МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

НАДІЙНІСТЬ КОМП'ЮТЕРНИХ СИСТЕМ

Методичні вказівки
для здобувачів першого (бакалаврського) рівня
вищої освіти за спеціальностями
123 «Комп'ютерна інженерія» та 125 «Кібербезпека»

Київ 2024

УДК 004.942
Н17

Укладач Д.О. Гуменний, канд. техн. наук, доцент

Рецензент О.В. Чкалов, канд. техн. наук, доцент кафедри САП Національного університету «Львівська політехніка».

Відповідальний за випуск Ю.І. Хлапонін д-р техн. наук, професор

Затверджено на засіданні кафедри кібербезпеки та комп'ютерної інженерії, протокол № 1 від 29 серпня 2024 року.

Видається в авторській редакції.

Надійність комп'ютерних систем [Електронний ресурс] : методичні
Н17 вказівки / уклад. Гуменний Д. О. – Київ : КНУБА, 2024. – 52 с.

Наведено стислий зміст курсу «Надійність комп'ютерних систем» та податі теми розрахунково-графічних робіт.

Призначено для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальностями 123 «Комп'ютерна інженерія» та 125 «Кібербезпека».

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Курс «Надійність комп'ютерних систем» охоплює широкий спектр питань, включаючи методи аналізу надійності, оцінку ризиків, методи зменшення ризику, а також побудову надійних і відмовостійких систем з використанням сучасних технологій та інструментів.

Метою курсу є підготовка студентів до вирішення складних завдань у галузі інформаційних технологій, де відмовостійкість і надійність систем відіграють критичну роль. Приділяючи увагу ключовим аспектам побудови надійних систем, ці методичні рекомендації забезпечують фундаментальні знання, необхідні для проєктування і впровадження систем, які здатні функціонувати безперебійно навіть у випадку виникнення критичних ситуацій.

Рекомендації містять структурований виклад основних тем курсу, розділи з прикладами практичного застосування методів, що розглядаються, а також рекомендації щодо виконання розрахунково-графічної роботи (РГР). Розрахунково-графічна робота є важливою складовою курсу, яка дає змогу студентам застосувати на практиці знання, отримані під час лекцій та самостійного вивчення матеріалу. Виконання РГР сприяє глибшому розумінню теоретичних аспектів і дає змогу студентам продемонструвати свої навички у реальних умовах.

Окрім теоретичного матеріалу, методичні рекомендації містять також опис сучасних методів і інструментів, що використовуються для оцінки та забезпечення надійності систем. Це охоплює аналіз видів і наслідків відмов (FMEA), аналіз дерев відмов (FTA), HARA (Hazard and Risk Analysis) та інші методи, які є стандартними в індустрії для побудови критично важливих систем.

Важливим аспектом курсу є розгляд питань, пов'язаних із функціональною безпекою (Functional Safety), яка є невід'ємною частиною розробки суперкритичних систем, таких як авіаційні системи управління польотом, атомні електростанції, медичні пристрої та інші системи, де відмова може мати катастрофічні наслідки. Студенти дізнаються про стандарти, що регулюють ці галузі, а також про методи, які використовуються для досягнення необхідного рівня надійності і безпеки.

Особливо слід відзначити, що ці методичні рекомендації базуються на практичних навичках, які укладач здобув, працюючи на позиціях Senior Software Engineer та Engineering Manager у компаніях GlobalLogic та N-iX.

Досвід, отриманий під час виконання реальних проєктів у цих компаніях, став основою для створення цього матеріалу, що робить його особливо цінним для підготовки майбутніх фахівців.

Загалом, ці методичні рекомендації надають студентам комплексне розуміння процесів забезпечення надійності та безпеки комп'ютерних систем, що дасть змогу їм застосовувати отримані знання у майбутній професійній діяльності. Успішне засвоєння матеріалу курсу допоможе студентам стати висококваліфікованими фахівцями, здатними ефективно вирішувати задачі з проєктування, аналізу та експлуатації надійних систем у різних галузях.

КОРОТНИЙ ЗМІСТ КУРСУ

Текст цього розділу ні в якому разі не є конспектом лекцій чи матеріалом, що може їх замінити. Також він не замінює самі лекції. Це швидше коротка витримка матеріалу, яка служить довідковим ресурсом для орієнтації в курсі та виконання розрахунково-графічної роботи. Студенти повинні використовувати цей розділ як допоміжний інструмент, але основну увагу слід приділяти активній участі в лекціях і самостійному опрацюванню повного обсягу матеріалу.

ПРОВЕДЕННЯ HARA (HAZARD AND RISK ANALYSIS)

Основи HARA

Hazard and Risk Analysis (HARA) – це систематичний процес, що використовується для виявлення потенційних небезпек, пов'язаних з роботою комп'ютерних систем, і оцінки ризиків, які ці небезпеки можуть викликати. HARA є основою для розробки ефективних стратегій управління ризиками, оскільки дозволяє розробникам і аналітикам зрозуміти, які аспекти системи потребують особливої уваги і які заходи слід вжити для мінімізації можливих негативних наслідків.

Методологія проведення HARA

Процес проведення HARA складається з кількох етапів:

1. **Ідентифікація небезпек.** На першому етапі аналізуються всі можливі ситуації, які можуть призвести до небажаних подій або збоїв у роботі системи. Цей етап включає детальне вивчення архітектури системи, її компонентів та взаємодії між ними.

Приклад. *Для автомобільної системи керування двигуном небезпекою може бути відмова датчика положення дросельної заслінки, що призведе до неконтрольованого прискорення.*

2. **Оцінка ймовірності виникнення небезпек.** Після ідентифікації небезпек необхідно оцінити ймовірність їх виникнення. Для цього використовуються історичні дані, статистичні моделі або експертні оцінки. Важливо враховувати всі можливі фактори, які можуть вплинути на ймовірність виникнення небезпеки.

Приклад. *У системі зберігання даних можна оцінити ймовірність збою жорсткого диска на основі статистики виробника.*

3. **Оцінка значущості наслідків.** Визначення значущості наслідків передбачає аналіз потенційних наслідків для системи або користувачів у разі реалізації небезпеки. Цей етап є критичним для розуміння того, наскільки значною є небезпека і які заходи слід вжити для її мінімізації.

Приклад. *У банківській системі збій бази даних може призвести до втрати критично важливої інформації, що має високу значущість для компанії та клієнтів.*

4. **Розрахунок рівня ризику.** Рівень ризику визначається як функція ймовірності виникнення небезпеки та значущість її наслідків. Це допомагає ранжувати ризики за ступенем їх критичності і визначати пріоритетність дій для їх зменшення.

Приклад. *У медицинській системі автоматичного введення ліків ризик неправильної дози оцінюється на основі ймовірності відмови дозатора і значні наслідків для пацієнта.*

5. **Розробка та впровадження заходів щодо зниження ризику.** На цьому етапі розробляються і впроваджуються заходи, спрямовані на зменшення або усунення ризиків. Це може включати технічні рішення, зміни в процесах, додаткове навчання персоналу або оновлення політик безпеки.

Приклад. *У системі авіаційного управління може бути впроваджено додаткове резервування критичних компонентів для зменшення ризику відмов.*

Таблиця 1

Базове подання HARA

Небезпека	**Важкість (S)**	**Частота (E)**	**Керованість (C)**	**Рівень ризику (S*E*C)**
Втрата контролю керування	Висока	Середня	Низька	Середній
Відмова гальмівної системи	Дуже висока	Висока	Низька	Високий
Непередбачуване прискорення	Висока	Низька	Середня	Середній

Приклади і підходи побудови HARA

Розглянемо декілька варіантів підходів до проведення HARA:

Функціональний підхід. Орієнтований на аналіз конкретних функцій системи і виявлення небезпек, пов'язаних із виконанням цих функцій.

Приклад. *Аналіз функції керування доступом у системі безпеки банку.*

Компонентний підхід. Зосереджений на аналізі окремих компонентів системи і визначенні ризиків, пов'язаних із відмовою або несправністю цих компонентів.

Приклад. *Аналіз жорсткого диска у сервері даних.*

Сценарний підхід. Включає аналіз можливих сценаріїв використання системи і визначення небезпек, які можуть виникнути в різних умовах експлуатації.

Приклад: *Аналіз роботи системи під час відмови живлення або збоїв у мережі.*

Важливі аспекти та посилання

Під час проведення HARA слід звертати увагу на такі аспекти:

- **Частота оновлення аналізу.** Регулярне оновлення HARA забезпечує актуальність аналізу з урахуванням нових даних, змін у системі та нових загроз.
- **Документування результатів**. Важливо вести детальний запис усіх етапів HARA, що дозволяє відслідковувати процес і приймати обґрунтовані рішення.
- **Посилання на стандарти.** У процесі проведення HARA слід звертатися до міжнародних стандартів, таких як ISO 26262 для автомобільних систем або IEC 61508 для функціональної безпеки.

МЕТОДИ РОЗРАХУНКУ НАДІЙНОСТІ

Вступ до розрахунку надійності

Надійність комп'ютерних систем – це характеристика, що відображає здатність системи виконувати свої функції без збоїв протягом визначеного часу. У контексті комп'ютерних систем, надійність включає в себе апаратну, програмну та мережеву складові. Для оцінки надійності системи застосовуються різноманітні методи, які базуються на математичних моделях, статистичному аналізі, а також історичних даних про роботу системи.

Основні поняття

MTBF (Mean Time Between Failures). Середній час між відмовами (MTBF) – це основний показник, що використовується для оцінки надійності системи. Він визначається як середній час роботи системи між послідовними відмовами.

Формула: MTBF = Σ (Час роботи між відмовами) / Кількість відмов.

***Приклад**. Якщо сервер працює 1000 годин до першої відмови і 1500 годин до другої, MTBF буде (1000 + 1500) / 2 = 1250 годин.*

MTTF (Mean Time To Failure). Середній час до відмови (MTTF) використовується для компонентів, які не ремонтуються після відмови. Це середній час роботи компонента до його остаточної відмови.

***Приклад.** Жорсткий диск, який не підлягає ремонту, може мати MTTF 20000 годин.*

MTTR (Mean Time To Repair). Середній час на відновлення (MTTR) – це середній час, необхідний для відновлення працездатності системи після відмови.

***Приклад.** Якщо на відновлення серверу після відмови йде 4 години, MTTR дорівнює 4 години.*

Надійність (R(t)). Надійність R(t) – це ймовірність того, що система буде працювати без відмов протягом часу t.

Формула: $R(t) = \exp(-\lambda t)$, де λ – інтенсивність відмов.

***Приклад.** Якщо $\lambda = 0.001$ год$^{-1}$, то ймовірність того, що система пропрацює 1000 годин без відмови, дорівнює $R(1000) = \exp(-0.001 * 1000) = \exp(-1) \approx 0.3679$.*

Методи розрахунку надійності

Експоненційний закон розподілу відмов. Один з найпоширеніших методів розрахунку надійності, що базується на припущенні, що ймовірність відмови системи у будь-який момент часу є постійною. Використовується для систем, де відмови мають незалежний характер.

Формула: $R(t) = \exp(-\lambda t)$.

Приклад. *Якщо інтенсивність відмови сервера дорівнює 0.0005 год$^{-1}$, то його ймовірність безвідмовної роботи протягом 2000 годин буде $R(2000) = \exp(-0.0005 * 2000) \approx 0.3679$.*

Нормальний розподіл. Використовується для моделювання надійності систем, де ймовірність відмови розподілена нормально. Це підходить для систем з прогнозованими відмовами, які мають піковий період відмов.

Формула: $R(t) = 1 - \Phi((t - \mu) / \sigma)$, де μ – середнє значення, σ – стандартне відхилення, Φ – функція розподілу нормального закону.

Приклад. *Для компонента з $\mu = 5000$ годин і $\sigma = 1000$ годин ймовірність роботи без відмови протягом 4000 годин буде $R(4000) = 1 - \Phi((4000 - 5000) / 1000) \approx 0.8413$.*

Логнормальний розподіл. Використовується для оцінки надійності систем, у яких час до відмови розподілений логнормально. Це часто застосовується для компонентів з нерівномірним зносом.

Формула: $R(t) = 1 - \Phi((\ln(t) - \mu) / \sigma)$, де μ – середнє значення логарифму часу до відмови, σ – стандартне відхилення логарифму часу.

Приклад. *Для компонента з $\mu = 8$ і $\sigma = 0.5$ ймовірність роботи без відмови протягом 1000 годин буде $R(1000) = 1 - \Phi((\ln(1000) - 8) / 0.5) \approx \approx 0.1587$.*

Метод дерев відмов (Fault Tree Analysis). Цей метод дає змогу моделювати складні системи шляхом розбиття їх на підсистеми та компоненти і аналізу ймовірності відмови кожної з підсистем.

Приклад. *Для системи, що складається з трьох незалежних підсистем з ймовірностями відмови 0.1, 0.2 і 0.3 відповідно, загальна ймовірність відмови буде обчислюватися як $1 - (1 - 0.1) * (1 - 0.2) * (1 - 0.3) \approx 0.488$.*

Приклади застосування методів на практиці

Прогнозування надійності серверної інфраструктури. Для великої дата-центру можна застосувати експоненційний закон розподілу відмов для оцінки надійності серверів та визначення потреби в резервуванні або удосконаленні архітектури.

Аналіз надійності мережевого обладнання. За допомогою методу дерев відмов можна визначити ймовірність збоїв у мережевій інфраструктурі, враховуючи ймовірності відмов окремих компонентів (маршрутизаторів, комутаторів, кабелів тощо).

Розрахунок надійності електронних компонентів у промислових системах. Використання логнормального розподілу для аналізу надійності електронних компонентів, які схильні до деградації з часом.

Посилання на стандарти та джерела

- IEC 61078: Стандарт для аналізу надійності і відмовостійкості систем за допомогою діаграм блоків надійності.
- MIL-HDBK-217F: Довідник з надійності електронних систем і компонентів, який надає методики розрахунку надійності для військових і промислових застосувань.
- ISO 26262: Стандарт для автомобільних систем, що охоплює методи аналізу надійності та відмовостійкості.

МЕТОДИ РОЗРАХУНКУ ВІДМОВОСТІЙКОСТІ

Вступ до відмовостійкості

Відмовостійкість – це здатність комп'ютерної системи або її компонентів продовжувати функціонувати коректно навіть у разі виникнення відмови одного або кількох її елементів. У контексті критичних систем, таких як авіаційні системи або медичні пристрої, відмовостійкість є вирішальним фактором для забезпечення безпеки та надійності. Для аналізу та забезпечення відмовостійкості використовуються спеціальні методи, які дозволяють оцінити ймовірність збереження працездатності системи після відмови одного або більше її компонентів.

Основні поняття

MTTFd (Mean Time to Dangerous Failure). Середній час до небезпечної відмови (MTTFd) – це показник, який використовується для оцінки часу до виникнення відмови, що може призвести до небезпечної ситуації. Він є критичним для оцінки відмовостійкості в системах, де безпека є пріоритетом.

Формула: $MTTFd = 1 / \lambda d$, де λd – інтенсивність небезпечних відмов.

***Приклад**. Для компонента з $\lambda d = 0.0001$ год$^{-1}$ MTTFd дорівнює 10000 годин.*

FIT (Failures In Time). FIT – це кількість відмов на мільярд годин роботи компонента. Цей показник широко використовується для оцінки надійності та відмовостійкості електронних компонентів.

Формула: $FIT = 1 / MTBF * 10^9$.

***Приклад.** Якщо MTBF компонента становить 100000 годин, то його $FIT = 1 / 100000 * 10^9 = 10000$ FIT.*

SFF (Safe Failure Fraction). Доля безпечних відмов (SFF) – це показник, який відображає відсоток відмов, що не призводять до небезпечних ситуацій. Він використовується для оцінки відмовостійкості в критичних системах.

Формула: $SFF = (\lambda s + \lambda d) / (\lambda s + \lambda d + \lambda u)$, де λs – інтенсивність безпечних відмов, λd – інтенсивність небезпечних відмов, λu – інтенсивність невиявлених відмов.

***Приклад.** Якщо $\lambda s = 0.001$, $\lambda d = 0.0005$, $\lambda u = 0.0002$, то $SFF = (0.001 + 0.0005) / (0.001 + 0.0005 + 0.0002) \approx 0.857$.*

Методи розрахунку відмовостійкості

Метод резервування (Redundancy). Резервування є одним із найпоширеніших підходів до забезпечення відмовостійкості. Воно полягає у використанні додаткових компонентів або систем, які дублюють функції основних, що дозволяє системі продовжувати роботу навіть у разі відмови основних компонентів.

Види резервування

- Холодне резервування: Резервний компонент активується тільки після відмови основного.
- Тепле резервування: Резервний компонент постійно підтримується у стані готовності і може швидко бути активованим.
- Гаряче резервування: Резервний компонент працює паралельно з основним і негайно заміняє його в разі відмови.

Приклад. *У серверній інфраструктурі може використовуватися гаряче резервування для забезпечення безперервності роботи бази даних.*

Діаграми блоків надійності (Reliability Block Diagrams, RBD). RBD – це графічний метод, який дозволяє моделювати і оцінювати відмовостійкість системи, розбиваючи її на окремі блоки (компоненти) і аналізуючи ймовірність збереження працездатності при відмові одного або більше блоків.

Приклад. *В автомобільній електроніці можна використовувати RBD для моделювання відмовостійкості системи керування двигуном, враховуючи резервування сенсорів і електронних блоків.*

Аналіз дерева відмов (Fault Tree Analysis, FTA). Метод FTA дає змогу моделювати можливі відмови системи і оцінювати їхній вплив на загальну працездатність. Цей метод корисний для виявлення вузьких місць у системі та розробки стратегій для підвищення відмовостійкості.

Приклад*. У системі управління потягом FTA може бути використаний для аналізу ймовірності відмови системи гальмування.*

Марковські моделі (Markov Models). Марковські моделі використовуються для моделювання систем з кількома станами, де ймовірність переходу між станами залежить від поточного стану. Це дає змогу оцінити ймовірність збереження працездатності системи після відмови певного компонента.

Приклад. *У телекомунікаційній системі Марковська модель може бути використана для моделювання відмовостійкості мережевих маршрутизаторів.*

Теорія мультиплексування (Multiplexing Theory). Цей метод передбачає використання кількох каналів або ліній зв'язку для передачі інформації, що дозволяє уникнути втрат даних у разі відмови одного з каналів.

Приклад*. У супутниковому зв'язку використовуються мультиплексовані канали для забезпечення відмовостійкості передачі даних.*

Приклади застосування методів на практиці

Резервування в авіаційних системах. Для авіаційних систем, таких як автопілот, застосовується гаряче резервування, що забезпечує негайний перехід на резервний автопілот у разі відмови основного.

Відмовостійкість серверних ферм. У дата-центрах широко застосовуються методи резервування на рівні серверів, дискових масивів і мережевих підключень для забезпечення безперервності роботи.

Забезпечення відмовостійкості у промислових системах автоматизації. Використання FTA дає змогу виявити критичні компоненти, відмова яких може призвести до зупинки виробничого процесу, і розробити стратегії резервування.

Посилання на стандарти та джерела

- IEC 61508: Стандарт для функціональної безпеки електричних, електронних і програмних систем, який охоплює методи оцінки відмовостійкості.
- MIL-HDBK-338B: Довідник з надійності та відмовостійкості військових систем.
- ISO 13849: Стандарт для забезпечення безпеки машин і устаткування, включаючи методи оцінки відмовостійкості.

МЕТОДИ ОЦІНКИ ЙМОВІРНОСТІ ВІДМОВИ ЧИ ЗБОЮ (І)

Вступ до оцінки ймовірності відмови

Оцінка ймовірності відмови або збою є одним з ключових аспектів забезпечення надійності та безпеки комп'ютерних систем. Цей процес дозволяє визначити ймовірність того, що система або її компоненти вийдуть з ладу протягом певного часу. Знання цієї ймовірності дозволяє інженерам і аналітикам розробляти більш надійні системи, передбачати можливі збої та вживати необхідних заходів для їх запобігання.

Основні поняття

Ймовірність відмови (Failure Probability, P(f)). Ймовірність відмови визначає ймовірність того, що система або компонент вийде з ладу протягом певного часу або при виконанні певної кількості операцій.

Формула: $P(f) = 1 - R(t)$, де $R(t)$ – надійність системи за час t.

Приклад. *Якщо надійність компонента протягом 1000 годин дорівнює 0.9, то ймовірність його відмови $P(f) = 1 - 0.9 = 0.1$.*

Інтенсивність відмов (Failure Rate, λ). Інтенсивність відмов характеризує кількість відмов, що очікуються на одиницю часу. Вона використовується для розрахунку ймовірності відмови за заданий період часу.

Формула: $\lambda = P(f) / t$.

Приклад. *Якщо ймовірність відмови системи за 500 годин дорівнює 0.02, то $\lambda = 0.02 / 500 = 0.00004$ год$^{-1}$.*

Ймовірність безвідмовної роботи (Reliability, R(t)). Ймовірність безвідмовної роботи визначає ймовірність того, що система або її компонент буде функціонувати без відмов протягом певного часу.

Формула: $R(t) = \exp(-\lambda t)$.

Приклад. *Якщо $\lambda = 0.001$ год$^{-1}$, то ймовірність того, що система буде працювати без відмови протягом 1000 годин, становить $R(1000) = \exp(-0.001 * 1000) \approx 0.3679$.*

Методи оцінки ймовірності відмови

Статистичний аналіз на основі історичних даних. Один з найбільш простих і широко використовуваних методів оцінки ймовірності

відмови – це аналіз історичних даних про відмови компонентів або систем. Цей метод дає змогу прогнозувати ймовірність відмов на основі статистики відмов за певний період часу.

***Приклад**. На основі даних про роботу серверів за останні 5 років можна визначити ймовірність відмови серверів протягом наступного року.*

Аналіз дерева відмов (Fault Tree Analysis, FTA). Метод FTA дає змогу моделювати можливі відмови системи та оцінювати їхню ймовірність. Відмови описуються у вигляді дерева, де кожна гілка представляє можливий шлях до відмови системи. Це дає змогу обчислити загальну ймовірність відмови на основі ймовірностей відмов окремих компонентів.

***Приклад.** Для складної мережевої системи можна побудувати дерево відмов, де ймовірність відмови кожного маршрутизатора або комутатора враховується у загальній оцінці.*

Байєсівські мережі (Bayesian Networks). Байєсівські мережі – це графічні моделі, які дають змогу оцінювати ймовірність відмови системи з урахуванням залежностей між її компонентами. Вони застосовуються для складних систем з високою кількістю взаємозалежних компонентів.

***Приклад.** У медичній системі моніторингу пацієнтів можна використовувати байєсівські мережі для оцінки ймовірності відмови системи на основі стану різних сенсорів і зв'язків між ними.*

Аналіз Марковських процесів (Markov Process Analysis). Марковські процеси використовуються для оцінки ймовірності відмови систем з різними станами, де ймовірність переходу між станами залежить від поточного стану системи. Цей метод дає можливість моделювати динаміку ймовірності відмови з урахуванням часу та стану системи.

***Приклад**. У системах з резервуванням Марковські процеси можуть використовуватися для оцінки ймовірності відмови основного і резервного компонентів залежно від їхнього поточного стану.*

Метод Монте-Карло (Monte Carlo Simulation). Метод Монте-Карло використовує випадкові вибірки та симуляції для оцінки ймовірності відмови. Він дозволяє моделювати різні сценарії роботи системи та оцінювати ймовірність відмови на основі великої кількості ітерацій.

***Приклад**. Для оцінки ймовірності відмови серверної ферми можна провести симуляцію роботи ферми під різними навантаженнями та умовами.*

Приклади застосування методів на практиці

Оцінка ймовірності відмови електронних компонентів у космічних системах. За допомогою методу Монте-Карло можна оцінити ймовірність відмови електронних компонентів на космічному апараті під впливом космічного випромінювання.

Оцінка надійності критичних медичних систем. Байєсівські мережі можуть бути використані для оцінки ймовірності відмови медичних систем моніторингу пацієнтів, де враховуються залежності між різними сенсорами і системами.

Оцінка ймовірності відмови мережевих систем у дата-центрі. Аналіз дерева відмов може бути застосований для моделювання й оцінки ймовірності відмови мережевої інфраструктури у великому дата-центрі.

Посилання на стандарти та джерела

- IEC 60812: Стандарт, що охоплює методи аналізу ймовірності відмови, включаючи FTA.
- MIL-HDBK-338B: Довідник, який містить методи розрахунку ймовірності відмови для військових систем.
- NASA Fault Tree Handbook: Керівництво з аналізу дерева відмов, що широко використовується у космічній галузі.

МЕТОДИ ОЦІНКИ ТЯЖКОСТІ ЗБОЮ (S)

Вступ до оцінки тяжкості збою

Тяжкість збою (Severity, S) – це міра, яка визначає вплив збою або відмови системи на її функціональність, безпеку, та кінцевих користувачів. Оцінка тяжкості збою є критичним етапом в аналізі надійності і ризиків, оскільки вона дозволяє визначити, наскільки значущі наслідки може мати збій для системи та її середовища. Цей параметр використовується для прийняття рішень щодо пріоритетності виправлення збоїв та впровадження заходів для зменшення ризиків.

Основні поняття

Тяжкість збою (Severity, S). Тяжкість збою відображає значущість наслідків збою для функціонування системи. Вона оцінюється за шкалою, яка визначає, наскільки критичною є відмова для різних аспектів роботи системи.

***Приклад**. У системі керування автомобілем, збій гальм може мати високу тяжкість (S = 10), оскільки він може призвести до аварії.*

Оцінка тяжкості у FMEA (Failure Modes and Effects Analysis). У методі FMEA тяжкість збою визначається як частина трьох факторів, що входять до розрахунку пріоритетного числа ризику (Risk Priority Number, RPN). Вона оцінюється за шкалою від 1 до 10, де 1 – мінімальний вплив, а 10 – максимально значущі наслідки.

***Приклад**. Якщо збій в елементі UI не впливає на критичну функціональність, тяжкість може бути оцінена як 2 або 3.*

Критичність збою. Критичність збою визначає, наскільки важливою є функція, яку впливає збій, і які наслідки це має для системи в цілому.

***Приклад**. Збій у системі контролю температури у серверній кімнаті може мати високу критичність, оскільки це може призвести до перегріву обладнання.*

Методи оцінки тяжкості збою

Шкалування на основі наслідків. Цей метод передбачає оцінку тяжкості збою за допомогою шкали, яка враховує наслідки для різних

аспектів роботи системи – безпеки, продуктивності, задоволення користувачів, фінансових втрат тощо.

Шкала оцінки:

- **1-3:** Незначний вплив, легко виправляється, не впливає на безпеку.
- **4-6**: Середній вплив, можливо потребує тимчасового припинення роботи, але не становить загрози для безпеки.
- **7-8:** Значний вплив, суттєво впливає на функціональність або продуктивність, може мати потенційні наслідки для безпеки.
- **9-10:** Критичний вплив, може призвести до значущої аварій або небезпеки для життя.

***Приклад**. Збій у системі подачі кисню у медичному обладнанні отримає оцінку 10 за шкалою тяжкості.*

Метод причинно-наслідкового аналізу. Включає аналіз можливих причин збоїв і оцінку їхнього впливу на різні функції системи. Це дає змогу визначити тяжкість наслідків для кожного типу збою.

***Приклад.** У разі відмови датчика швидкості в автомобілі, метод дозволить оцінити, як цей збій вплине на системи ABS та ESP.*

Аналіз небезпеки та операцій (HAZOP). HAZOP використовується для виявлення потенційних небезпек і аналізу наслідків відмов у складних системах. Цей метод допомагає оцінити тяжкість можливих збоїв шляхом систематичного аналізу різних сценаріїв роботи системи.

***Приклад**. У хімічному виробництві HAZOP може бути використаний для оцінки тяжкості збоїв у системі контролю процесу, що може призвести до викидів небезпечних речовин.*

Ієрархічний аналіз процесів (Process Hierarchy Analysis). Цей метод використовується для оцінки тяжкості збоїв шляхом аналізу впливу на ключові процеси системи. Оцінюється, як збій у конкретному компоненті або процесі вплине на загальну роботу системи.

***Приклад.** У банківській системі збій у процесі обробки транзакцій може мати значущі наслідки для обслуговування клієнтів і фінансових операцій.*

Приклади застосування методів на практиці

Оцінка тяжкості збоїв у авіоніці. Метод шкалування на основі наслідків використовується для оцінки тяжкості збоїв у авіоніці, де критичні збої можуть призвести до катастрофічних наслідків.

Аналіз збоїв у медичному обладнанні. HAZOP застосовується для оцінки тяжкості збоїв у медичних системах, де навіть незначний збій може мати значні наслідки для здоров'я пацієнтів.

Оцінка тяжкості відмов у промислових системах автоматизації. Причинно-наслідковий аналіз допомагає оцінити вплив відмов у системах управління виробничими процесами, що дозволяє запобігти зупинці виробництва і зниженню якості продукції.

Посилання на стандарти та джерела

- ISO 26262: Стандарт для автомобільних систем, що охоплює методи оцінки тяжкості збоїв у контексті функціональної безпеки.
- IEC 61508: Стандарт для функціональної безпеки, що включає методики оцінки тяжкості збоїв у промислових системах.
- MIL-STD-882E: Стандарт з системної безпеки, що використовується для оцінки тяжкості збоїв у військових системах.

МЕТОДИ ОЦІНКИ РИЗИКІВ

Вступ до оцінки ризиків

Оцінка ризиків – це процес ідентифікації, аналізу та оцінки потенційних небезпек, які можуть вплинути на функціонування комп'ютерної системи. Оцінка ризиків допомагає визначити можливі загрози, оцінити ймовірність їх реалізації та наслідки, що можуть виникнути у разі їхнього впливу на систему. Це важливий етап у забезпеченні надійності та безпеки систем, оскільки дозволяє розробникам і аналітикам приймати обґрунтовані рішення щодо запобіжних заходів та управління ризиками.

Основні поняття

Ризик (Risk, R). Ризик визначається як функція ймовірності виникнення небезпечної події та тяжкості її наслідків для системи. Він може бути оцінений за формулою:

Формула: R = P(f) * S, де P(f) – ймовірність відмови, S – тяжкість збою.

***Приклад**. Якщо ймовірність збою системи становить 0.01, а тяжкість наслідків оцінюється в 7 за шкалою від 1 до 10, ризик дорівнюватиме 0.07.*

Пріоритетне число ризику (Risk Priority Number, RPN). RPN – це показник, який використовується для оцінки ризику в FMEA (Failure Modes and Effects Analysis). Він обчислюється як добуток трьох показників: ймовірності виникнення збою, тяжкості наслідків та можливості виявлення збою.

Формула: RPN = O * S * D, де O – ймовірність виникнення, S – тяжкість збою, D – можливість виявлення збою.

***Приклад**. Якщо ймовірність виникнення збою дорівнює 5, тяжкість – 8, а можливість виявлення – 3, RPN = 5 * 8 * 3 = 120.*

Методи оцінки ризиків

Аналіз дерева відмов (Fault Tree Analysis, FTA). FTA – це метод графічного моделювання, що дозволяє визначити можливі причини відмови системи та оцінити ризики, пов'язані з цими відмовами. Дерево відмов

показує всі можливі шляхи до відмови системи та дозволяє оцінити ймовірність виникнення кожного сценарію.

Приклад. *У промисловій системі можна побудувати дерево відмов для оцінки ризиків збоїв у виробничому процесі, враховуючи можливі відмови обладнання та людські помилки.*

Аналіз видів та наслідків відмов (Failure Modes and Effects Analysis, FMEA). FMEA є одним з найпоширеніших методів оцінки ризиків, що дозволяє систематично виявляти можливі види відмов, аналізувати їхні наслідки та оцінювати ризики за допомогою пріоритетного числа ризику (RPN).

Приклад*. У автомобільній промисловості FMEA використовується для оцінки ризиків збоїв у різних компонентах автомобіля, таких як гальма, система керування двигуном тощо.*

Аналіз небезпек і експлуатаційних ризиків (Hazard and Operability Study, HAZOP). HAZOP – це метод, що використовується для виявлення потенційних небезпек та оцінки ризиків, пов'язаних з експлуатацією системи в різних умовах. Він передбачає аналіз сценаріїв роботи системи та оцінку можливих ризиків для кожного сценарію.

Приклад*. У хімічному виробництві HAZOP може бути використаний для оцінки ризиків при роботі з небезпечними речовинами, враховуючи можливі помилки оператора або збої обладнання.*

Аналіз критичності (Criticality Analysis). Аналіз критичності використовується для оцінки ризиків, пов'язаних з найбільш критичними компонентами системи. Він дозволяє виявити компоненти, відмова яких може мати найбільш значущі наслідки, і оцінити ризики, пов'язані з цими компонентами.

Приклад*. У системах управління повітряним рухом критичний аналіз може бути застосований для оцінки ризиків, пов'язаних з відмовою радарів або систем зв'язку.*

Байєсівські мережі (Bayesian Networks). Байєсівські мережі – це методи оцінки ризиків, що дозволяють моделювати ймовірності ризиків з урахуванням взаємозалежностей між компонентами системи. Вони використовуються для оцінки складних систем, де ризики можуть впливати один на одного.

Приклад*. У складних IT-системах, таких як центри обробки даних, байєсівські мережі можуть використовуватися для моделювання ризиків збоїв у мережевій інфраструктурі.*

Приклади застосування методів на практиці

Оцінка ризиків у авіаційних системах. FTA широко використовується в авіаційній галузі для оцінки ризиків збоїв у критичних системах літака, таких як системи навігації та управління польотом.

Оцінка ризиків у фармацевтичному виробництві. HAZOP може бути застосований для оцінки ризиків, пов'язаних із збоєм у виробництві лікарських препаратів, що може призвести до забруднення продукту або порушення процесу виробництва.

Оцінка ризиків у енергетичній галузі. Аналіз критичності використовується для оцінки ризиків збоїв у системах генерації та розподілу електроенергії, де відмова окремих компонентів може мати суттєві наслідки для енергопостачання.

Посилання на стандарти та джерела

- ISO 31000: Стандарт з управління ризиками, що охоплює принципи та рекомендації для оцінки ризиків.
- IEC 60812: Стандарт, що описує методи аналізу видів і наслідків відмов (FMEA).
- MIL-STD-1629A: Стандарт з аналізу видів і наслідків відмов для військових систем

МЕТОДИ ЗМЕНШЕННЯ РИЗИКУ

Вступ до зменшення ризику

Зменшення ризику – це процес впровадження заходів, які спрямовані на зниження ймовірності виникнення небажаних подій або зменшення їхнього впливу на систему. Цей процес є невід'ємною частиною управління ризиками, особливо в критичних системах, де відмови можуть мати значущі наслідки для безпеки, продуктивності та репутації організації. Методи зменшення ризику можуть включати як технічні рішення, так і організаційні заходи.

Основні поняття

Зменшення ймовірності ризику. Це підхід, який передбачає зниження ймовірності виникнення ризику за рахунок впровадження різноманітних заходів, таких як поліпшення якості компонентів, регулярне технічне обслуговування або навчання персоналу.

***Приклад**. Використання високоякісних компонентів у критичних системах, таких як авіоніка, зменшує ймовірність їхньої відмови.*

Зменшення впливу ризику. Зменшення впливу ризику означає зниження тяжкості наслідків у разі реалізації ризику. Це може бути досягнуто шляхом резервування, впровадження аварійних систем або оптимізації процесів реагування на відмови.

***Приклад**. Впровадження резервних систем живлення в дата-центрі дозволяє зменшити вплив відмови основного джерела живлення.*

Методи зменшення ризику

Резервування (Redundancy). Резервування передбачає використання додаткових компонентів або систем, які можуть взяти на себе функції основних у разі їх відмови. Існує кілька типів резервування: гаряче, тепле та холодне.

***Приклад**. У системах управління польотом літаків використовується гаряче резервування для забезпечення безперервної роботи у разі відмови основних систем.*

Фізичне та логічне розділення (Physical and Logical Separation). Розділення фізичних або логічних ресурсів дозволяє зменшити ризики,

пов'язані з відмовою одного компонента або системи. Наприклад, розподіл мережевих маршрутів або використання різних дата-центрів для зберігання даних.

***Приклад**. Використання різних серверних приміщень для зберігання резервних копій даних забезпечує захист від фізичних загроз, таких як пожежа або повінь.*

Контроль та моніторинг (Control and Monitoring). Регулярний контроль і моніторинг стану системи дозволяє своєчасно виявляти потенційні проблеми та запобігати їхньому переростанню в значні відмови. Це включає використання діагностичних інструментів, систем попереджень та автоматичних перевірок.

***Приклад**. Моніторинг температури у серверних приміщеннях та автоматичне включення додаткового охолодження при досягненні критичних значень.*

Розробка та впровадження аварійних планів (Emergency Planning and Response). Планування аварійних ситуацій та розробка процедур реагування дозволяють зменшити наслідки у разі виникнення надзвичайних подій. Аварійні плани включають дії з евакуації, перемикання на резервні системи, та відновлення роботи після аварій.

***Приклад**. У банківських системах створюються аварійні плани для перемикання операцій на резервні сервери у разі відмови основної системи.*

Резервування даних (Data Backup and Recovery). Регулярне резервування даних та наявність процедур їх відновлення дозволяють зменшити ризики втрати інформації через збої або кібератаки. Це може включати автоматизовані резервні копії, хмарні рішення або фізичні носії.

***Приклад**. У медичних системах регулярне резервування баз даних з інформацією про пацієнтів забезпечує захист від втрати даних у разі збоїв.*

Впровадження систем безперервної роботи (Continuous Operations Systems). Впровадження систем безперервної роботи дозволяє зменшити ризики, пов'язані з відмовами, забезпечуючи постійну готовність до відновлення функціональності. Це можуть бути рішення для забезпечення відмовостійкості та високої доступності.

***Приклад.** Використання кластерів серверів з автоматичним перемиканням на резервні ресурси у разі відмови одного з вузлів.*

Технічне обслуговування та оновлення (Maintenance and Upgrades). Регулярне технічне обслуговування та своєчасні оновлення системного програмного забезпечення та обладнання дозволяють зменшити

ризики, пов'язані з потенційними відмовами через зношування або застаріле ПЗ.

Приклад. *У автомобільних системах проводиться регулярна діагностика та заміна компонентів, що піддаються зношуванню, для зниження ризиків відмови на дорозі.*

Приклади застосування методів на практиці

Зменшення ризиків у енергетичних системах. Використання резервних генераторів та систем управління живленням у великих енергетичних компаніях дозволяє зменшити ризики, пов'язані з відмовами основних джерел енергії.

Зменшення ризиків у IT-інфраструктурі. Впровадження систем моніторингу та аварійного реагування в центрах обробки даних дозволяє мінімізувати час простою у разі відмови обладнання або мережевих збоїв.

Зменшення ризиків у медичних системах. Регулярне резервування медичних даних та наявність аварійних планів забезпечують безперервність медичних послуг у разі відмови систем або кібернападів.

Посилання на стандарти та джерела

- ISO 22301: Стандарт для систем управління безперервністю бізнесу, що охоплює методи зменшення ризиків.
- IEC 62443: Стандарт з кібербезпеки для промислових систем, який охоплює методи зменшення ризиків у контексті інформаційної безпеки.
- NIST SP 800-30: Керівництво з управління ризиками інформаційних технологій, що включає методи зменшення ризиків.

ІНСТРУМЕНТИ ЗМЕНШЕННЯ РИЗИКУ

Безкоштовні інструменти

OpenFTA. Інструмент для аналізу дерева відмов (FTA), використовується для моделювання сценаріїв збоїв і оцінки ризиків. Переваги: безкоштовний, відкритий код. Недоліки: обмежений функціонал, складний інтерфейс.

Scilab. Платформа для математичних розрахунків і симуляцій, альтернативна MATLAB. Переваги: відкритий код, гнучкість. Недоліки: обмежена підтримка специфічних моделей, потреба в налаштуванні.

Платні інструменти

Medini Analyze. Потужний інструмент для HARA, широко використовується в автомобільній та авіаційній промисловості. Переваги: широкий функціонал, підтримка стандартів. Недоліки: висока вартість, потреба в навчанні.

MATLAB/Simulink. Інструмент для математичних розрахунків і симуляцій, використовується для моделювання відмовостійкості. Переваги: потужний функціонал, інтеграція з іншими системами. Недоліки: висока вартість, складність освоєння.

ПОБУДОВА НАДІЙНИХ І ВІДМОВОСТІЙКИХ СИСТЕМ

Вступ до побудови надійних і відмовостійних систем

Надійність комп'ютеризованих систем є критичною характеристикою, особливо у сферах, де відмови можуть призвести до значущих наслідків, таких як авіація, автомобільна промисловість, медицина та енергетика. Побудова надійних систем вимагає комплексного підходу, який включає використання резервування, розподіленої архітектури, фізичного та логічного розділення, а також моніторингу та контролю.

Основні принципи побудови надійних і відмовостійких систем

Резервування. Резервування – це ключовий принцип, який дозволяє системам продовжувати роботу навіть у разі відмови окремих компонентів. Залежно від рівня критичності, резервування може бути:

- Гаряче резервування. Резервний компонент працює паралельно з основним і негайно активується у разі його відмови.
- Тепле резервування. Резервний компонент перебуває у стані готовності та активується із затримкою після відмови основного.
- Холодне резервування. Резервний компонент не активний і вмикається лише після відмови основного.

***Приклад**. У системах керування польотом літаків використовуються гарячі резерви для сенсорів і виконавчих механізмів, щоб забезпечити безперервну роботу навіть у разі відмови.*

Розподілена архітектура. Розподілена архітектура дозволяє мінімізувати вплив відмови одного компонента на загальну працездатність системи. Вона передбачає розподіл функцій між незалежними модулями, які можуть працювати автономно або у координації.

***Приклад**. У розподілених обчислювальних системах, таких як хмарні платформи, відмова одного сервера не впливає на загальну продуктивність завдяки розподілу навантаження між іншими серверами.*

Фізичне та логічне розділення. Фізичне та логічне розділення ресурсів мінімізує ризик одночасної відмови декількох компонентів.

Фізичне розділення означає використання окремих фізичних пристроїв, тоді як логічне – ізоляцію на рівні програмного забезпечення.

Приклад. *У банківських системах дані зберігаються у різних дата-центрах з фізичною та логічною ізоляцією, що забезпечує стійкість до регіональних збоїв або кібератак.*

Моніторинг і контроль. Постійний моніторинг і контроль стану системи дозволяють своєчасно виявляти відхилення від нормального функціонування та запобігати відмовам. Використання діагностичних інструментів та систем попередження є обов'язковим.

Приклад. *У промислових автоматизованих системах використовується моніторинг температури, вібрацій та інших параметрів для виявлення потенційних відмов обладнання до того, як вони стануть критичними.*

ПОБУДОВА СИСТЕМ ХОЛОДНОГО РЕЗЕРВУ

Вступ до систем холодного резерву

Системи холодного резерву є важливою частиною забезпечення надійності та безперервності роботи критичних комп'ютерних систем. Холодний резерв передбачає наявність резервних компонентів або обладнання, які залишаються неактивними до моменту відмови основної системи. Цей підхід є економічно вигідним та підходить для систем, де певна затримка у відновленні є прийнятною.

Основні поняття

Холодний резерв (Cold Standby). Холодний резерв означає, що резервний компонент або система не використовується до моменту відмови основної. Активація резерву відбувається після виявлення збою, що може призводити до затримки у відновленні.

Приклад. *У системах зберігання даних резервні сервери залишаються вимкненими до моменту відмови основного сервера.*

Активація на вимогу (On-Demand Activation). Резервний компонент активується лише після того, як основна система виходить з ладу. Це знижує витрати на підтримку, але може призвести до деякого часу простою під час активації.

Приклад*. У мережевих системах резервні маршрутизатори запускаються лише після відмови основного маршрутизатора.*

Планування відновлення (Recovery Planning). Планування відновлення є ключовим аспектом побудови систем холодного резерву. Це включає розробку чітких інструкцій щодо активації резервних компонентів та перевірку їхньої готовності до роботи.

Приклад*. Розробка сценаріїв відновлення для баз даних, які передбачають активацію резервного сервера після збою основного.*

Методи побудови систем холодного резерву

Моніторинг стану системи (System Health Monitoring). Постійний моніторинг основної системи дозволяє вчасно виявляти збої та ініціювати активацію резервних компонентів. Це включає використання програмних інструментів для автоматичного сповіщення про відмови.

***Приклад**. Використання Zabbix для моніторингу серверів і автоматичного запуску резервних ресурсів у разі збою.*

Тестування резерву (Standby Testing). Регулярне тестування резервних компонентів забезпечує їхню готовність до роботи у разі необхідності. Це включає перевірку працездатності обладнання та оновлення програмного забезпечення.

***Приклад**. Щомісячне тестування резервних серверів на предмет працездатності та актуальності даних.*

Синхронізація даних (Data Synchronization). Забезпечення актуальності даних у резервних системах є важливим для швидкого та ефективного відновлення. Це може включати періодичне копіювання даних на резервні носії або використання реплікації в реальному часі.

***Приклад**. Використання системи реплікації баз даних, яка періодично оновлює резервні копії даних.*

Приклади застосування систем холодного резерву

Корпоративні IT-системи. Холодний резерв використовується для серверів, де резервні сервери залишаються вимкненими до моменту відмови основного, що дозволяє знизити витрати на енергію та технічне обслуговування.

Промислові системи. У виробничих процесах холодний резерв використовується для обладнання, яке рідко виходить з ладу, але є критичним для безперервного виробництва.

Мережеві інфраструктури. У мережах холодний резерв застосовується для маршрутизаторів і комутаторів, які активуються лише в разі виходу з ладу основного обладнання.

Посилання на стандарти та джерела

- ISO 22301: Стандарт з управління безперервністю бізнесу, який охоплює планування та реалізацію систем холодного резерву.
- NIST SP 800-34: Керівництво з планування безперервності роботи інформаційних систем, що включає методи побудови систем холодного резерву.
- IEC 62351: Стандарт з кібербезпеки для енергетичних систем, що охоплює стратегії резервування та відновлення.

ПОБУДОВА СИСТЕМ ГАРЯЧОГО РЕЗЕРВУ

Вступ до систем гарячого резерву

Системи гарячого резерву забезпечують високу надійність та доступність комп'ютеризованих систем, особливо в критично важливих середовищах, де навіть короткочасна зупинка роботи є неприпустимою. Гарячий резерв передбачає наявність резервних компонентів або систем, які працюють паралельно з основними та можуть негайно взяти на себе їхні функції у разі відмови.

Основні поняття

Гарячий резерв (Hot Standby). Гарячий резерв означає, що резервні компоненти постійно активні та синхронізовані з основною системою. У разі відмови основного компонента резерв автоматично та негайно починає виконувати його функції без переривання роботи системи.

***Приклад**. У банківських системах гарячий резерв використовується для серверів баз даних, щоб забезпечити безперервність транзакцій навіть у разі збою основного сервера.*

Автоматичне переключення (Automatic Failover). Автоматичне переключення на резервні компоненти відбувається миттєво після виявлення збою, що мінімізує час простою і втрати даних. Це забезпечує високу доступність системи.

***Приклад**. У системах управління польотом літаків автоматичне переключення на резервний комп'ютер відбувається без втрати керування літаком у разі збою основного комп'ютера.*

Синхронізація в реальному часі (Real-Time Synchronization). Постійна синхронізація даних між основними та резервними компонентами забезпечує готовність гарячого резерву взяти на себе функції основної системи без затримок або втрат даних.

***Приклад**. У розподілених базах даних синхронізація в реальному часі дозволяє резервному серверу негайно продовжити обробку запитів після відмови основного.*

Методи побудови систем гарячого резерву

Кластеризація (Clustering). Кластеризація передбачає об'єднання декількох серверів або інших компонентів у кластер, де всі компоненти активно працюють та забезпечують безперервність роботи. У разі відмови одного з компонентів його функції автоматично переходять до іншого.

***Приклад**. Кластеризація серверів у дата-центрі дозволяє забезпечити безперебійне обслуговування вебсайтів навіть при збоях окремих серверів.*

Балансування навантаження (Load Balancing). Балансування навантаження розподіляє роботу між кількома активними компонентами, забезпечуючи рівномірний розподіл ресурсів і миттєве переключення на резерв у разі відмови.

***Приклад**. У мережевих системах балансувальники навантаження розподіляють трафік між кількома маршрутизаторами, забезпечуючи безперебійний доступ до мережі.*

Реплікація даних (Data Replication). Реплікація даних забезпечує постійну синхронізацію інформації між основними та резервними системами, що дозволяє зберігати актуальність даних навіть у разі відмови одного з компонентів.

***Приклад.** У банківських системах реплікація баз даних у режимі реального часу дозволяє зберігати всі транзакції та забезпечувати їх безперервність.*

Приклади застосування систем гарячого резерву

Банківські системи. У банківських установах використовується гарячий резерв для забезпечення безперервності обробки фінансових транзакцій. Це включає резервні сервери баз даних та системи управління, що забезпечують миттєве переключення у разі відмови.

Авіаційні системи. У системах управління польотом літаків гарячий резерв використовується для забезпечення безперебійної роботи критичних систем, таких як навігація та управління польотом.

Мережеві інфраструктури. У великих мережевих інфраструктурах використовується гарячий резерв для комутаторів і маршрутизаторів, що дозволяє забезпечити безперебійний доступ до мережевих ресурсів навіть у разі збоїв обладнання.

Посилання на стандарти та джерела

- ISO/IEC 20000-1: Стандарт для управління IT-послугами, що включає вимоги до забезпечення безперервності роботи та використання гарячого резерву.
- IEEE 1471: Стандарт з архітектури програмних систем, що охоплює принципи побудови відмовостійких систем, включаючи гарячий резерв.
- ISO 22301: Стандарт для управління безперервністю бізнесу, що охоплює стратегії резервування та автоматичного переключення.

ПОБУДОВА СИСТЕМ ТЕПЛОГО РЕЗЕРВУ

Вступ до систем теплого резерву

Системи теплого резерву є компромісним рішенням між холодним і гарячим резервуванням. Вони забезпечують баланс між швидкістю відновлення та економічністю, зберігаючи резервні компоненти в стані готовності, що дозволяє швидко активувати їх у разі відмови основної системи, але з невеликою затримкою у порівнянні з гарячим резервом.

Основні поняття

Теплий резерв (Warm Standby). Теплий резерв означає, що резервний компонент знаходиться в стані готовності, але не активний. Він може бути швидко активований у разі відмови основного компонента, хоча й з деякою затримкою у відновленні.

Приклад. *У корпоративних IT-системах резервні сервери в стані теплого резерву працюють у режимі очікування і можуть бути активовані за кілька хвилин після відмови основного сервера.*

Активація з мінімальною затримкою (Minimal Delay Activation). Хоча теплий резерв не є миттєво активним, він забезпечує відновлення з мінімальною затримкою. Це досягається за рахунок попередньої підготовки системи до роботи, такої як синхронізація конфігурацій та періодичне оновлення даних.

Приклад*. У системах баз даних резервні сервери в теплому резерві синхронізуються з основними базами через регулярні проміжки часу, що дозволяє швидко взяти на себе навантаження після збою.*

Економія ресурсів (Resource Efficiency). Теплий резерв дозволяє знизити витрати на підтримку, оскільки резервні компоненти не працюють постійно, як у випадку гарячого резерву, але готові до швидкої активації.

Приклад*. У мережевих системах комутатори в теплому резерві споживають мінімальні ресурси до моменту активації, що знижує витрати на енергоспоживання.*

Методи побудови систем теплого резерву

Регулярна синхронізація (Regular Synchronization). Регулярна синхронізація даних і конфігурацій між основною системою та резервом забезпечує готовність резервного компонента до швидкої активації. Цей процес може бути автоматизованим, що зменшує час на підготовку резерву у разі відмови основного компонента.

Приклад. *Використання інструментів реплікації даних, таких як Microsoft SQL Server Replication, для регулярного оновлення резервної бази даних.*

Періодичне тестування резерву (Periodic Standby Testing). Періодичне тестування теплого резерву є критичним для забезпечення його готовності. Це включає тестування працездатності, синхронізації даних та швидкості активації, щоб гарантувати мінімальні затримки під час реальної відмови.

Приклад. *Щотижневе тестування активації резервного сервера для перевірки його працездатності та відповідності конфігурацій.*

Автоматизоване перемикання (Automated Failover). Автоматизоване перемикання на резерв у разі відмови основного компонента забезпечує швидке відновлення роботи з мінімальними затримками. Цей процес може включати автоматичне розподілення навантаження, перенаправлення трафіку або запуск резервних сервісів.

Приклад. *Використання балансувальників навантаження, які автоматично перемикають трафік на резервні сервери в разі збою основного.*

Приклади застосування систем теплого резерву

Корпоративні IT-системи. У великих корпоративних мережах теплий резерв використовується для серверів додатків, де резервні сервери запускаються автоматично після відмови основних, забезпечуючи відновлення роботи з мінімальними затримками.

Фінансові системи. У банківських системах використовується теплий резерв для критичних сервісів, таких як обробка платежів, щоб забезпечити швидке відновлення після збоїв без необхідності постійного дублювання даних у режимі реального часу.

Промислові системи. У виробничих процесах теплий резерв застосовується для контролерів автоматизації, які знаходяться в стані готовності і можуть бути швидко активовані для відновлення управління виробництвом у разі збою основного контролера.

Посилання на стандарти та джерела

- ISO 22301: Стандарт з управління безперервністю бізнесу, що охоплює стратегії теплого резерву.
- NIST SP 800-34: Керівництво з планування безперервності роботи інформаційних систем, що включає методи побудови систем теплого резерву.
- IEC 62443: Стандарт з кібербезпеки для промислових систем, що охоплює резервування та відновлення.

СУПЕРКРИТИЧНІ СИСТЕМИ. ПОБУДОВА СУПЕРКРИТИЧНИХ СИСТЕМ

Вступ до суперкритичних систем

Суперкритичні системи є найбільш надійними та безпечними серед усіх типів комп'ютеризованих систем, оскільки їхня відмова може призвести до катастрофічних наслідків. Ці системи застосовуються в галузях, де безпека є пріоритетом, наприклад, в авіації, атомній енергетиці, медичних пристроях і оборонних технологіях. Побудова суперкритичних систем вимагає застосування найсучасніших методів резервування, контролю та верифікації, щоб мінімізувати ймовірність відмови та забезпечити їх безперебійну роботу.

Основні поняття

Суперкритична система (Supercritical System). Суперкритична система – це система, відмова якої може мати надзвичайно значні наслідки, включаючи загрозу життю, значні фінансові втрати або шкоду довкіллю. Для таких систем висуваються особливі вимоги щодо надійності, безпеки та відмовостійкості.

Приклад: *Системи управління реакторами в атомних електростанціях, де відмова може призвести до радіаційної катастрофи.*

Відмовостійкість на рівні компонентів (Component-Level Fault Tolerance). У суперкритичних системах забезпечується висока відмовостійкість на рівні окремих компонентів. Це досягається за рахунок дублювання, гарячого резервування, а також використання високонадійних компонентів.

Приклад. *В авіаційних системах управління польотом застосовуються дубльовані сенсори та виконавчі механізми, щоб забезпечити безперебійну роботу навіть при відмові одного з них.*

Функціональна безпека (Functional Safety). Функціональна безпека забезпечує, що система буде безпечною навіть у разі виникнення відмов. Це включає розробку захисних механізмів, таких як аварійне вимкнення, запобігання небезпечним діям, та автоматичне відновлення після збою.

Приклад. *У медичних пристроях, наприклад, кардіостимуляторах, вбудовуються захисні механізми, які перешкоджають небезпечним режимам роботи при збоях.*

Методи побудови суперкритичних систем

Повторювані резервні архітектури (Redundant Architectures). Суперкритичні системи будуються на основі резервних архітектур, де кожна функція дублюється кілька разів для забезпечення безперебійної роботи. Це включає гаряче резервування на рівні компонентів, систем та підсистем.

Приклад: *В атомній енергетиці системи управління реактором можуть мати трикратне дублювання всіх критичних компонентів, щоб гарантувати їхню безперебійну роботу.*

Верифікація та валідація (Verification and Validation, V&V). Процеси верифікації та валідації є невід'ємною частиною розробки суперкритичних систем. Вони включають ретельне тестування, формальну перевірку, аналіз помилок і перевірку відповідності системи всім нормативним вимогам.

Приклад: *У розробці програмного забезпечення для авіоніки проводиться формальна верифікація кожного рядка коду для забезпечення відповідності суворим стандартам безпеки.*

Безперервний моніторинг та самодіагностика (Continuous Monitoring and Self-Diagnosis). Суперкритичні системи оснащуються механізмами безперервного моніторингу та самодіагностики, що дозволяють оперативно виявляти та реагувати на відмови або відхилення в роботі системи.

Приклад. *У сучасних авіаційних системах використовується безперервний моніторинг стану систем і компонентів з автоматичним повідомленням пілотів або наземних служб про будь-які відхилення.*

Приклади застосування суперкритичних систем

Авіаційні системи. В авіації суперкритичні системи включають управління польотом, де відмовостійкість забезпечується через дублювання всіх ключових систем, таких як навігація, зв'язок, та управління двигунами.

Атомні електростанції. В атомній енергетиці суперкритичні системи управління реактором передбачають наявність багаторівневого

захисту, включаючи аварійні системи охолодження та автоматичне вимкнення у разі відхилення від нормальних умов.

Медичні пристрої. Суперкритичні системи в медицині, такі як кардіостимулятори або апарати штучного дихання, мають вбудовані механізми резервування та аварійного вимкнення, що забезпечує безпеку пацієнтів навіть при збої.

Посилання на стандарти та джерела

- IEC 61508: Стандарт з функціональної безпеки електричних, електронних і програмних систем, що охоплює вимоги до розробки суперкритичних систем.
- DO-178C: Стандарт для програмного забезпечення авіоніки, що включає вимоги до верифікації та валідації.
- ISO 26262: Стандарт з функціональної безпеки для автомобільної промисловості, який застосовується при розробці суперкритичних систем у транспортних засобах.

САМОСТІЙНА РОБОТА СТУДЕНТІВ

Розрахунково-графічна робота (РГР)

Студент повинен підготувати та захистити Розрахунково-графічну роботу (РГР), яка включає наступні пункти:

1. Проведення HARA.
2. Методи розрахунку надійності.
3. Методи розрахунку відмовостійкості.
4. Методи оцінки ймовірності відмови чи збою (I).
5. Методи оцінки тяжкості збою (S).
6. Методи оцінки ризиків.
7. Методи зменшення ризику.
8. Інструменти зменшення ризику.
9. Побудова надійних систем.
10. Побудова відмовостійких систем.
11. Побудова системи холодного резерву.
12. Побудова систем гарячого резерву.
13. Побудова систем теплого резерву.
14. Суперкритичні системи. Побудова суперкритичних систем.

Вимоги до роботи

1. **Оформлення:** РГР повинна бути виконана згідно зі стандартом ДСТУ 3008:2015 "Звіти у сфері науки і техніки. Структура та правила оформлення". Усі текстові, графічні та табличні матеріали повинні відповідати вимогам цього стандарту. Зокрема:
   - Титульний аркуш, зміст, вступ, основна частина, висновки та список літератури мають бути оформлені відповідно до вимог стандарту.
   - Всі таблиці, рисунки та діаграми повинні мати номери та назви, оформлені згідно зі стандартом. Таблиці повинні бути розміщені після першого згадування у тексті або на наступній сторінці.
   - Шрифт основного тексту — Times New Roman, розмір 14, міжрядковий інтервал — 1,5. Поля документа: верхнє і нижнє — 2 см, ліве — 3 см, праве — 1 см.

2. **Короткість викладу:** Виклад матеріалу повинен бути лаконічним, чітким і зрозумілим. Надмірна деталізація або відступи від основної теми не допускаються. Студент повинен концентруватися на головних аспектах і уникати включення несуттєвої інформації.

3. **Захист роботи:** Захист РГР є обов'язковим етапом. Студент повинен підготувати презентацію, в якій чітко і структуровано представить виконану роботу. Під час захисту студент повинен продемонструвати глибоке розуміння теми, пояснити застосовані методи, результати та зроблені висновки. Також студент повинен бути готовим відповісти на запитання комісії щодо будь-яких аспектів своєї роботи.

4. **Унікальність роботи:** Кожна робота повинна бути унікальною в поданні. Плагіат не допускається і буде негативно впливати на оцінку. Всі роботи перевіряються на унікальність, і виявлення запозиченого матеріалу без належного посилання призведе до зниження оцінки або неприйняття роботи.

5. **Індивідуальні відмінності:** Кожна робота має індивідуальні відмінності, що задаються унікальним коефіцієнтом студента. Цей коефіцієнт розраховується на основі перших трьох літер прізвища та першої літери імені студента. Деталі щодо розрахунку коефіцієнта та його впливу на завдання описані у наступних розділах методички.

Варіації завдань

Завдання розподіляються відповідно до перших літер прізвища та імені студента. Кожен студент отримує індивідуальне завдання, яке покриває всі етапи, зазначені у розрахунково-графічній роботі (РГР).

Для кожного студента буде обчислюватись унікальний коефіцієнт, який визначатиме, який параметр він використовуватиме у своїй розрахунково-графічній роботі (РГР). Формула для обчислення коефіцієнта виглядає так:

$$K=(P1\times P2\times P3) / (10\times L1),$$

де

- P1, P2, P3 — порядкові номери трьох перших літер прізвища студента.

- L1 — порядковий номер першої літери імені студента.

Після обчислення коефіцієнта K, асоціюйте його зі списком параметрів.

Таблиця 2

Значення P1,P2,P3, L1

Літера	**Порядковий номер**	**Літера**	**Порядковий номер**
А	1	М	17
Б	2	Н	18
В	3	О	19
Г	4	П	20
Ґ	5	Р	21
Д	6	С	22
Е	7	Т	23
Є	8	У	24
Ж	9	Ф	25
З	10	Х	26
И	11	Ц	27
І	12	Ч	28
Ї	13	Ш	29
Й	14	Щ	30
К	15	Ь	31
Л	16	Ю	32
		Я	33

Приклад обчислення коефіцієнта

Студент: Іван Петренко

- Прізвище: Петренко
  - Перша літера: **П** (номер 20)
  - Друга літера: **е** (номер 7)
  - Третя літера: **т** (номер 23)
- Ім'я: Іван
  - Перша літера: **І** (номер 12)

Коефіцієнт K:

$K = (20 \times 7 \times 23)/(12 \times 10) \approx 26.83$

Таблиця 3

Таблиця параметрів для студентів (на основі K)

Інтервал коефіцієнтів K	Параметри завдання	Коментар
0 - 50	Побудова системи на основі одного критичного компоненту з високою ймовірністю відмови (P)	Завдання полягає у розробці системи, що залежить від одного важливого компоненту та його захисту.
51 - 100	Оптимізація системи під змінне навантаження та визначення критичних точок при пікових навантаженнях	Важливо знайти та усунути критичні точки при високих навантаженнях на систему.
101 - 150	Планування процесу відновлення системи з урахуванням складних багатофакторних відмов	Завдання включає розробку плану дій при настанні складних відмов, що впливають на систему.
151 - 200	Моделювання та управління потоками помилок у системі з високим навантаженням	Необхідно створити модель, яка здатна справлятися з високим навантаженням та зменшувати помилки.
201 - 250	Розробка та порівняння варіантів резервування з акцентом на вартість і ефективність	Потрібно оцінити різні стратегії резервування та обрати найкращу з точки зору ефективності та вартості.
251 - 300	Планування та оптимізація кількості резервних компонентів з урахуванням їхньої надійності	Завдання полягає в знаходженні оптимального балансу між кількістю резервних компонентів та їх надійністю.
301 - 350	Аналіз відмовостійкості системи при застосуванні різних стратегій резервування	Необхідно проаналізувати, як різні стратегії резервування впливають на загальну відмовостійкість системи.
351 - 400	Розробка профілактичних заходів з урахуванням вартості простою та ефективності системи	Завдання полягає в розробці заходів, які мінімізують час простою системи, забезпечуючи її ефективність.
401 - 450	Оцінка ефективності управління часом простою	Важливо оцінити, наскільки ефективно система управляє

Інтервал коефіцієнтів K	Параметри завдання	Коментар
	системи при різних сценаріях відмов	простоєм під час різних відмов.
451 - 500	Розрахунок і мінімізація ймовірності критичної відмови системи	Завдання передбачає розробку стратегій для мінімізації ймовірності виникнення критичних відмов.
501 - 550	Оцінка швидкості реакції системи на відмови при різних рівнях навантаження	Необхідно визначити, як швидко система може реагувати на відмови при різних умовах навантаження.
551 - 600	Розробка стратегії підвищення надійності системи в умовах нестабільного енергопостачання	Важливо розробити стратегії для підвищення надійності системи в умовах нестабільного енергопостачання.
601 - 650	Аналіз і оптимізація часу між відмовами (MTBF) для складних інтегрованих систем	Завдання полягає в тому, щоб збільшити час між відмовами у складних інтегрованих системах.
651 - 700	Оптимізація структури системи з метою зменшення кількості компонентів та підвищення ефективності	Необхідно оптимізувати систему, зменшуючи кількість компонентів без втрати ефективності.
701 - 750	Розробка та впровадження стратегії відновлення системи при катастрофічних збоях	Завдання передбачає розробку стратегії для відновлення системи після значних збоїв.
751 - 800	Оцінка ризиків та розробка стратегій їх мінімізації на основі прогнозних моделей	Студент повинен оцінити ризики та розробити стратегії їх мінімізації, використовуючи прогнозні моделі.
801 - 850	Моделювання інтенсивності відмов системи під впливом зовнішніх загроз	Завдання полягає в тому, щоб змоделювати, як зовнішні загрози впливають на інтенсивність відмов.
851 - 900	Оцінка часу до критичної відмови системи з	Важливо розрахувати час до критичної відмови з

Інтервал коефіцієнтів K	Параметри завдання	Коментар
	урахуванням старіння та зносу	урахуванням зносу компонентів.
901 - 950	Аналіз рівня загрози для системи з урахуванням використання систем безпеки	Необхідно оцінити, як системи безпеки впливають на загальний рівень загрози для системи.
951 - 1000	Комплексний аналіз відмовостійкості системи з урахуванням ризиків і сценарного планування	Завдання полягає в проведенні комплексного аналізу відмовостійкості системи з урахуванням можливих ризиків.

ОЦІНЮВАННЯ РОБОТИ СТУДЕНТІВ

Оцінювання успішності студентів базується на кількох ключових критеріях, які охоплюють як практичні, так і теоретичні аспекти навчання. Основний акцент робиться на виконанні та захисті розрахунково-графічної роботи (РГР), яка є головним елементом курсу. Система оцінювання складається з таких компонентів:

1. Розрахунково-графічна робота (РГР) – 80 % загальної оцінки

- **Якість виконання:** 50% Оцінюється правильність та точність виконання завдання, відповідність стандартам оформлення (ДСТУ 3008:2015), здатність студента застосувати теоретичні знання на практиці, а також глибина аналізу.
- **Унікальність роботи:** 20 % Враховується оригінальність підходу, відсутність плагіату, індивідуальний характер виконаної роботи з урахуванням унікального параметра, що задає особливості виконання.
- **Захист роботи:** 10 % Оцінюється здатність студента презентувати свою роботу, обґрунтовувати вибрані підходи та методи, захищати свої рішення, а також відповідати на питання комісії. Увага приділяється глибині розуміння теми та вмінню аргументовано відповідати на запитання.

2. Активність під час занять – 10 % загальної оцінки

- **Участь у дискусіях:** 5 % Оцінюється активність студента в обговореннях під час лекцій та практичних занять, здатність висловлювати свої думки, задавати питання та аналізувати відповіді інших.
- **Відвідуваність:** 5 % Оцінюється регулярність відвідування занять та активна участь у них.

3. Підсумковий іспит – 10 % загальної оцінки

- **Теоретичний тест:** 6 % Включає питання на перевірку теоретичних знань, що охоплюють весь матеріал курсу.
- **Практичне завдання:** 4 % Завдання, яке студент повинен виконати під час іспиту, демонструючи здатність застосовувати знання на практиці.

Підсумкова оцінка

Підсумкова оцінка формується як сума всіх вищезазначених компонентів. Основний акцент робиться на якості та унікальності РГР, що відображає практичні навички та здатність студента виконати комплексне завдання самостійно. Така система оцінювання забезпечує об'єктивне та комплексне оцінювання знань та навичок студентів, з урахуванням як теоретичних, так і практичних аспектів курсу.

ЗАКЛЮЧНЕ СЛОВО

Завершуючи цей курс, важливо підкреслити, що надійність та відмовостійкість є основними складовими успішного функціонування сучасних комп'ютерних систем. Вивчення методів забезпечення надійності, аналізу ризиків, а також впровадження систем захисту і резервування – це не лише теоретичні аспекти, але й практичні навички, які студенти зможуть застосувати у своїй професійній діяльності.

Матеріали, представлені в цих методичних рекомендаціях, покликані допомогти вам глибше зрозуміти процеси, що лежать в основі створення надійних та безпечних систем. Кожен розділ методичних рекомендацій базується на досвіді, накопиченому під час роботи у провідних технологічних компаніях, і відображає актуальні практики та стандарти галузі. Це робить їх цінним ресурсом для будь-якого інженера, який прагне досягти високого рівня професійної компетентності.

Успішне завершення курсу і виконання розрахунково-графічної роботи засвідчить ваше глибоке розуміння предмету та готовність до вирішення реальних завдань у сфері інформаційних технологій. Сподіваюсь, що знання, здобуті під час вивчення цього курсу, стануть для вас міцним фундаментом у вашій майбутній кар'єрі.

Не зупиняйтесь на досягнутому. Постійно розширюйте свої знання, удосконалюйте навички, і ви зможете стати справжніми професіоналами, здатними створювати і підтримувати надійні, безпечні та ефективні системи у будь-якій галузі.

Бажаю вам успіху в усіх починаннях та впевненості у власних силах на шляху до професійного зростання!

Дмитро Гуменний, Ph.D.

Додаток А

Таблиця стандартів

Стандарт	Опис
IEC 61078	Стандарт для аналізу надійності і відмовостійкості систем за допомогою діаграм блоків надійності
MIL-HDBK-217F	Довідник з надійності електронних систем і компонентів, який надає методики розрахунку надійності для військових і промислових застосувань
ISO 26262	Стандарт для автомобільних систем, що охоплює методи оцінки тяжкості збоїв у контексті функціональної безпеки
IEC 61508	Стандарт для функціональної безпеки електричних, електронних і програмних систем
MIL-STD-882E	Стандарт з системної безпеки, що використовується для оцінки тяжкості збоїв у військових системах
ISO 22301	Стандарт з управління безперервністю бізнесу, що охоплює стратегії теплого резерву
NIST SP 800-34	Керівництво з планування безперервності роботи інформаційних систем
IEC 62443	Стандарт з кібербезпеки для промислових систем, що охоплює резервування та відновлення
IEC 60812	Стандарт, що охоплює методи аналізу ймовірності відмови, включаючи FTA
MIL-HDBK-338B	Довідник, який містить методи розрахунку ймовірності відмови для військових систем
ISO 31000	Стандарт з управління ризиками, що охоплює принципи та рекомендації для оцінки ризиків
ISO/IEC 20000-1	Стандарт для управління IT-послугами, що включає вимоги до забезпечення безперервності роботи та використання гарячого резерву
IEEE 1471	Стандарт з архітектури програмних систем, що охоплює принципи побудови відмовостійких систем, включаючи гарячий резерв
MIL-STD-1629A	Стандарт з аналізу видів і наслідків відмов для військових систем
NASA Fault Tree Handbook	Керівництво з аналізу дерева відмов, що широко використовується у космічній галузі
DO-178C	Design Assurance Guidance for Airborne Electronic Hardware

Додаток В

Таблиця скорочень

Скорочення	**Повна назва**
HARA	Hazard and Risk Analysis
RPN	Risk Priority Number
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
FTA	Fault Tree Analysis
FMEA	Failure Modes and Effects Analysis
SFF	Safe Failure Fraction
R(t)	Reliability over time
FIT	Failures In Time
RBD	Reliability Block Diagram
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MIL-HDBK	Military Handbook
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology

Навчально-методичне видання

НАДІЙНІСТЬ КОМП'ЮТЕРНИХ СИСТЕМ

Методичні вказівки
для здобувачів першого (бакалаврського) рівня
вищої освіти за спеціальностями
123 «Комп'ютерна інженерія» та 125 «Кібербезпека»

Укладач **Гуменний** Дмитро Олександрович

Комп'ютерне верстання *А. П. Селівестрової*

Ум. друк. арк. 3,02. Обл.-вид. арк. 3,25
Електронний документ. Вид № 45/V-24.

Виконавець і виготовлювач
Київський національний університет будівництва і архітектури

Проспект Повітряних Сил, 31, Київ, Україна, 03680

Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи ДК № 808 від 13.02.2002 р