднання з мережею та перевантаження мережі затримує роботу підприємства. Для вирішення мережевих проблем є декілька етапів:

Перший з них, це резервне джерело інтернет зв’язку, що не залежить від електроживлення. Хоча, в зазначеній вище схемі підприємства, ми і захистили електромережу підприємства від відключень світла від міста, але для мережевого з’єднання потрібні додаткові схеми захисту.

Перш за все, це провести до підприємства не звичайну виту пару, яка залежить від електромережі, а оптоволокно (fiber optic). Даний тип передачі сигналу не залежить від електромережі, має вищу пропускну здатність ніж звичайний кабель, стійкий до радіоперешкод та зовнішніх факторів.

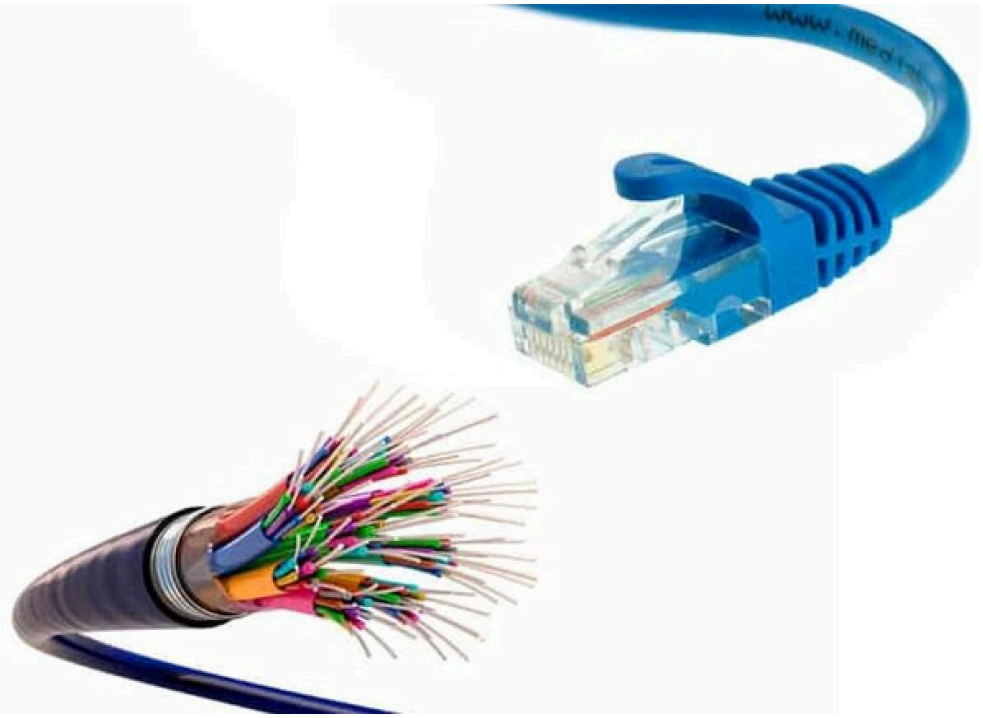


Рисунок 5.3.1 - Порівняння вигляду витої пари та оптичного волокна

Основні відмінності між оптичним кабелем та витою парою.

Технологія передачі даних:

- оптичний кабель використовує світлові імпульси, які проходять через оптичне волокно. Світло має властивість переносити інформацію на великі відстані без значної втрати сигналу, оскільки оптичні кабелі майже не піддаються електромагнітним перешкодам;

- вита пара використовує електричний сигнал, що проходить по металевих провідниках (зазвичай з міді). Щоб зменшити перешкоди, пара дротів переплетена (звита), що також знижує втрати сигналу, але це менш ефективно, ніж оптика.

Швидкість передачі даних:

- оптичний кабель підтримує набагато вищу швидкість передачі даних до кількох терабітів на секунду у сучасних системах. Це робить оптику найкращим вибором для передачі великих обсягів даних на великі відстані, зберігаючи стабільність і швидкість;

- вита пара обмежена швидкістю до 1 Гбіт/с у звичайних кабелях категорії CAT5e, до 10 Гбіт/с у кабелях CAT6 та CAT7. На великих відстанях сигнал швидко слабшає, через що звичайно кабелі використовують для локальних мереж або підключення всередині будівлі.

Відстань передачі даних:

- оптичний кабель підтримує стабільний зв'язок на відстанях до 40 км для стандартних кабелів та до 100 км і більше для спеціалізованих рішень;

- вита пара ефективна на відстанях до 100 метрів, хоча зі спеціальним обладнанням її можна використовувати на трохи більшій відстані. Але для більш віддаленого з'єднання знижуються швидкість і стабільність.

Стійкість до зовнішніх впливів:

- оптичний кабель не піддається впливу електромагнітних та радіочастотних перешкод, тому добре підходить для індустріальних зон, де є багато джерел електромагнітного випромінювання. Він також стійкий до кліматичних умов, що робить його надійним для зовнішніх мереж;

- вита пара більш вразлива до електромагнітних перешкод, особливо в зонах із сильними радіохвилями чи потужними електричними полями, що може впливати на якість зв'язку.

В усіх сучасних серверах є порти підключення для оптичного волокна, а потім вже від серверної, до звичайних користувачів підводиться вита пара. Так як серверна в схемі вже енергонезалежна від зовнішніх умов то конвертування оптичного волокна в виту пару буде безперервною і не буде залежить від відключень світла.

Хоча, оптичного волокна буде більш ніж достатньо для того, щоб інтернет мережа не зникала, але все одно, для більшої відмовостійкості системи необхідно мати додаткове джерело інтернет зв’язку.

Таким додатковим джерелом може бути супутниковий інтернет зв’язок, наприклад Starlink.

Рисунок 5.3.2 - Супутникова система Starlink

Навіть при відсутності постачання інтернет з’єднання від провайдера оптоволоконного інтернет зв’язку супутникова система з’єднання може надавати доступ з інтернет мережею [3].

5.4. Резервування та відновлення після збоїв

Для захисту даних сервера під час можливих кібератак чи помилок, що можуть призвести до пошкодження бази даних слід застосовувати технологію RAID для організації накопичувачів.

Серед усіх RAID технологій - RAID 6 забезпечує найкращу відмовостійкість у стандартних умовах [11]. Робота RAID 6 полягає в тому, що дані розподіляються між усіма дисками з додаванням двох контрольних блоків (паритету), які дозволяють відновлювати інформацію у разі відмови навіть двох дисків.

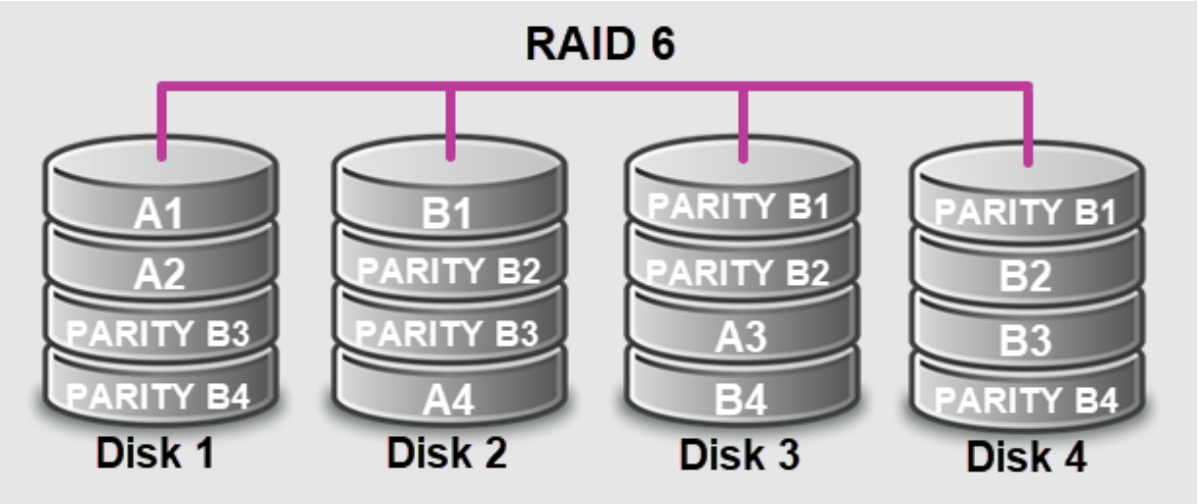


Рисунок 5.4.1 - Принцип формування RAID 6

RAID 6 працює на контрольних блоках (паритетах). Для того, щоб зрозуміти, що таке паритет і чому він забезпечує в нашій системі більшу безпеку

даних при збоях треба зрозуміти, що саме являє собою паритет.

Паритет - це обчислювальне значення, яке використовується для відновлення даних з інших дисків у випадку відмови якогось диску в наборі, в нашому випадку це два диски. Паритет визначає кількість парних та непарних біт в числі, що допомагає у відновленні даних у випадку втрати послідовності чисел, що відбувається під час відмови певної кількості дисків, в нашому випадку - два.

У випадку, коли треба забезпечити безперервну роботу сервера навіть при відмові одного з елементів мережі, зазвичай, використовують гаряче або холодне резервування обладнання.

Для більшої безпеки для описаного раніше проекту офісу було обрано гарячий тип резервування, при якому завжди є резервний елемент обладнання, який знаходиться в активному стані та при відмові основного елемента обладнання виконує функції за нього [7]. При такому типі резервування система автоматично та майже без затримок продовжує працювати.

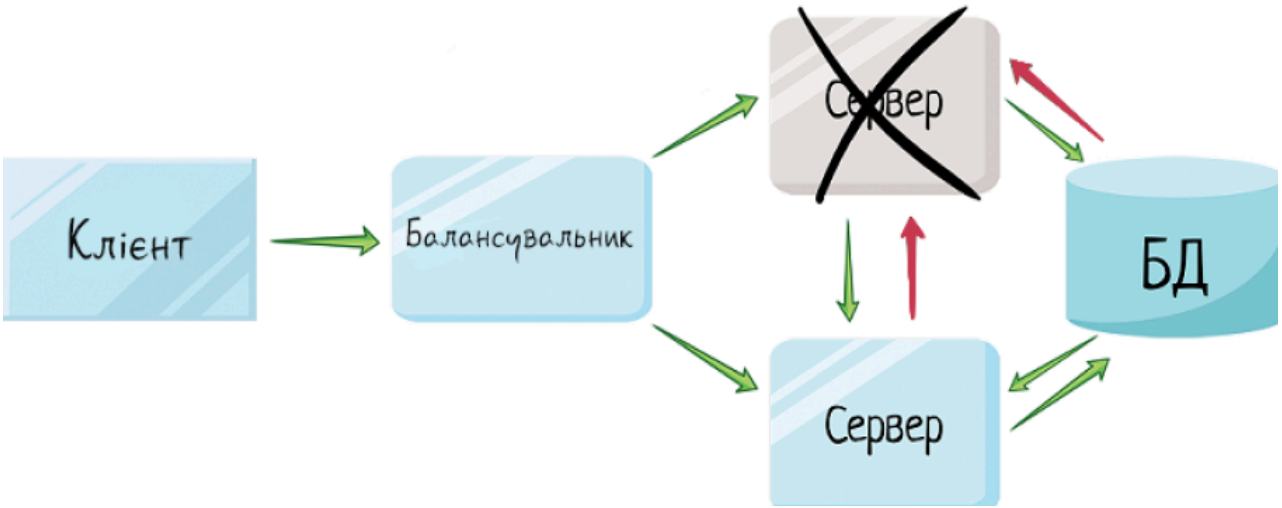


Рисунок 5.4.2 - Принцип роботи гарячого резервування

Зазвичай, для цього декілька комп'ютерів, а іноді навіть більше ніж десяток серверів під'єднуються до єдиного кластеру, щоб при відмові або при затримках певної кількості серверів можна було б підключитися на робочий сервер автоматично, що значно підвищує відмовостійкість системи.

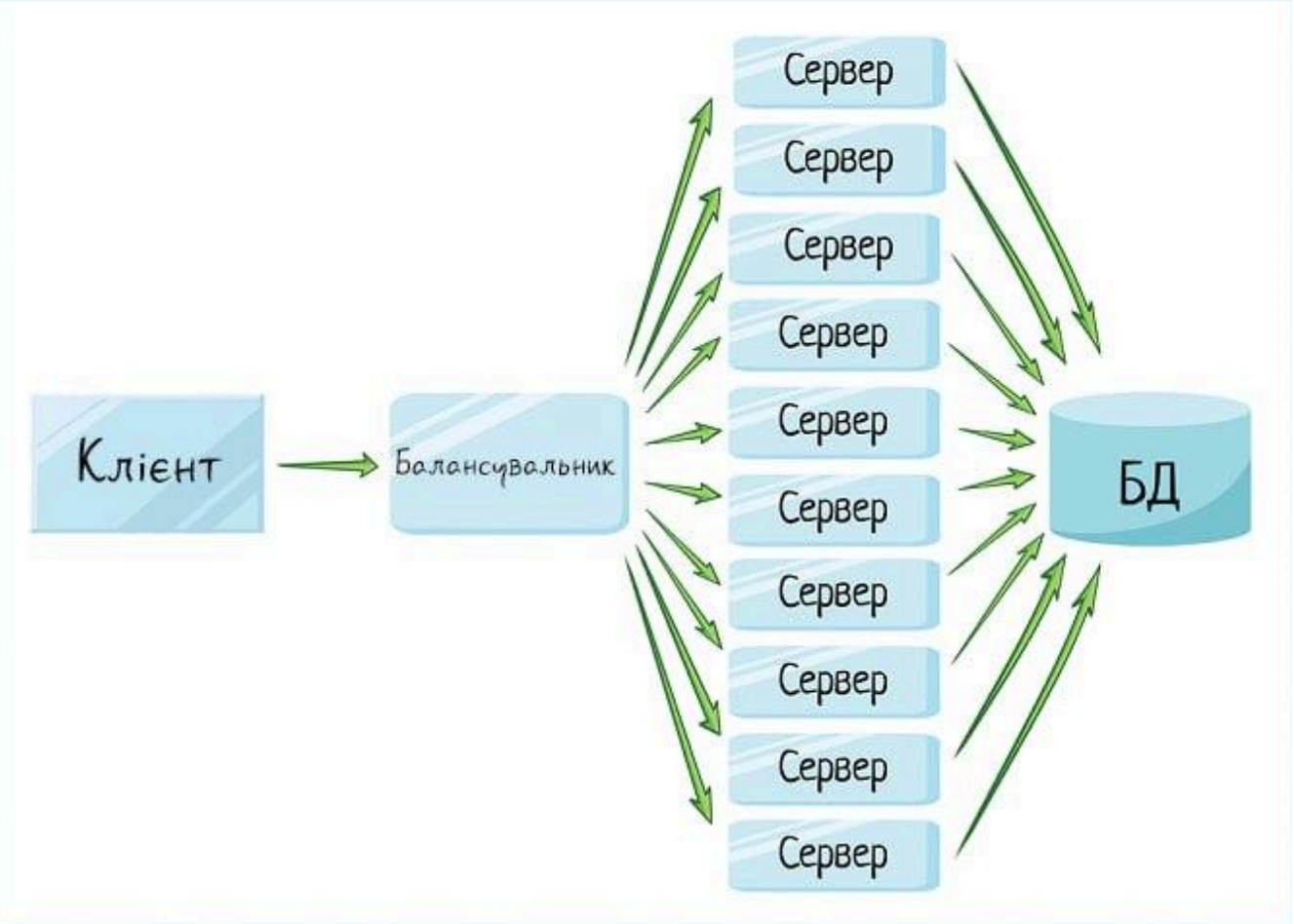


Рисунок 5.4.3 - Кластер резервних серверів

5.5. Коливання напруги та відсутність електроживлення

До загальної схеми електромережі будинку, яку контролює реле разом з автоматичним перемикачем (changeover switch) було підключено додаткове джерело живлення у вигляді генератора [5].

Для того, щоб краще зрозуміти як працює автоматичне перемикання джерела живлення представлено схему її роботи, яка має декілька етапів:

1) Автоматичний перемикач завдяки сенсорам бачить, що електроживлення з міста було втрачено

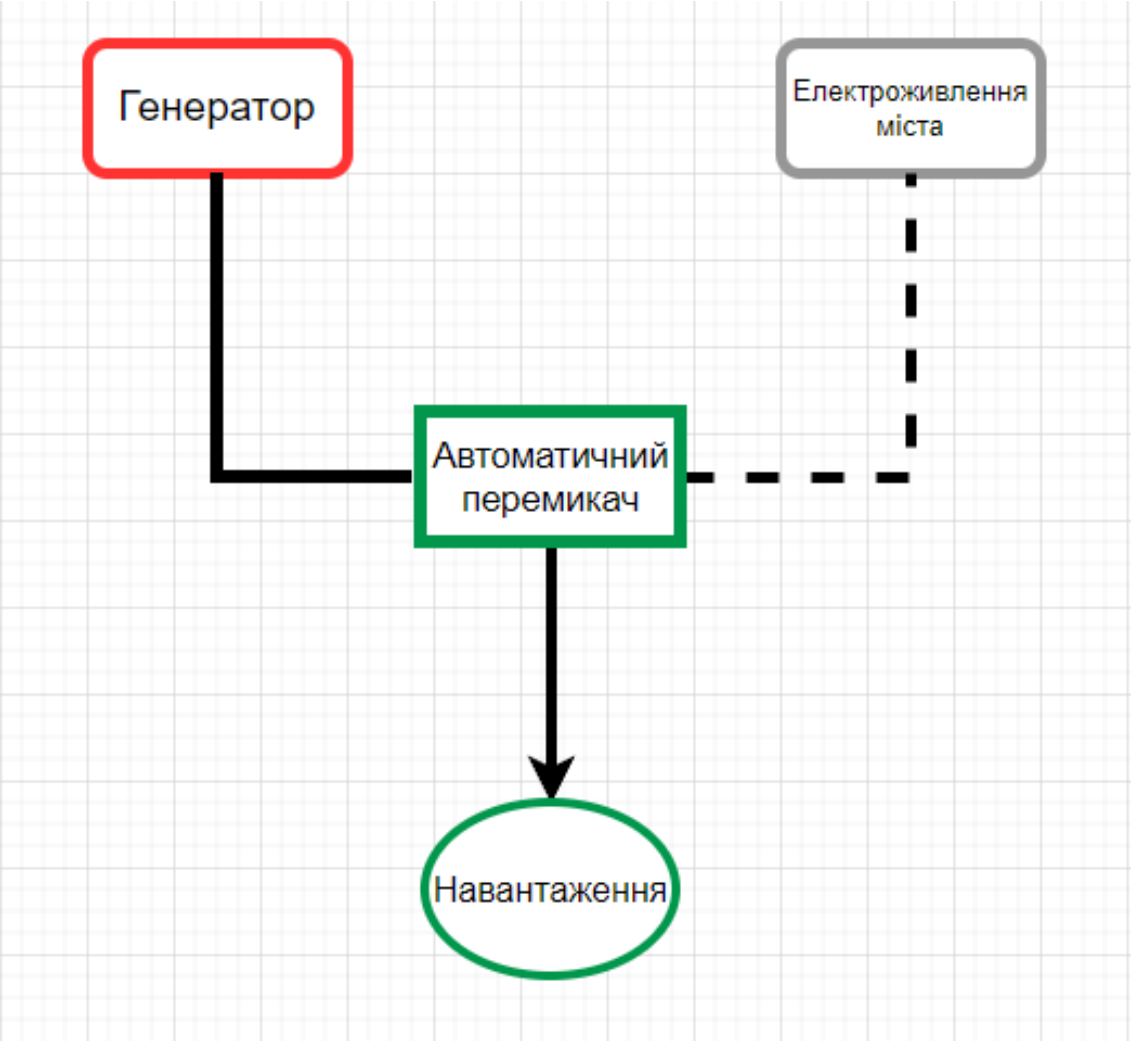


Рисунок 5.5.1 - Автоматичний перемикач бачить зміну в електромережі

Після того, як автоматичний перемикач виявляє збій живлення він автоматично дає команду на ввімкнення генератора.

Рисунок 5.5.2 - Автоматичний перемикач дає команду генератору на ввімкнення

Коли основна подача електроенергії відновлюється, автоматичний перемикач вимикає генератор.

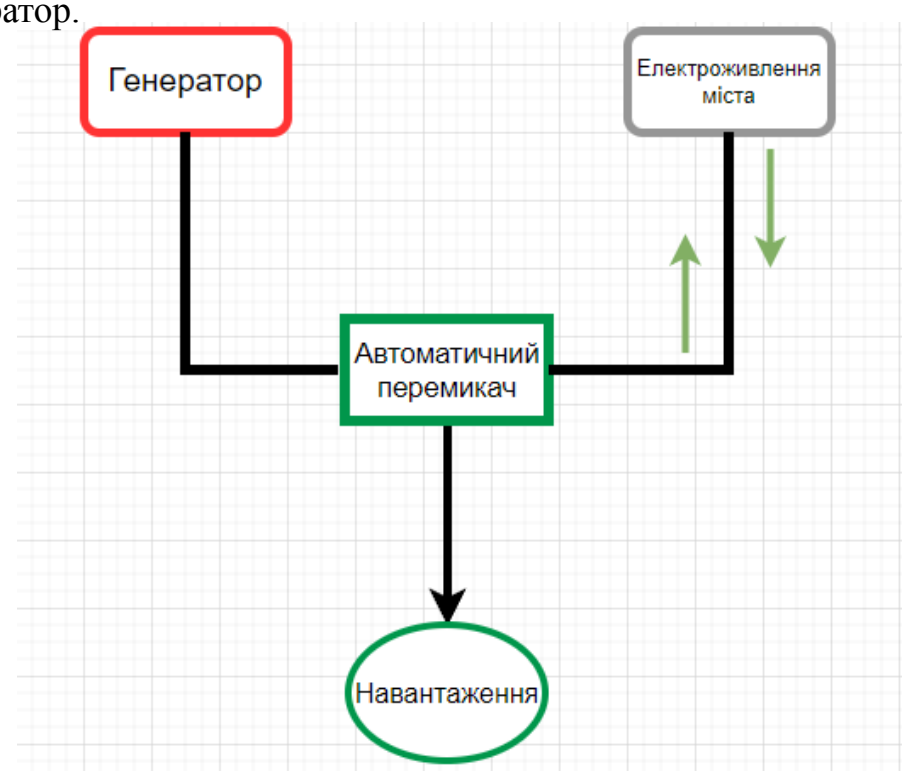


Рисунок 5.5.3 - Автоматичний перемикач відновлює з’єднання з містом

Щоб визначити якої потужності необхідний генератор підрахуємо приблизне споживання користувачами в мережі. Для цього, припустимо, що робота офісу становить 8 годин на день та загальна кількість кабінетів з звичайними офісними пк - 39. В кожному кабінеті по 2 комп’ютера та багатофункційний пристрій.

Обчислимо споживання комп’ютера разом із монітором у кіловат-годинах за 8 годин. Для цього, треба врахувати їх середню потужність:

1. Стаціонарний комп'ютер (залежить від конфігурації):

- середня потужність: 200–500 Вт (0.2–0.5 кВт).

2. Монітор (залежно від типу):

- LCD/LED-монітор: 20–50 Вт (0.02–0.05 кВт).

Підсумуємо потужність комп'ютера і монітора.
Наприклад: 300 Вт (комп'ютер) + 40 Вт (монітор) = 340 Вт (0.34 кВт).

Також, розрахуємо споживання БФП (багатофункціонального пристрою), враховуючи його режим роботи:

1. Режим очікування: БФП споживає приблизно 2–5 Вт.
2. Активний режим (друк): Споживання зростає до 300–500 Вт, але друк зазвичай займає незначний час. Зазначимо, що в офісі друкують активно.
1. Режим очікування:
   5 Вт × 7 год = 35 Вт\год = (0.035 кВт\год).
2. Активний друк:
   400 Вт×1 год = 400 Вт = (0.4 кВт\год)

Середнє споживання БФП:
БФП: 0.230 кВт/год

Загальне споживання за 8 годин:

- Комп'ютер з монітором: 0.340 кВт·год.
- БФП: 0.230 кВт·год.

Разом:

0.340 + 0.230 = 0.570 кВт\год

Враховуючи вище зазначені дані про споживання пристроїв, розрахуємо загальне середнє споживання енергії для 39 кабінетів, у кожному з яких є:

- 2 комп'ютери з моніторами.
- 1 лазерний БФП.

Вихідні дані:

- Середнє споживання одного комп'ютера з монітором:

0.340 кВт\год.

- Середнє споживання одного БФП:

0.230 кВт\год.

Розрахунок для одного кабінету:

- 2 комп'ютери з моніторами:

2×0.340 кВт\год = 0.68 кВт\год

- 1 БФП:

0.230 кВт\год.

Разом для одного кабінету:

0.68+0.23=0.91 кВт\год.

Розрахунок для 39 кабінетів:

- 0.91 кВт\год×39=35.49 кВт\год

Отже, 39 кабінетів із зазначеним обладнанням споживають в середньому 35.49 кВт·год.

Також, треба додати до загальних потреб серверну кімнату, конвертори з оптоволоконного інтернет з'єднання на виту пару, два обчислювальні сервери, FTP-сервер, два маршрутизатори, чотири комутатори, KVM - switch, Firewall, CCTV-сервер, сервер IP телефонії та база даних.

Щоб розрахувати одночасне споживання енергії зазначених пристроїв, потрібно оцінити середню потужність кожного типу обладнання. Нижче наведено орієнтовні значення потужності для кожного елемента:

Потужність обладнання:

1. **Конвертори з оптоволоконного інтернет-з'єднання на виту пару:**

- потужність одного конвертора: **5–10 Вт**.

- припустимо: 2 конвертори, середня потужність: 2×10=20 Вт.

2. **Обчислювальні сервери (1 + 1 резервний):**

- потужність: **400–600 Вт**.

- припустимо: 500 + 500 = 1000 Вт.

3. **Маршрутизатори (1 + 1 резервний):**

- потужність одного маршрутизатора: **60–100 Вт**.

- припустимо: 2 × 80=160 Вт.

4. **Комутатори (2 + 2 резервних):**

- потужність одного маршрутизатора: **100–250 Вт**.

- припустимо: 2 × 200=400 Вт.

5. **Firewall:**

- потужність: **100–200 Вт**.

- припустимо: 150 Вт.

6. **CCTV-сервер (сам сервер та камери):**

- потужність: **300–400 Вт**.

- припустимо: 350 Вт.

7. **Сервер IP-телефонії:**

- потужність: **250–350 Вт**.

- припустимо: 300 Вт.

8. **Сервер KVM-Switch:**

- потужність: 10-20 Вт.

- припустимо: 15 Вт.

9. **FTP сервер з RAID 6 (1 + 1 резервний):**

- RAID 6 додає до споживання звичайного сервера ще приблизно **10–20%** через обчислення паритету та використання додаткових дисків;

- потужність звичайного сервера: **400–500 Вт**;

- з урахуванням RAID 6: 500 Вт×1.2=600 * 2 = 1.2 кВт/год.

Отже, потреба тільки серверного обладнання:
20 + 1000 + 160 + 400 + 150 + 350 + 300 + 15 + 1200 = 3,595 кВт/год

Але ці розрахунки ще не остаточні, бо до потреби обладнання треба додати також систему прецизійного кондиціювання.

Для такої маленької серверної кімнати можна обрати системи прецизійного кондиціювання до 10 кВт, наприклад, Liebert CRV (10 кВт) [11].

Характеристики кондиціонера:

- потужність: **10 кВт**;

- середнє споживання (залежно від навантаження): **3–4 кВт** (орієнтовно **3.5 кВт**).

Рисунок 5.5.4 - прецизійний кондиціонер Liebert CRV

Отже, сума потреби всієї системи:

3.295 + 3.5 + 35.49 = 42.285 кВт/год.

Також треба зазначити, що обчислена потреба системи в приблизно 42 кВт/год може зменшуватись, так як балансувальник роботи сервера зменшує навантаження на систему та прецизійний кондиціонер може зменшувати свою потребу через адаптацію до зовнішніх умов, що зменшує споживання енергії та сприяє більшої енергоефективності системи. Також, через правильну температуру

та вологість в серверній кімнаті збільшується її енергоефективність - це виникає через те, що обчислювальні системи не втрачають свою ефективність через високі температури - скидаючи свої робочі частоти, та менше споживають енергії, бо споживання сервера може збільшитись до 50% через збільшення використання потужностей систем охолодження.

Дивлячись на потребу в приблизно 42 кВт/год, підбираємо необхідної потужності генератор, що може витримати таку потребу. Додатково, краще обирати генератори з запасом потужності, бо потребу вираховують за середнім споживанням, але бувають і випадки коли сумарна потреба вище через одночасну роботу пристроїв, що призводить до збільшення споживання.

Як впливає оптимізація.

Балансування навантаження: Передбачається зниження серверного навантаження на 20–30%.

Прецизійний кондиціонер: Зменшує споживання на 10–15% порівняно зі звичайним кондиціонером.

Розрахунок оптимізованого споживання:

Початкові дані:

Серверне обладнання:

Споживання до оптимізації: 3.595 кВт.

Прецизійний кондиціонер:

Споживання до оптимізації: 3.5 кВт.

Оптимізоване споживання:

1. **Серверне обладнання:**

   3.595×0.8=2.876 кВт

2. **Прецизійний кондиціонер:**

   3.5×0.9=3.15 кВт

3. **Загальне оптимізоване споживання серверної кімнати:**

   2.876+3.15=6.026 кВт

Споживання дизеля після оптимізації серверної:

За годину: 6.026 × 0.3 = 1.8078 л/год

За 8 годин: 1.8078 × 8 = 14.4624 л

Порівняння до і після оптимізації серверної:

До оптимізації:

За годину: 3.595 + 3.5 = 7.095 кВт

Споживання дизеля: 7.095 × 0.3 = 2.1285 л/год

За 8 годин: 2.1285 × 8 = 17.028 л.

Після оптимізації:

За годину: 6.026 кВт.

Споживання дизеля: 1.8078 л/год.

За 8 годин: 14.4624 л.

Економія за 8 годин: 17.028 − 14.4624 = 2.5656 л

Для даного випадку, коли споживання сягає 42 кВт/год краще обрати генератор з автоматичним стартером, щоб він включався як було раніше описано в схемі і робочої потужності від 60 кВт/год мінімум для можливих перебільшень в потребі.

Рисунок 5.5.5 - Дизельний генератор з автоматичним запуском

Для автоматичної зміни джерела електроживлення можна використати автоматичний перемикач з таким з’єднанням:

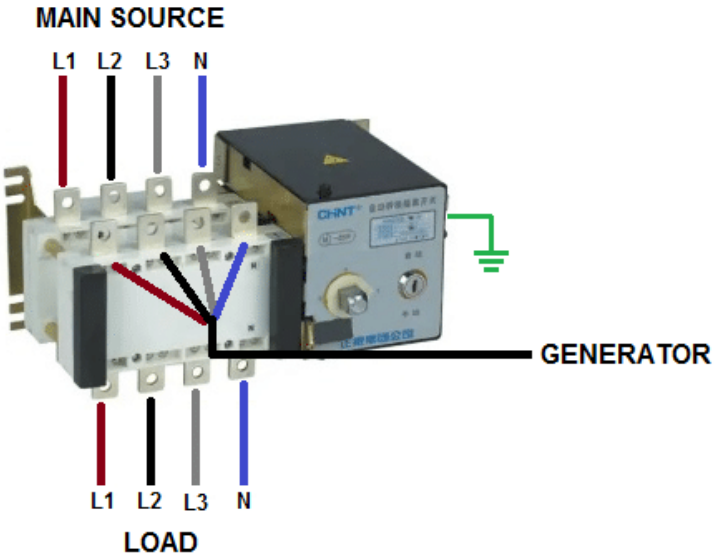


Рисунок 5.5.6 - Автоматичний перемикач

Далі, було додано джерело безперебійного живлення лінійно - інтерактивного типу з батареями великої ємності, яке з’єднано з реле до якого під’єднано online генератор і може заряджати батареї, дивлячись від джерела, від загальної мережі електропостачання або від додаткового джерела живлення, в нашому випадку - генератора.

У випадку, коли потрібне безперебійне постачання електроживлення до техніки, треба зазначити, що для офісних рішень треба використовувати визначені типи джерел безперебійного живлення, а саме лінійно-інтерактивні джерела безперебійного живлення або джерела безперебійного живлення з подвійним перетворенням, які ще називають online-безперебійниками.

Дані типи ДБЖ були вибрані через декілька причин. На даний момент, розповсюджені 3 типи джерел безперебійного живлення: ДБЖ резервного типу, лінійно-інтерактивні ДБЖ та ДБЖ з правильною синусоїдою.

До ДБЖ резервного типу, які ще називають offline ДБЖ, відносяться безперебійники, зазвичай, самі прості моделі. При відключені загальної мережі

безперебійник перемикається на аккумулятор, а коли напруга стає номінального значення, знову підключається до мережі міста [1]. Такий ДБЖ є дуже простим і не потребує технічного обслуговування, тому, має великі недоліки.

Перш за все це те, що такий тип ДБЖ не має у складі стабілізатора напруги, тому коли в мережі починає сильно просідати напруга, то він одразу перемикається на живлення від акумулятора. Проблема полягає в тому, що переключень може бути дуже багато за короткий проміжок часу через просадки напруги, відповідно, постійні перемикання призводять до швидкого зносу ДБЖ.

Крім цих чинників, ще є проблема в тому, що при перемиканні з загальної мережі на акумулятор і навпаки є невелика затримка в подачі напруги і деякі пристрої до цього не чутливі та продовжують працювати, інші, можуть бути дуже чутливими до затримки і в момент зміни мережі можуть вимикатись.

Рисунок 5.5.7 Схема ДБЖ резервного типу

Другий тип ДБЖ - це лінійно-інтерактивний ДБЖ, який і був обраний для даної системи. Він є найбільш розповсюдженим типом безперебійників і зазвичай використовується для побутової та офісної техніки. На відміну від ДБЖ резервного типу цей тип ДБЖ має вбудований стабілізатор напруги [1]. За допомогою цього стабілізатора лінійно-інтерактивний ДБЖ не лише надає резервне живлення, а також виробляє ідеальне значення напруги.

Слід зазначити, що в лінійно-інтерактивних ДБЖ є два типи сигналу: модифікована синусоїда та правильна синусоїда. Для безпеки та довговічності техніки яка підключена до ДБЖ треба використовувати ДБЖ з правильною синусоїдою, а не з модифікованою.

ДБЖ з модифікованою синусоїдою мають, зазвичай, меншу ціну, але пристрої, які будуть підключені до такого типу сигналу можуть перегріватися або виходити з ладу. Слід зазначити, що є техніка, яка може працювати з модифікованою синусоїдою, але таких пристроїв не багато. Тому, краще встановлювати лінійно-інтерактивні ДБЖ з правильною синусоїдою, що не шкодить техніці.

Незважаючи на переваги, лінійно-інтерактивні безперебійники не завжди можуть забезпечити ідеальну роботу підключених пристроїв. Наприклад, коли в електромережі є просідання чи перевищення напруги в проміжку, приблизно, 180-200 В. ДБЖ в такому випадку буде намагатись стабілізувати напругу, але коли це буде неможливо, тоді безперебійник буде перемикатися на аккумулятор і будуть такі ж часті перемикання, як і в ДБЖ резервного типу.

Слід зазначити, якщо напруга в електромережі не буде сильно змінюватися, як в представленій схемі, то цей ДБЖ підійде для будь-якої офісної техніки, але якщо в мережі є часті зміни напруги, або якщо є чутлива техніка до таких змін, наприклад в медицині, лабораторіях та серверних, як в нашому випадку.

Рисунок 5.5.8 - Схема ДБЖ лінійно інтерактивного типу

ДБЖ з подвійним перетворенням можуть похизуватись стабільною та ідеальною роботою навіть при найгірших показниках загальної мережі. Такого типу безперебійники використовують для роботи дорогих та точних пристроїв в медицині, серверних, телерадіомовленні та лабораторіях [1].

ДБЖ з подвійним перетворенням, або як їх ще називають - онлайн безперебійниками, влаштовані таким чином, що у них відсутні затримки при перемиканні із загальної мережі на акумулятор. Такий ідеальний результат досягається через те, що отримана з мережі електроенергія, відразу йде на акумулятор, а вже після акумулятора - подається на пристрій. Завдяки цьому, безперебійник такого типу весь час живить підключений пристрій одразу з акумулятора, не витрачаючи час на перемикання чи стабілізацію вхідної напруги.

Рисунок 5.5.9 - Схема ДБЖ з подвійним перетворенням

Отже, беручи до уваги вище приведені факти було обрано два типи ДБЖ для системи: ДБЖ лінійно інтерактивного типу для офісної техніки та ДБЖ з подвійним перетворенням для чутливої до подачі живлення техніки.

5.6. Людські фактори

Останнє, але, тимнеменш, важливе - це людський фактор. Людські помилки - одна з основних причин збоїв у роботі обчислювальних систем. Для їх мінімізації використовуються різні засоби:

1) Автоматизація. Чим більше операцій автоматизовано, тим менша ймовірність помилок, викликаних людським фактором. В розробленій системі майже все автоматизовано, від встановлення прецизійних кондиціонерів, що самостійно підтримують необхідну температуру та вологість для роботи обчислювальної системи до мережевого екрану, що обладнаний системою зі штучним інтелектом який самостійно реагує на можливі загрози та може вимикати клієнтські комп’ютери з мережі та повідомляти про це персонал;

2) Інструкції та тренінги. Персонал, що обслуговує обчислювальні системи, повинен регулярно проходити тренінги та бути ознайомлений з актуальними інструкціями щодо управління і відновлення систем у разі виникнення збоїв. Це дозволяє зменшити ймовірність помилок, пов'язаних з людським фактором, та забезпечити чітке реагування у випадку аварійних ситуацій.

Висновки

У ході виконання дипломної роботи було створено систему забезпечення високої автономності та відмовостійкості комп'ютерних систем підприємства та проведено всебічний аналіз методів і засобів забезпечення високої автономності й відмовостійкості. Поставлені завдання дозволили виявити сучасні підходи до покращення роботи обчислювальних систем у критичних умовах; розробити практичні рекомендації для забезпечення їхньої стабільності, надійності та оптимізації в умовах сьогодення України; побудувати модель архітектури приватного підприємства з високим рівнем автономності та відмовостійкості обчислювальних систем.

Забезпечення автономності та відмовостійкості - один із ключових аспектів для ефективного функціонування сучасних обчислювальних систем. Використання комплексного підходу до резервування та реплікації компонентів і даних дозволяє мінімізувати простої та забезпечити безперервну роботу навіть у разі відмови основних системних компонентів.

Методи резервування (апаратне і програмне) підтвердили свою ефективність для підвищення надійності обчислювальних систем. Сучасні методи, такі як RAID-масиви для збереження даних, резервні мережеві канали та кластеризація серверів, дозволяють забезпечити доступність обчислювальних ресурсів навіть у разі відмови окремих компонентів.

Моніторинг і системи виявлення збоїв є невід'ємною складовою сучасних систем відмовостійкості. Вони дають можливість оперативно реагувати на потенційні загрози та усувати збої на ранніх стадіях. Інтеграція технологій машинного навчання у системи моніторингу підвищує ефективність виявлення аномалій та збільшує стабільність роботи обчислювальних систем.

Захист від фізичних і технічних факторів досягається за допомогою спеціалізованих приміщень для серверів і систем безперебійного живлення. Використання таких засобів дозволяє мінімізувати вплив збоїв у живленні та інших зовнішніх загроз.

Протидія кіберзагрозам та захист від людського фактора вимагають комплексного підходу, який включає автоматизацію процесів, обмеження доступу, фаєрволи та антивірусні програми. Використання цих засобів підвищує загальний рівень безпеки обчислювальної системи, забезпечуючи захист даних та стабільність її роботи.

Комплексний підхід до захисту від динамічного середовища є найбільш ефективним для підвищення автономності обчислювальних систем. Комбінація технічних, апаратних та організаційних заходів допомагає створити стабільні та надійні системи, здатні працювати у важких умовах та забезпечувати безперервний доступ до інформації.

Загалом, результати дослідження демонструють, що інтеграція сучасних технологій моніторингу, резервування, автоматизації та захисту може значно підвищити відмовостійкість та автономність обчислювальних систем. Це дослідження є корисним для подальшого розвитку обчислювальних систем і надає рекомендації для підвищення їхньої стабільності у мінливих умовах сучасного технологічного середовища.

Електронні ресурси

1. Джерела безперебійного живлення [Електронний ресурс] – https://home-energy.com.ua/ibp/line-interactive-ibp/ (дата звернення: 11.10.2024)
2. Прецизійні кондиціонери [Електронний ресурс] – https://ventbazar.ua/uk/blog/pretsizionnye-konditsionery-printsip-raboty/ (дата звернення: 11.10.2024)
3. Супутникова система Starlink [Електронний ресурс] – https://www.starlink.com/ua (дата звернення: 11.10.2024)
4. Мережеві екрани та антивіруси [Електронний ресурс] – https://www.fortinet.com (дата звернення: 11.10.2024)
5. Автоматичні меремикачі енергоживлення [Електронний ресурс] – https://chintglobal.com/blog/changeover-switch/ (дата звернення: 15.10.2024)
6. Моніторинг система Nagios [Електронний ресурс] - https://idealsoft.com.ua/vendory/vendors-more/nagios/ (дата звернення: 15.10.2024)
7. Що таке гаряче резервування? [Електронний ресурс] - https://www.geeksforgeeks.org/what-is-hot-standby-mode/ (дата звернення: 16.10.2024)
8. Гаряче резервування протоколів роутера [Електронний ресурс] - https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html (дата звернення: 16.10.2024)
9. Основні переваги сертифікації ISO/IEC 27001 [Електронний ресурс] - https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001
10. Інсталяція Liebert CRD10 [Електронний ресурс] - https://www.vertiv.com/4adbed/globalassets/products/thermal-management/in-ro

w-cooling/liebert-crv-in-row-cooling-system-10-40kw/vertiv-liebert-crv-crd10-installation-manual-sl-71306-.pdf (дата звернення: 16.10.2024)

11. Робота системи RAID [Електронний ресурс] - https://www.geeksforgeeks.org/raid-redundant-arrays-of-independent-disks/ (дата звернення: 21.10.2024)
12. Балансувальник напруги від Amazon [Електронний ресурс] - https://aws.amazon.com/elasticloadbalancing/?nc1=h_ls (дата звернення: 21.10.2024)
13. Поняття віртуалізації [Електронний ресурс] - https://aws.amazon.com/what-is/virtualization/ (дата звернення: 23.10.2024)
14. Резервування в техніці [Електронний ресурс] - https://www.geeksforgeeks.org/redundancy-system-design/ (дата звернення: 23.10.2024)
15. Коливання напруги та її вплив [Електронний ресурс] - https://europan.ua/news/kolivannja-naprugi-ta-sposobi-zahistu/ (дата звернення: 23.10.2024)

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Магістерська робота

«Система забезпечення високої автономності та відмовостійкості обчислювальних систем»

Виконав: студент групи КСДМ-61 Бобков Роман Анатолійович

Керівник: завідувач кафедри КІ Лащевська Наталія Олександрівна

Київ - 2025

МЕТА, ОБ'ЄКТА ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета роботи: розробка системи забезпечення високої автономності та відмовостійкості обчислювальних систем

Об'єкт дослідження: процес забезпечення автономності та відмовостійкості обчислювальних систем у середовищах із зовнішніми впливами.

Предмет дослідження: методи та засоби забезпечення автономності та відмовостійкості обчислювальних систем, включаючи інноваційні технології, адаптивні алгоритми, моніторинг та резервування.

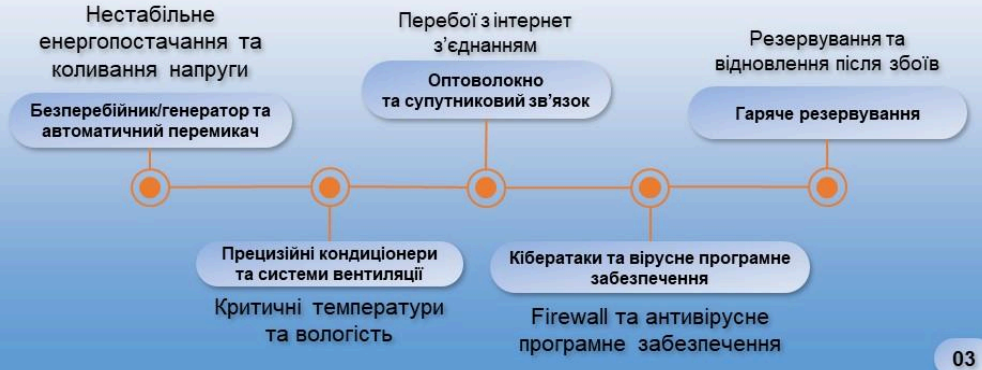
Для досягнення цієї мети необхідно вирішити такі завдання:

- Проаналізувати та впровадити методи підвищення автономності та відмовостійкості обчислювальних систем під впливом різних чинників;
- Оцінити ефективність запропонованих рішень на основі моделювання та експериментів.

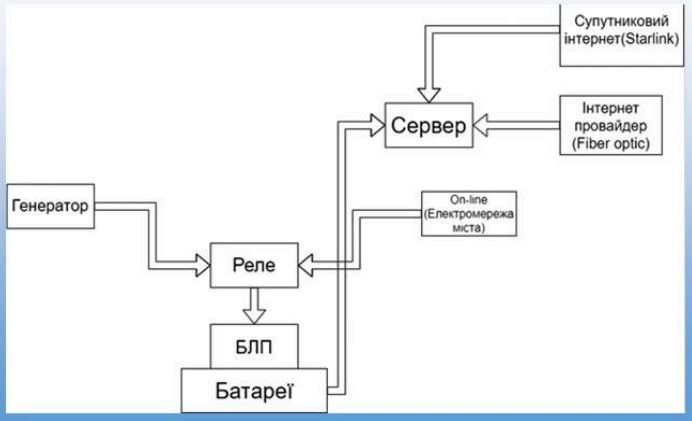
АКТУАЛЬНІСТЬ РОБОТИ

Ця робота є вкрай актуальною на теперешній час. Наявні системи забезпечення високої автономності та відмовостійкісті обчислювальних систем, які використовуються у критичних підприємствах або компаніях розраховані на епізодичні, не систематичні відмови, тому, я обрав дану тему для створення більш оптимізованої системи підвищеної автономності та відмовостійкості в умовах сьогодення України.

Елементи системи для підвищення відмовостійкості та автономності обчислювальних систем



Система забезпечення високої автономності та відмовостійкості обчислювальних систем



Нестабільне енергопостачання та коливання напруги

За умов нестабільного енергопостачання та коливання напруги необхідно застосувати наступні методи вирішення проблеми:

- До електромережі будинку, яку контролює реле разом з автоматичним перемикачем треба підключити генератор з функцією автоматичного ввімкнення;
- До реле підключити джерело безперебійного живлення з подвійним перетворенням, що буде на постійній основі давати електроживлення пристроям в серверній.

Рисунок 1 - Генератор

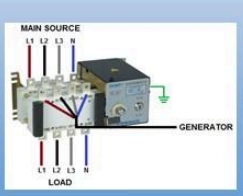


Рисунок 2 – Автоматичний перемикач

Рисунок 3 – ДБЖ з подвійним перетворенням

Аргументація вибору елементів для компенсування нестабільного енергопостачання та коливання напруги

Споживання енергії за годину

Категорія	Кількість	Споживання за годину (кВт)	Загальне споживання за годину (кВт)	Сумарне споживання за годину (кВт)
Офісні ПК (2 ПК на кабінет)	78	0.34	78×0.34=26.52	42.585
БФП (1 на кабінет)	39	0.23	39×0.23=8.97	
Серверне обладнання (конвертори, сервери, маршрутизатори, комутатори, Firewall, CCTV-сервер, сервер IP телефонії, KVM-Switch, FTP-сервер)	1 комплект	Конвертори: 2×0.01=0.022; Сервери: 2×0.5=1.02; Маршрутизатори: 2×0.08=0.16; Комутатори: 2×0.2=0.42; Firewall: 0.150; CCTV-сервер: 0.350; Сервер IP телефонії: 0.30; KVM-Switch: 0.015; FTP-сервер з RAID 6: 2×0.6=1.22	3.59	
Прецизійний кондиціонер	1	3.5	3.53	

Порівняльна таблиця типів ДБЖ

Параметр	ДБЖ резервного типу	Лінійно-інтерактивний ДБЖ	ДБЖ подвійного перетворення (з правильною синусоїдою)
Принцип роботи	Вмикається лише при відключенні основного живлення.	Забезпечує корекцію напруги за допомогою автотрансформатора.	Постійно працює у режимі подвійного перетворення: змінний струм — постійний — змінний.
Форма вихідного сигналу	Спрощена (квазі-синусоїда).	Модифікована синусоїда.	Ідеальна синусоїда.
Час перемикання	4–10 мс.	2–4 мс.	Відсутній (нульовий).
Корекція напруги	Відсутня.	Присутня, обмежена діапазоном.	Повна стабілізація напруги.
Ефективність роботи	Висока (низьке енергоспоживання)	Середня.	Нижча через постійне перетворення.
Рівень захисту	Мінімальний, тільки від короткочасних перебоїв.	Середній: захист від перепадів напруги та короткочасних відключень.	Максимальний: захист від усіх видів перебоїв і високоточна стабілізація.
Область застосування	Домашні ПК, периферія.	Малі сервери, робочі станції, офіси.	Критично важливі системи: сервери, медичне обладнання, ЦОД.
Вартість	Низька.	Середня.	Висока.

Критичні температури та вологість

За умов критичних температур та вологості необхідно застосувати наступні методи вирішення проблеми:

- Встановлення серверного кондиціонера - прецизійного кондиціонера;
- Встановлення додаткової системи вентиляції.

Рисунок 4 – Принцип роботи прецизійного кондиціонера

Рисунок 5 – Взаємодія прецизійного кондиціонера з вентиляцією

Аргументація вибору елементів для компенсування критичних температур та вологості

Порівняльна таблиця звичайного кондиціонера та прецизійного		
Параметр	Звичайний кондиціонер	Прецизійний кондиціонер
Призначення	Охолодження приміщень, де перебувають люди	Охолодження серверних кімнат та обладнання
Точність контролю	±2–3°C для температури, ±10% для вологості	±0.5°C для температури, ±5% для вологості
Режим роботи	Циклічний (вмикається та вимикається залежно від потреб)	Постійний, з адаптацією до змін теплового навантаження
Енергоспоживання	Нижче в умовах нерегулярного навантаження	Вище через постійне функціонування
Надійність	Обмежена при постійній роботі	Висока, призначений для безперервної роботи
Розподіл повітря	Не враховує гарячі/холодні зони	Оптимізоване для розподілу повітря в гарячих/холодних зонах
Тривалість служби	Коротша при використанні в серверних кімнатах	Довша, розроблений для роботи в критичних умовах
Вартість обладнання	Низька	Висока
Вартість обслуговування	Низька	Вища через складну конструкцію
Приклади використання	Офіси, житлові приміщення	Серверні кімнати, центри обробки даних

Резервування та відновлення після збоїв

За умов збоїв в роботі сервера та можливого максимально швидкого повернення до роботи слід використовувати:

- Технологію RAID 6 для організації накопичувачів;
- Використання гарячого або холодного резервування.

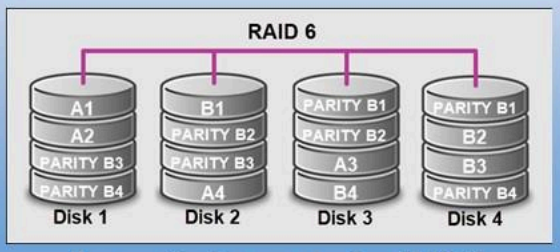


Рисунок 6 – Приклад роботи RAID 6

Рисунок 7 – Приклад роботи балансувальника

Аналіз впливу резервування

Переваги та недоліки рівнів RAID				
RAID рівень	Відмовостійкість	Продуктивність	Обсяг пам'яті	Недоліки
RAID 0	Відсутня	Максимальна	100%	Втрата даних при відмові одного диска
RAID 1	Висока	Висока	50%	Використовується лише половина загального обсягу
RAID 5	Середня (1 диск)	Середня	67–80%	Зниження швидкості запису через обчислення паритету
RAID 6	Висока (2 диски)	Середня	50–70%	Складна реалізація
RAID 10	Дуже висока	Висока	50%	Мінімальна кількість дисків: 4
RAID 50	Висока	Вища, ніж RAID 5	67–80%	Потребує багато дисків для реалізації
RAID 60	Дуже висока	Висока	50–70%	Складність у налаштуванні та висока вартість

Порівняння гарячого та холодного резервування		
Параметр	Гаряче резервування	Холодне резервування
Час відновлення	Миттєвий (< 1 сек)	Від кількох хвилин
Синхронізація даних	Постійна, у реальному часі	Не потрібна
Вартість	Висока	Низька
Використання ресурсів	Постійно використовується	Використовується при відмові
Складність реалізації	Висока	Низька

Кібератаки та вірусне програмне забезпечення

За умов кібератак та вірусних программ необхідно застосувати :

- Потрібно встановити міжмережевий екран (checkpoint) з ШІ,
- Всім клієнтам обчислювальної системи встановити антивірусне програмне забезпечення яке підключається та контролюється сервером.

Рисунок 8 – Fortinet 901G

Рисунок 9 – Fortinet GUI

Переваги міжмережевих екранів (checkpoint)

Критерій	Check Point	Звичайний фаєрвол
Призначення	Корпоративне рішення для захисту великих мереж	Базовий захист окремих пристроїв або невеликих мереж
Функціонал	Розширений: IDS/IPS, VPN, NAT, антишпіон, фільтрація додатків, DLP, і т.д.	Обмежений: зазвичай лише фільтрація портів та IP-адрес
Гнучкість налаштувань	Дуже висока, з можливістю створення складних політик	Мінімальна або середня, залежно від продукту
Масштабованість	Легко масштабується для великих організацій	Обмежена потужністю пристрою чи ОС
Інтеграція	Підтримка інтеграції з SIEM, IAM, іншими рішеннями	Зазвичай ізольований, без інтеграції
Інтерфейс користувача	Зручний веб-інтерфейс або GUI, централізоване управління	Базовий, часто CLI або простий GUI
Аналітика і звіти	Розширені аналітичні інструменти та журналювання	Обмежене логування, без деталізованих звітів
Підтримка ШІ	ШІ, яке самостійно реагує на небезпеку та навчається	Відсутня
Ціна	Висока, через комплексний функціонал та підтримку	Зазвичай безкоштовний або дешевий
Оновлення та захист	Часті оновлення баз загроз і патчів	Рідкісні або залежні від сторонніх виробників
Рівень безпеки	Високий: захист від сучасних загроз, включаючи Zero-Day атаки	Середній: базовий рівень безпеки
Тип користувачів	Підприємства, корпорації, держструктури	Домашні користувачі, малі підприємства

Перебої з інтернет з'єднанням

За умов перебоїв з інтернет з'єднанням необхідно застосувати наступні методи вирішення проблеми:

- Резервне джерело інтернет зв'язку, що не залежить від електроживлення - оптоволокно;
- Підключення супутникового зв'язку, як аварійне підключення інтернет мережі.

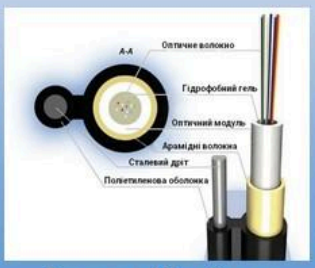


Рисунок 10 – Склад Оптичного волокна

Рисунок 11 – Starlink

Порівняння інтернет з’єднання

Критерій	Вита пара	Оптоволоконний кабель	Супутниковий зв'язок
Принцип роботи	Передача даних через електричні сигнали	Передача даних через світлові імпульси	Передача даних через радіохвилі на великі відстані
Пропускна здатність	До 10 Гбіт/с (Cat 6a і вище)	До 400 Гбіт/с і вище	До 100 Мбіт/с (залежить від провайдера)
Максимальна відстань передачі	До 100 м (без підсилювача)	До 80 км (без ретрансляторів)	Тисячі кілометрів (через супутник)
Затримки (латентність)	Низька (<1 мс у локальній мережі)	Дуже низька	Висока (400–600 мс) через відстань до супутника
Стійкість до перешкод	Середня (чутливий до електромагнітних завад)	Висока (нечутливий до електромагнітних завад)	Середня (вразливий до погодних умов)
Вартість прокладання	Низька	Висока (через дорогі матеріали та обладнання)	Висока (обладнання + підписка)
Надійність	Середня (вразливий до механічних пошкоджень)	Висока (захищений, але важче ремонтувати)	Середня (залежить від погодних умов і лінії зору)
Область використання	Локальні мережі (LAN), офіси, будинки	Магістральні лінії, дата-центри, швидкісні мережі	Віддалені регіони, морські судна, авіація
Переваги	Дешевий, простий у монтажі, поширений	Дуже висока швидкість і надійність	Глобальне покриття, незалежність від кабельних мереж
Недоліки	Обмежена відстань і чутливість до перешкод	Висока ціна, складність прокладання	Висока латентність, залежність від погодних умов
Типи пристроїв	Ethernet, комп'ютери, маршрутизатори	Мережеві магістралі, провайдери, сервери	Супутники, антени, термінали

Вплив оптимізації на систему

Початкові дані:

Серверне обладнання: 3.595 кВт\год.

Прецизійний кондиціонер: 3.5 кВт\год.

Оптимізоване споживання:

Серверне обладнання: 3.595×0.8=2.876 кВт

Прецизійний кондиціонер: 3.5×0.9=3.15 кВт

Загальне оптимізоване споживання серверної кімнати: 2.876+3.15=6.026 кВт

Споживання дизеля після оптимізації серверної:

- За годину: 6.026 × 0.3 = 1.8078 л/год
- За 8 годин: 1.8078 × 8 = 14.4624 л

Загальне споживання після оптимізації серверної:

- За годину: 7.095 – 6.026 = 1.069 кВт\год

Споживання дизеля:

- За годину: 2.1285-1.8078 = 0.3207 л
- За 8 годин: 17.028 − 14.4624 = 2.5656 л

Висновки

- Система з додаткового джерела живлення для офісу (дизельний генератор), лінійно-інтерактивних ДБЖ, ДБЖ з подвійним перетворенням та прецизійний кондиціонер будуть створювати «бар'єр» від зовнішніх умов;
- Балансувальник навантаження серверів та прецизійний кондиціонер зменшують споживання та збільшують продуктивність серверної кімнати через зменшення одночасного навантаження та простоїв обчислювальної системи через запити від користувачів;
- Міжмережевий екран (check point), який включає в собі велику кількість функцій та навчається в реальному часі виявляти внутрішні та зовнішні загрози завдяки штучному інтелекту та має систему моніторингу за комп'ютерами користувачів;
- Інтернет з'єднання офісу також не буде перериватися через відключення світла чи можливі електромагнітні перешкоди та має аварійний тип з'єднання – супутниковий зв'язок.
- Даний комплексний підхід дозволив зменшити споживання сервера на 1 кВт\год та споживання дизеля генератором на 0.3 л\год або 2.57 л. за 8 годин через зменшення одночасного споживання користувачами енергії та балансування навантаження серверу.

Загалом, результати дослідження демонструють, що інтеграція сучасних технологій моніторингу, резервування, автоматизації та захисту може значно підвищити відмовостійкість та автономність обчислювальних систем. Це дослідження є корисним для подальшого розвитку обчислювальних систем і надає рекомендації для підвищення їхньої стабільності у мінливих умовах сучасного технологічного середовища.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Магістерська робота

«Система забезпечення високої автономності та відмовостійкості обчислювальних систем»

Виконав: студент групи КСДМ-61 Бобков Роман Анатолійович

Керівник: к.т.н., доцент кафедри КІ Лащевська Наталія Олександрівна

Київ - 2025