**MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE**
NATIONAL AVIATION UNIVERSITY
Faculty of Aeronavigation, Electronics and Telecommunications
Department of computer integrated complexes

**ADMIT TO DEFENSE**
Head of the graduating department
_____ Viktor M. Sineglazov

“_____”_____2024y
.

# QUALIFICATION WORK
## (EXPLANATORY NOTE)

OF THE GRADUATE OF THE EDUCATIONAL DEGREE
“BACHELOR”
Specialty 151 "Automation and computer-integrated technologies"
Educational and professional program "Computer-integrated technological processes and production"

**Theme: Control system of the MRPD – 05 microprocessor relay protection device**

Performer: student of FAET-421 group Kostiuchenko Maksym Volodymyrovych
Supervisor: Doctor of Technical Sciences, Professor Synieglazov Viktor Mykhailovych

Norm controller: _____ Filyashkin M.K.
(sign)

Kyiv – 2024

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет аеронавігації, електроніки та телекомунікацій
Кафедра авіаційних комп'ютерно-інтегрованих систем

**ДОПУСТИТИ ДО ЗАХИСТУ**
Завідувач випускової кафедри
_____ Віктор СИНЄГЛАЗОВ
“____” _____2024 р.

# КВАЛІФІКАЦІЙНА РОБОТА
# (ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
“БАКАЛАВР”

Спеціалність 151 "Автоматизація, та комп’ютерно-інтегровані технології"

Освітньо-професійна програма "Комп’ютерно-інтегровані технологічні процеси і виробництва"

**Тема: Система керування мікропроцесорним пристроєм релейного захисту МРЗС - 05**

Виконавець: студент групи ІК-421 Костюченко Максим Володимирович
Керівник: доктор технічних наук, професор Синєглазов Віктор Михайлович

Нормоконтроллер: _____ Філяшкін М.К.
(підпис)

Київ – 2024

**NATIONAL AVIATION UNIVERSITY**
Faculty of Aeronautics, Electronics and Telecommunications
Department of aviation computer-integrated systems

Educational degree: Bachelor
Specialty 174 "Automation, computer-integrated technologies and robotics"
Educational and professional program "Computer-integrated technological processes and production"

**APPROVED**
Head of department
_____ Sineglazov V.M
“ ____” _____2024.

**TASK**
**For the student’s thesis**
**by: Kostiuchenko Maksym Volodymyrovych**

1. **Thesis topic** (project topic) “Control system of the MRPD – 05 microprocessor relay protection device”
2. **Deadline for an execution of a project**: from May 10 of 2024 to June 7 of 2024
3. **Initial data for the project**: The process of developing a control system for the microprocessor-based relay protection device MRZS - 05 to improve the reliability and efficiency of relay protection systems.
4. **Contents for explanatory note:**

1. General analysis of relay protection systems.
2. Analysis of microprocessor-based relay protection devices.
3. Analysis of the operating principles and functions of MRZS - 05.
4. Design of the control system for the microprocessor-based device.
5. Development and implementation of software for MRZS - 05.
6. Testing and tuning of the control system.
7. Analysis of results and evaluation of system effectiveness.

5. **List of required graphic material**: figures, tables and diagrams.

6. **Calendar schedule-plan:**

| № | Task | Execution term | Execution mark |
|---|---|---|---|
| 1. | Getting the task | 01.04.2024 – 02.04.2024 | Done |
| 2. | Formation of the purpose and main objectives of the study | 02.04.2024 – 14.04.2024 | Done |
| 3. | Analysis of existing methods | 15.04.2024 – 30.04.2024 | Done |
| 4. | Theoretical consideration of problem solving | 01.05.2024 – 05.05.2024 | Done |
| 5. | Analysis of algorithm for designing an industrial automation system using CAD software | 06.05.2024 – 25.05.2024 | Done |
| 6. | Preparation of an explanatory note | 26.05.2024 – 03.06.2024 | Done |
| 7. | Preparation of presentation and handouts | 04.06.2024 – 06.06.2024 | Done |

7. **Task issue date:** 01 “April” 2024.

Supervisor: _____ Sineglazov V.M
(sign)

Task is taken for completion by: _____ Kostiuchenko M. V.
(sign)

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**
Факультет аеронавігації, електроніки та телекомунікацій
Кафедра авіаційних комп'ютерно-інтегрованих комплексів

Освітній ступінь: Бакалавр
Спеціальність 151 "Автоматизація та комп'ютерно-інтегровані технології"
Освітньо-професійна програма "Комп'ютерно-інтегровані технологічні процеси і виробництва"

**ЗАТВЕРДЖУЮ**
Завідувач кафедри
_____ Віктор СИНЄГЛАЗОВ
" "
_____2024 р.

**ЗАВДАННЯ**
**на виконання кваліфікаційної роботи студента**
**Костюченко Максим Володимирович**

1. **Тема роботи** " Система керування мікропроцесорним пристроєм релейного захисту МРЗС - 05"
2. **Термін виконання роботи**: з 10.03.2024 по 7.06.2024
3. **Вихідні дані до роботи**: Процес розробки системи керування мікропроцесорним пристроєм релейного захисту МРЗС - 05 для підвищення надійності та ефективності функціонування систем релейного захисту
4. **Зміст пояснювальної записки (перелік питань, що підлягають розробці):**

1. Загальний аналіз систем релейного захисту. 2. Аналіз мікропроцесорних пристроїв релейного захисту.

3. Аналіз принципів роботи та функцій МРЗС - 05. 4. Проектування системи керування мікропроцесорним пристроєм.

5. Розробка та реалізація програмного забезпечення для МРЗС - 05. 6. Тестування та налагодження системи керування. 7. Аналіз результатів та оцінка ефективності системи.

5 **Перелік обов'язкового графічного матеріалу**: графіки, таблиці, зображення. діаграми.

6 **Календарний план-графік:**

| № | Завдання | Термін виконання | Відмітка про виконання |
|---|---|---|---|
| 1. | Отримання завдання | 01.04.2024 - 02.04.2024 | Виконано |
| 2. | Формування мети та основних завдань дослідження | 02.04.2024 – 14.04.2024 | Виконано |
| 3. | Аналіз існуючих методів | 15.04.2024 – 30.04.204 | Виконано |
| 4. | Теоретичний розгляд вирішення поставлених завдань | 01.05.2024 – 30.04.2024 | Виконано |
| 5. | Аналіз алгоритму проектування систем промислової автоматизації з використанням необхідного програмного забезпечення | 01.05.2024 – 05.05.2024 | Виконано |
| 6. | Оформлення пояснювальної записки | 26.05.2024 – 03.06. 2024 | Виконано |
| 7. | Підготовка презентації та роздаткового матеріалу | 04.06.2024 – 06.06.2024 | Виконано |

7 **Дата видачі завдання** ___ «01» березня 2024 р.

**Керівник: _____** Синєглазов В.М.
(підпис)

**Завдання прийняв до виконання: _____** Костюченко М.В
(підпис)

# ABSTRACT

Explanatory Note for the Qualification Work "Control System for the Microprocessor-Based Relay Protection Device MRZS - 05"

Keywords: MICROPROCESSOR DEVICE, RELAY PROTECTION, CONTROL SYSTEM, ELECTRICAL NETWORKS, AUTOMATIC DISCONNECTION.

Object of Study: The microprocessor-based relay protection device MRZS - 05 and its elements.

Subject of Study: The control system for the microprocessor-based relay protection device.

Purpose of the Qualification Work: To study and analyze the operating principles and architecture of the control system for the microprocessor-based relay protection device MRZS - 05 to enhance the reliability and efficiency of electrical network protection.

Research Method: Comparative analysis, literature review, modeling, and testing of the control system.

Theoretical Research: Involved a thorough analysis of the architecture and algorithms of microprocessor-based relay protection devices, as well as the principles of designing and implementing control systems.

Research Results: Demonstrated that the developed control system for the microprocessor-based relay protection device MRZS - 05 significantly improves the responsiveness to emergency situations, reduces the number and duration of outages, and enhances the reliability of power supply.

Practical Significance: The results of the qualification work can be used to familiarize with control systems for microprocessor-based relay protection devices, their features, and useful tools that can be employed by specialists to improve the efficiency of electrical networks.

# РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи "Система керування мікропроцесорним пристроєм релейного захисту МРЗС - 05"

МІКРОПРОЦЕСОРНИЙ ПРИСТРІЙ, РЕЛЕЙНИЙ ЗАХИСТ, СИСТЕМА КЕРУВАННЯ, ЕЛЕКТРИЧНІ МЕРЕЖІ, АВТОМАТИЧНЕ ВІДКЛЮЧЕННЯ.

Об'єкт дослідження: мікропроцесорний пристрій релейного захисту МРЗС - 05 та його елементи.

Предмет дослідження: система керування мікропроцесорним пристроєм релейного захисту.

Мета кваліфікаційної роботи: вивчити та проаналізувати принцип роботи та архітектуру системи керування мікропроцесорним пристроєм релейного захисту МРЗС - 05 для підвищення надійності та ефективності захисту електричних мереж.

Метод дослідження: порівняльний аналіз, обробка літературних джерел, моделювання та тестування системи керування.

Теоретичні дослідження: полягали в глибокому аналізі архітектури та алгоритмів роботи мікропроцесорних пристроїв релейного захисту, а також вивченні принципів проектування та реалізації систем керування.

Результати досліджень: показали, що розроблена система керування мікропроцесорним пристроєм релейного захисту МРЗС - 05 значно підвищує оперативність реагування на аварійні ситуації, знижує кількість та тривалість аварійних відключень, а також підвищує надійність енергопостачання.

Практичне значення: результати можуть бути використані для ознайомлення з системами керування мікропроцесорними пристроями релейного захисту, їх особливостями та корисними інструментами.

ЗМІСТ

# ВСТУП

Мікропроцесорні релейні захисні системи (МРЗС) є важливим компонентом сучасних електроенергетичних систем, забезпечуючи надійний захист від різних несправностей та аварійних ситуацій. Вони використовують передові технології обробки сигналів та алгоритми для виявлення, аналізу та усунення несправностей в електричних мережах. МРЗС значно перевершують традиційні електромеханічні реле за точністю, швидкістю реакції та можливістю інтеграції з іншими системами.

# РОЗДІЛ 1
# МІКРОПРОЦЕСОРНІ РЕЛЕЙНІ ЗАХИСНІ СИСТЕМИ (МРЗС)

## 1.1. МРЗС огляд та структура

МРЗС поєднують у собі високу точність, швидкодію та надійність, що робить їх незамінними у сучасних системах релейного захисту. Основні компоненти МРЗС включають:

**Сенсори**: Пристрої для вимірювання параметрів електричної мережі, таких як струм, напруга, частота. Сенсори можуть бути аналоговими або цифровими.

**Мікропроцесор**: Центральний компонент системи, який обробляє дані від сенсорів та приймає рішення на основі запрограмованих алгоритмів. Мікропроцесори в МРЗС зазвичай багатоядерні, що забезпечує високу швидкість обробки даних.

**Комунікаційні модулі**: Забезпечують зв'язок між різними компонентами системи та з іншими системами захисту. Вони можуть використовувати різні протоколи передачі даних, такі як Ethernet, Modbus або DNP3.

**Інтерфейси користувача**: Дозволяють операторам взаємодіяти з системою, налаштовувати параметри та отримувати інформацію про стан системи. Інтерфейси можуть бути у вигляді локальних дисплеїв або віддалених робочих станцій.

Мікропроцесорні релейні захисні системи також включають програмне забезпечення, яке керує всіма процесами в системі. Це

програмне забезпечення забезпечує алгоритми захисту, моніторинг стану системи та інтеграцію з іншими системами.

Типова структура МРЗС включає кілька основних елементів, що взаємодіють між собою для забезпечення ефективного захисту. На малюнку 1 представлена загальна схема структури МРЗС[1].

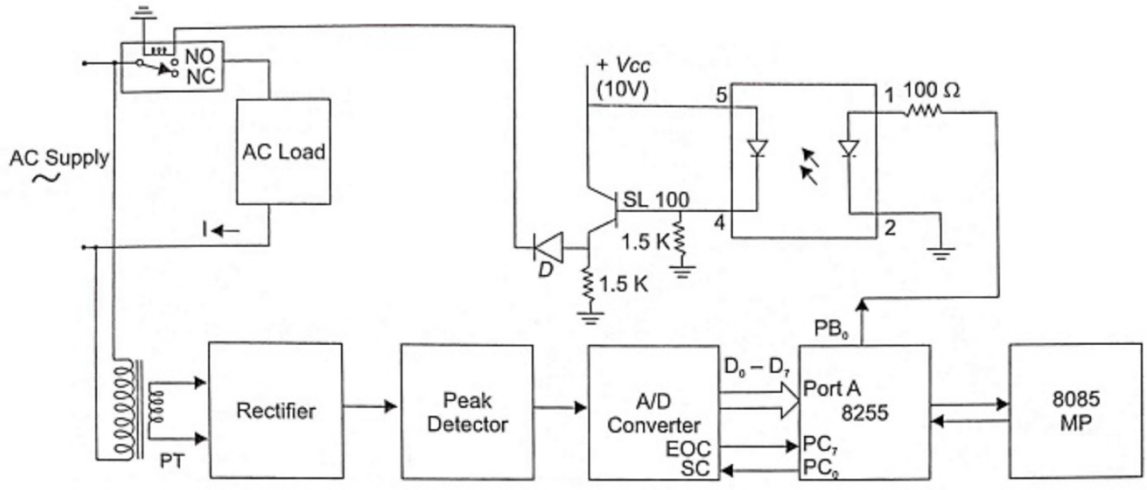


Рис. 1.1. Загальна схема структури МРЗС

У структурі МРЗС важливо розрізняти різні рівні системи: вимірювальний, обчислювальний та комунікаційний.

Вимірювальний рівень: Включає сенсори та інтерфейси збору даних. Цей рівень забезпечує первинні дані для обробки.

Обчислювальний рівень: Складається з мікропроцесорів та іншого апаратного забезпечення для обробки сигналів. Тут виконуються основні алгоритми захисту та аналізу даних.

Комунікаційний рівень: Забезпечує передачу даних між компонентами МРЗС та з зовнішніми системами.

Для точного опису роботи МРЗС використовуються різні математичні моделі та формули. Наприклад, модель виявлення несправностей може бути представлена рівнянням:

$I(t)=I_0 sin(\omega t + \varphi)$ (1.1)

де I(t) – струм в мережі

$I_0$ - амплітуда струму

$\omega$- кутова частота

$\varphi$- початкова фаза

Графік функції струму в залежності від часу можна побудувати для ілюстрації поведінки струму під час нормальної роботи та під час несправності.

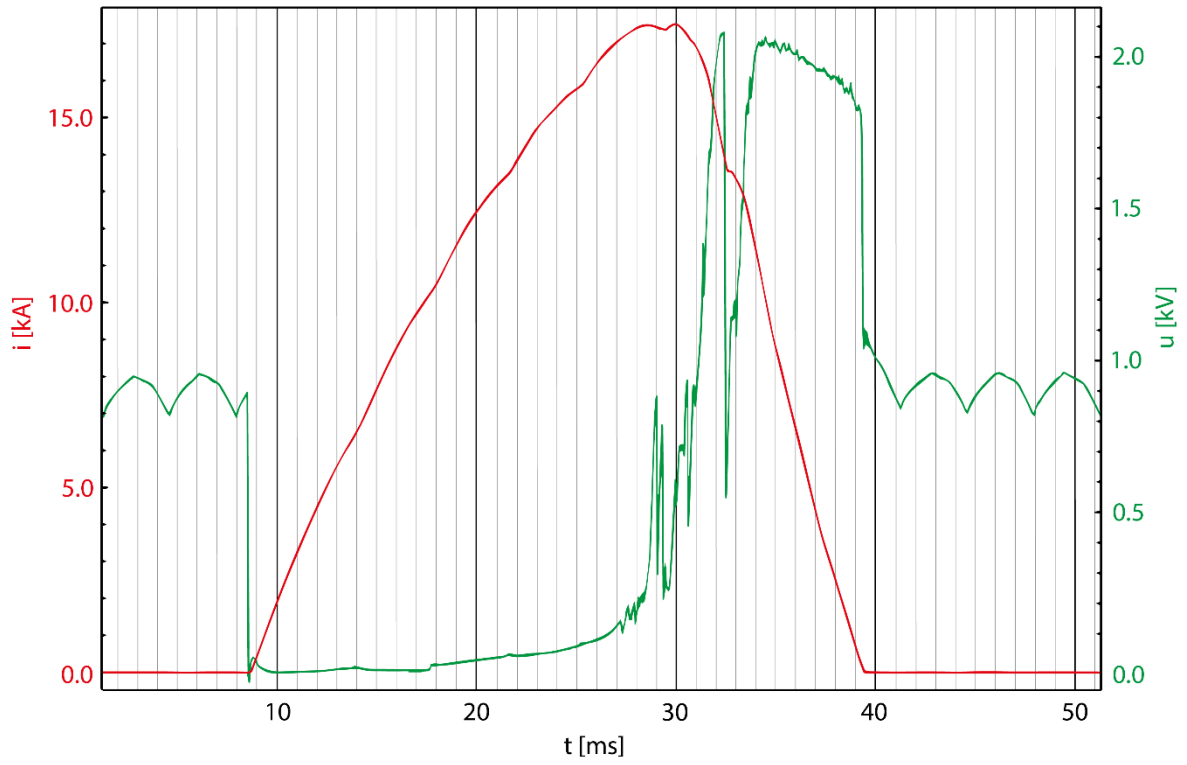


Рис. 1.2. Графік струму в залежності від часу

Важливим елементом МРЗС є фільтрація сигналів. Одним із методів фільтрації є використання цифрових фільтрів, які можуть бути описані рівняннями типу:

$y[n] = \sum_{k=0}^{N} b_k x[n-k] - \sum_{k=1}^{M} a_k y[n-k]$, (1.2)

де y[n] – вихідний сигнал,

$x[n]$ – вхідний сигнал

$b_k$ та $a_k$– коефіцієнти фільтра

Для більш детального аналізу роботи МРЗС можна використовувати спектральний аналіз сигналів, що дозволяє визначити частотні компоненти струмів та напруг у мережі.

## 1.2. Місце МРЗС в системі захисту

Мікропроцесорні релейні захисні системи (МРЗС) відіграють критичну роль у забезпеченні надійності та безпеки електричних мереж. Їх основна функція полягає у швидкому та точному виявленні несправностей і захисті обладнання від пошкоджень, викликаних короткими замиканнями, перевантаженнями та іншими аварійними ситуаціями.

Основні функції МРЗС включають:

1. **Виявлення несправностей**: МРЗС здатні швидко ідентифікувати різні типи несправностей, такі як короткі замикання, перевантаження, зниження напруги тощо. Це забезпечує своєчасне відключення пошкоджених ділянок мережі, що запобігає розповсюдженню аварійних ситуацій.
2. **Розподіл навантаження**: МРЗС можуть допомагати в оптимальному розподілі електричного навантаження, запобігаючи перевантаженням в окремих сегментах мережі. Це дозволяє забезпечити стабільну роботу системи, навіть у випадках підвищеного навантаження.
3. **Автоматичне відключення**: У разі виявлення несправності МРЗС можуть автоматично відключати пошкоджені секції мережі для запобігання подальших пошкоджень. Це зменшує час відновлення після аварії та мінімізує ризик пошкодження обладнання.
4. **Моніторинг і діагностика**: МРЗС забезпечують постійний моніторинг параметрів мережі і можуть проводити діагностику стану обладнання в режимі реального часу. Це дозволяє операторам своєчасно виявляти потенційні проблеми і вживати відповідних заходів для їх усунення.

МРЗС тісно взаємодіють з іншими компонентами системи захисту для забезпечення комплексного захисту електричної мережі. До цих

компонентів належать автоматичні вимикачі, трансформатори, сенсори та системи управління.

**Автоматичні вимикачі**: в разі виявлення несправності МРЗС передають сигнали автоматичним вимикачам для швидкого відключення пошкоджених ділянок мережі. Це дозволяє зменшити тривалість і масштаб аварійних ситуацій.

**Трансформатори**: МРЗС отримують дані від трансформаторів напруги і струму, які використовуються для оцінки стану мережі. Ці дані включають значення струмів та напруг, що дозволяє визначити стан мережі та виявити можливі несправності[2].

**Сенсори**: МРЗС взаємодіють із сенсорами, що вимірюють параметри електричної мережі, такі як струм, напруга, частота тощо. Ці сенсори можуть бути розташовані в різних точках мережі для забезпечення комплексного моніторингу.

**Системи управління**: МРЗС можуть бути інтегровані в загальні системи управління енергомережами, що забезпечує координацію захисту на рівні всієї мережі. Це дозволяє централізовано управляти захисними функціями та забезпечувати ефективну реакцію на аварійні ситуації.

Для ілюстрації місця МРЗС в системі захисту, розглянемо спрощену схему взаємодії між різними компонентами системи:

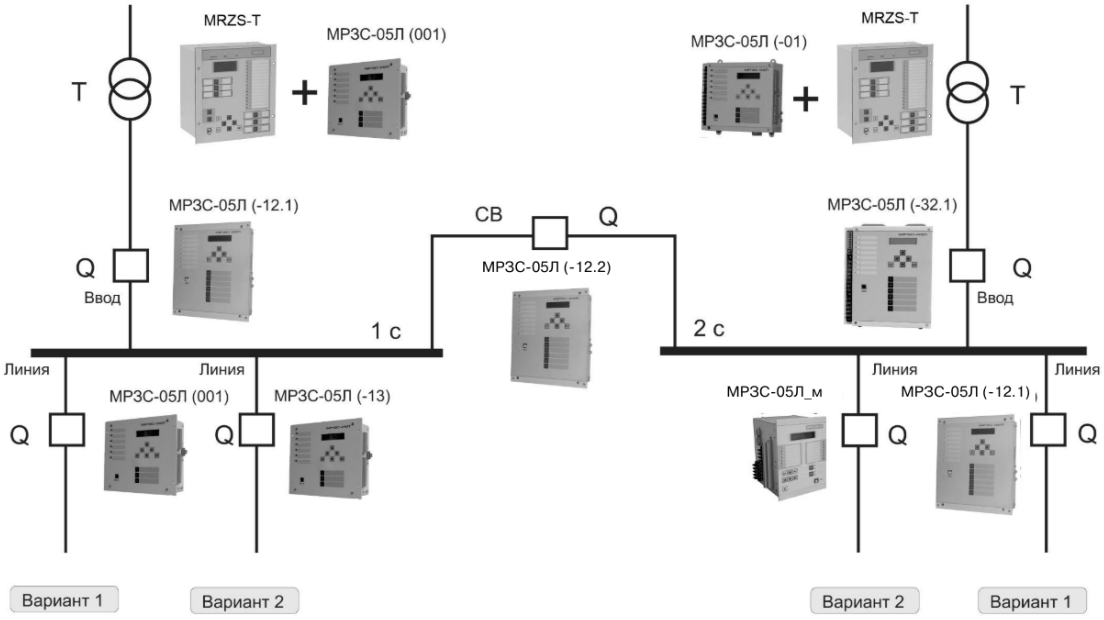


Рис. 1.3. Схема взаємодії МРЗС з іншими компонентами

Спрощена схема підключення МРЗС-05Л показана на малюнку 1.4:

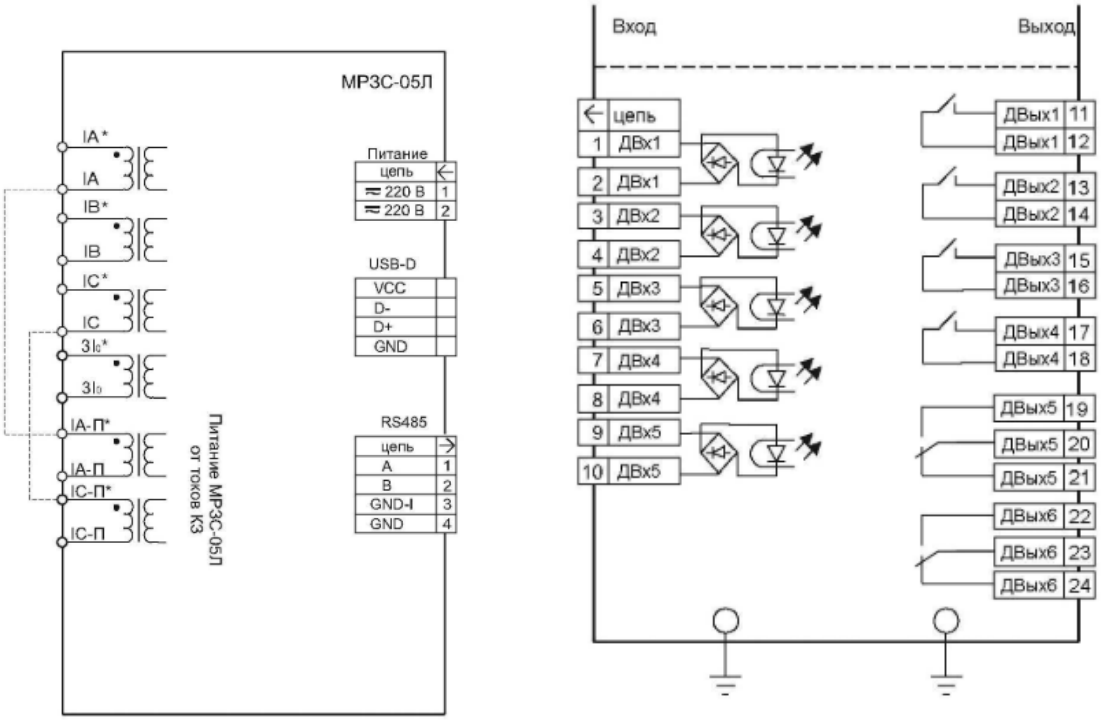


Рис. 1.4. Спрощена схема підключення МРЗС-05Л

Для оцінки ефективності роботи МРЗС використовуються різні математичні моделі та формули. Однією з важливих задач є визначення струму короткого замикання, який можна розрахувати за формулою:

$$I_{кз} = \frac{U}{Z_{кз}}, \qquad (1.3)$$

де $I_{кз}$- струм короткого замикання

U - напруга в мережі

$Z_{кз}$ - імпеданс короткого замикання

Для ілюстрації роботи МРЗС побудовано графік на малюнку 1.5 струму короткого замикання в залежності від часу, що показує, як швидко система виявляє та реагує на несправність.

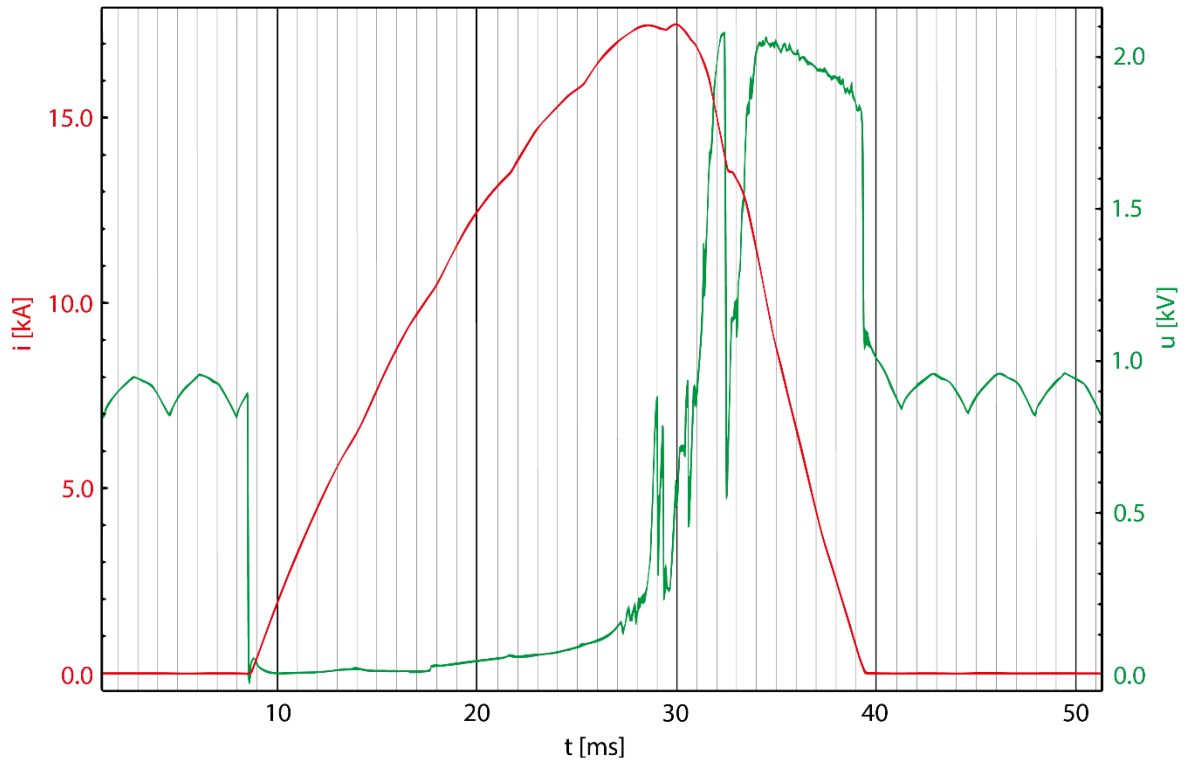


Рис. 1.5. Графік струму короткого замикання в залежності від часу

Спектральний аналіз є ще одним важливим інструментом для оцінки роботи МРЗС. Спектральний аналіз дозволяє визначити частотні компоненти струму або напруги, що може допомогти виявити несправності,

які не видно в часових діаграмах. Наприклад, частотний спектр сигналу може показати гармоніки, які вказують на наявність несправності.

Формула для спектрального аналізу може бути записана наступним чином:

$$X(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft}dt \qquad (1.4)$$

де *X(f)* - спектральна складова сигналу на частоті (f),

$x(t)$- часова функція сигналу

j – уявна одиниця

Спектр струму під час нормальної роботи та під час несправності можна побудувати для ілюстрації різниці в частотних компонентах.

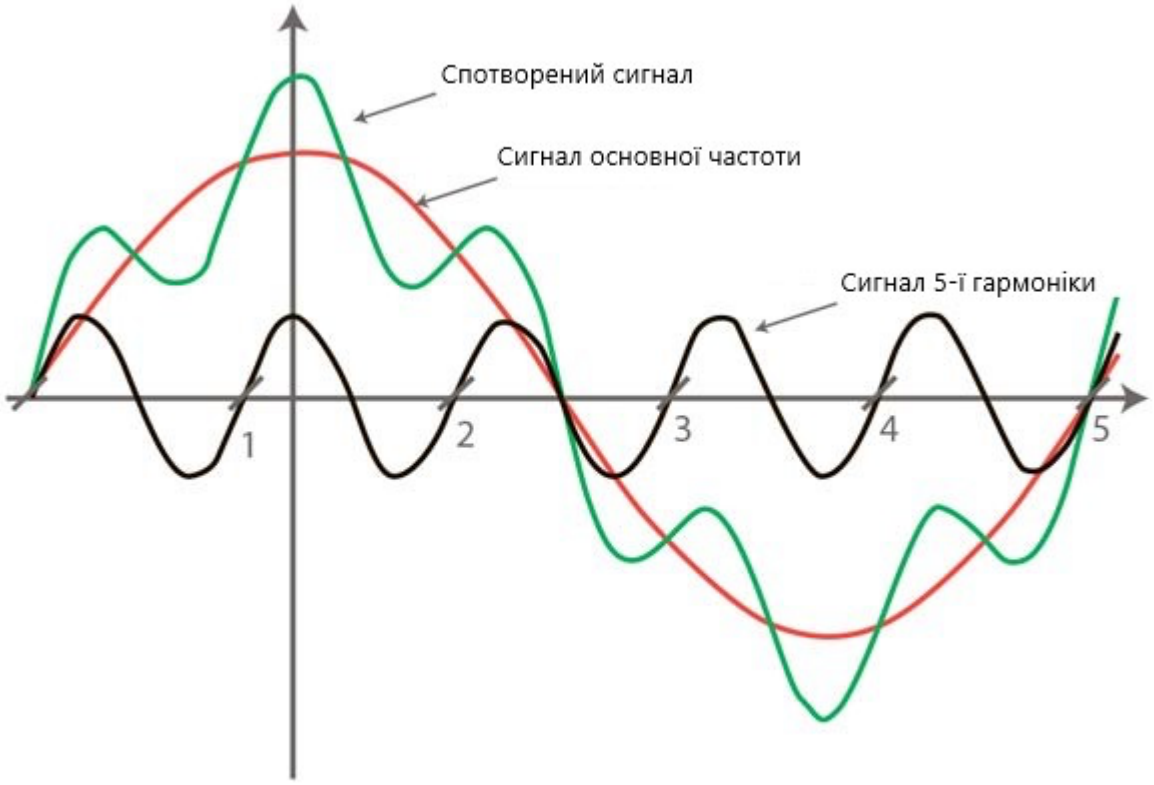


Рис. 1.6. Спектр струму під час нормальної роботи та під час несправності

Спектр струму під час нормальної роботи та під час несправності можна побудувати для ілюстрації різниці в частотних компонентах.

Додаткові аспекти роботи МРЗС включають:

**Адаптивний захист**: МРЗС можуть адаптуватися до змінних умов роботи мережі, автоматично коригуючи свої параметри захисту в залежності від поточної ситуації.

**Дистанційне управління**: Сучасні МРЗС можуть підтримувати дистанційне управління та моніторинг, що дозволяє операторам контролювати стан мережі з центрального диспетчерського пункту.

**Інтеграція з системами SCADA**: МРЗС можуть бути інтегровані в системи SCADA (Supervisory Control and Data Acquisition), що дозволяє забезпечити більш високий рівень автоматизації та контролю над електричними мережами.

Таким чином, МРЗС відіграють ключову роль у системі захисту електричних мереж, забезпечуючи високу надійність та ефективність роботи всієї системи. Їх взаємодія з іншими компонентами системи захисту та використання передових математичних методів дозволяють швидко та точно виявляти і усувати несправності, що підвищує загальну безпеку та надійність електричних мереж.

## 1.3. Структура та функції МРЗС

Мікропроцесорні релейні захисні системи (МРЗС) складаються з кількох основних компонентів, що взаємодіють між собою для забезпечення надійного та ефективного захисту електричних мереж. Основні компоненти МРЗС включають:

**Сенсори (датчики)**: Вимірюють параметри електричної мережі, такі як струм, напруга, частота тощо.

**Мікропроцесор**: Центральний обчислювальний блок, що обробляє дані від сенсорів та виконує алгоритми захисту.

**Комунікаційні модулі**: Забезпечують зв’язок між компонентами системи та з іншими зовнішніми системами.

**Інтерфейси користувача**: Дозволяють операторам взаємодіяти з системою, налаштовувати параметри та отримувати інформацію про стан системи.

**Електромеханічні реле**: Виконують команди мікропроцесора для відключення або переключення електричних ланцюгів.

Основні компоненти МРЗС можна детальніше розглянути таким чином:

**Сенсори (датчики)**: Використовуються для вимірювання параметрів електричної мережі, таких як струм, напруга, частота тощо. Вони можуть бути як аналоговими, так і цифровими. Сенсори відіграють ключову роль у зборі первинних даних для аналізу стану мережі. Аналогові сенсори зазвичай забезпечують високу точність вимірювань, тоді як цифрові сенсори мають перевагу у швидкості обробки даних.

**Мікропроцесор**: Це центральний обчислювальний блок системи, який обробляє дані від сенсорів та виконує алгоритми захисту. Мікропроцесори сучасних МРЗС часто багатоядерні, що забезпечує високу швидкість обробки даних і дозволяє паралельне виконання кількох завдань.

**Комунікаційні модулі**: Забезпечують зв’язок між компонентами системи та з іншими зовнішніми системами. Вони можуть використовувати різні протоколи передачі даних, такі як Ethernet, Modbus, DNP3 тощо. Це дозволяє інтегрувати МРЗС в загальну систему управління енергомережами.

**Інтерфейси користувача**: Дозволяють операторам взаємодіяти з системою, налаштовувати параметри та отримувати інформацію про стан системи. Інтерфейси можуть бути у вигляді локальних дисплеїв або віддалених робочих станцій з доступом до системи через мережу.

**Електромеханічні реле**: Виконують команди мікропроцесора для відключення або переключення електричних ланцюгів. Вони забезпечують фізичне роз'єднання ланцюгів у разі виявлення несправності.

МРЗС виконують кілька важливих функцій для забезпечення захисту електричних мереж:

1. **Виявлення несправностей**: МРЗС здатні швидко ідентифікувати різні типи несправностей, такі як короткі замикання, перевантаження, зниження напруги тощо. Це забезпечує своєчасне відключення пошкоджених ділянок мережі, що запобігає розповсюдженню аварійних ситуацій.

2. **Моніторинг і діагностика**: МРЗС забезпечують постійний моніторинг параметрів мережі і можуть проводити діагностику стану обладнання в режимі реального часу. Це дозволяє операторам своєчасно виявляти потенційні проблеми і вживати відповідних заходів для їх усунення.

3. **Автоматичне відключення**: У разі виявлення несправності МРЗС можуть автоматично відключати пошкоджені секції мережі для запобігання подальших пошкоджень. Це зменшує час відновлення після аварії та мінімізує ризик пошкодження обладнання.

4. **Адаптивний захист**: МРЗС можуть адаптуватися до змінних умов роботи мережі, автоматично коригуючи свої параметри захисту в залежності від поточної ситуації. Це дозволяє підвищити ефективність захисту та знизити кількість хибних спрацьовувань.

5. **Дистанційне управління**: Сучасні МРЗС можуть підтримувати дистанційне управління та моніторинг, що дозволяє операторам

контролювати стан мережі з центрального диспетчерського пункту. Це забезпечує можливість оперативного реагування на аварійні ситуації та дозволяє швидко приймати рішення.

6. **Інтеграція з системами SCADA**: МРЗС можуть бути інтегровані в системи SCADA (Supervisory Control and Data Acquisition), що дозволяє забезпечити більш високий рівень автоматизації та контролю над електричними мережами. Це забезпечує комплексний підхід до управління та моніторингу енергосистем.

Існує кілька основних типів МРЗС, які використовуються в сучасних електричних мережах:

1. **Цифрові реле**: Використовують цифрові сигнали та алгоритми для обробки даних і прийняття рішень. Вони відрізняються високою точністю і швидкодією.
2. **Аналогові реле**: Використовують аналогові сигнали для обробки даних. Хоча вони менш точні, ніж цифрові реле, вони можуть бути корисні в деяких специфічних застосуваннях.
3. **Гібридні реле**: Поєднують в собі характеристики як цифрових, так і аналогових реле, забезпечуючи високу точність і гнучкість.

Переваги використання МРЗС включають:

**Висока точність і швидкодія**: МРЗС забезпечують швидке і точне виявлення несправностей, що дозволяє мінімізувати пошкодження обладнання і зменшити час простою.

**Гнучкість і адаптивність**: МРЗС можуть бути налаштовані для роботи в різних умовах і можуть адаптуватися до змін у мережі.

**Інтеграція з іншими системами**: МРЗС можуть бути інтегровані з системами SCADA та іншими системами управління, що забезпечує комплексний підхід до захисту і управління мережею.

Недоліки включають:

**Висока вартість**: Впровадження і обслуговування МРЗС може бути дорожчим порівняно з традиційними реле.

**Складність налаштування**: Налаштування і управління МРЗС вимагає високої кваліфікації і спеціальних знань.

**Чутливість до зовнішніх впливів**: МРЗС можуть бути чутливими до зовнішніх електромагнітних перешкод і умов навколишнього середовища.

Для ілюстрації функцій МРЗС можна використовувати різні математичні моделі та графіки. Наприклад, для оцінки ефективності алгоритмів виявлення несправностей можна використовувати такі рівняння:

1. Рівняння для визначення миттєвого значення струму

$$I(t)=I_0 sin(\omega t + \varphi) \quad (1.5)$$

де I(t) – струм в мережі

$I_0$ - амплітуда струму

$\omega$- кутова частота

$\varphi$- початкова фаза

2. Формула для спектрального аналізу

$$X(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft}dt \quad (1.6)$$

де $X(f)$ - спектральна складова сигналу на частоті (f),

$x(t)$- часова функція сигналу

j – уявна одиниця

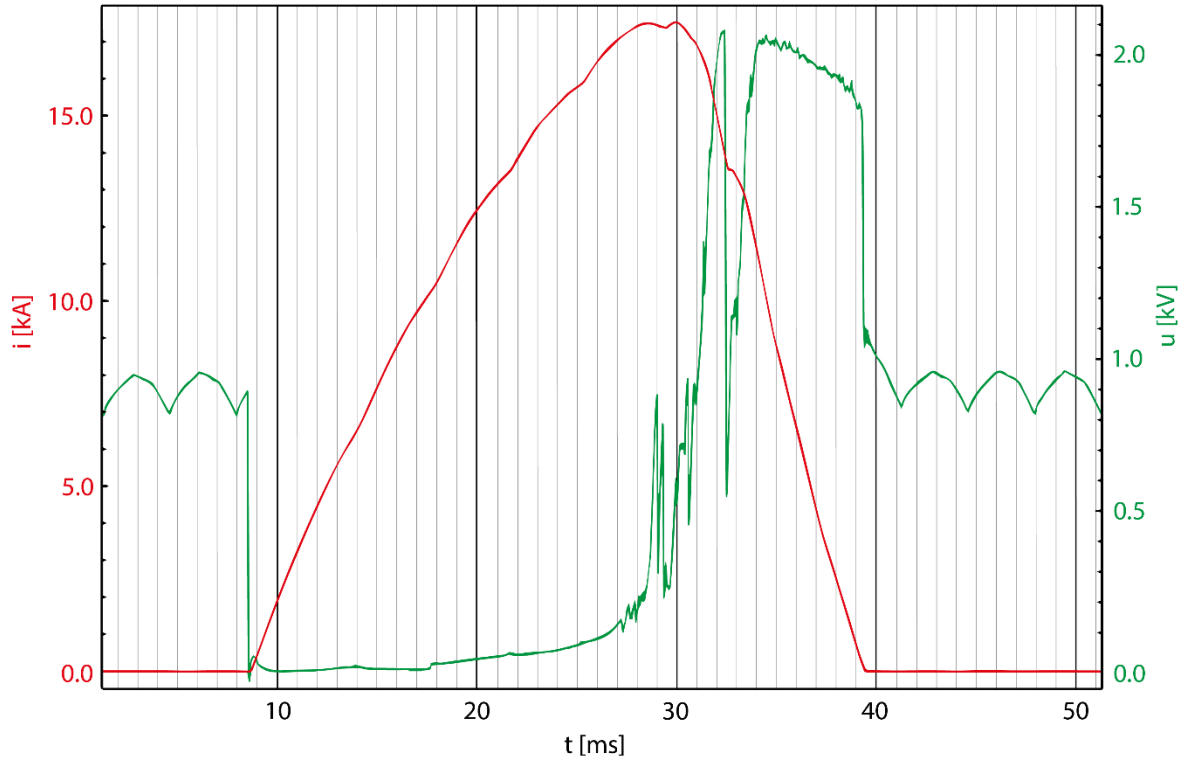


Рис. 1.7 Графік струму короткого замикання в залежності від часу

**Спектральний аналіз сигналу**:

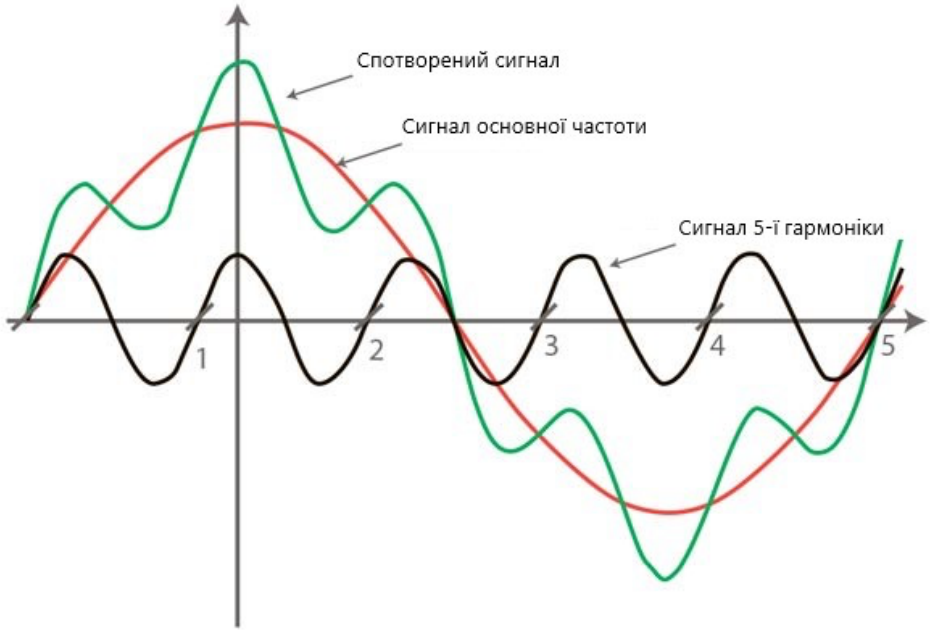


Рис. 1.8.Гграфік спектрального аналізу сигналу

МРЗС також забезпечують функції відновлення після аварійних ситуацій. Після виявлення і відключення несправної секції, система може автоматично перевіряти стан мережі і відновлювати нормальну роботу після усунення несправності. Це значно зменшує час простою і підвищує загальну надійність системи.

Сучасні МРЗС включають функцію самодіагностики, яка дозволяє виявляти внутрішні несправності в самій системі реле. Це забезпечує високу надійність роботи і дозволяє своєчасно виявляти і усувати внутрішні проблеми в системі.

МРЗС використовують різні протоколи комунікації для інтеграції з іншими системами і компонентами. Основні протоколи включають:

**Modbus**: Широко використовуваний протокол для передачі даних між електронними пристроями.

**DNP3 (Distributed Network Protocol)**: Протокол, розроблений для комунікації в енергомережах, що забезпечує високу надійність і захищеність даних.

**IEC 61850**: Міжнародний стандарт для комунікації в енергетичних системах, який забезпечує сумісність між різними виробниками обладнання.

МРЗС можуть бути інтегровані в системи SCADA (Supervisory Control and Data Acquisition), що дозволяє забезпечити більш високий рівень автоматизації та контролю над електричними мережами. Це забезпечує комплексний підхід до управління та моніторингу енергосистем, дозволяючи операторам отримувати реальну картину стану мережі в режимі реального часу.

МРЗС також можуть бути інтегровані з системами автоматизації підстанцій, що дозволяє автоматично керувати процесами на підстанціях, зменшуючи потребу в ручному втручанні і підвищуючи загальну ефективність роботи.

МРЗС використовуються для захисту трансформаторів від перевантажень, коротких замикань і інших несправностей. Вони можуть швидко виявляти несправності і відключати трансформатори для запобігання пошкодженням.

МРЗС забезпечують захист ліній електропередач, виявляючи несправності на лініях і автоматично відключаючи пошкоджені секції. Це допомагає запобігти поширенню аварійних ситуацій і мінімізувати втрати електроенергії[3].

МРЗС також використовуються для захисту генераторів від перевантажень, коротких замикань і інших несправностей. Вони забезпечують своєчасне виявлення проблем і відключення генераторів для запобігання серйозним пошкодженням.

Мікропроцесорні релейні захисні системи (МРЗС) забезпечують високу надійність і ефективність захисту електричних мереж. Вони відрізняються високою точністю, швидкодією і гнучкістю, що дозволяє їм адаптуватися до змінних умов роботи мережі. МРЗС забезпечують комплексний підхід до захисту і управління енергосистемами, забезпечуючи інтеграцію з іншими системами і компонентами. Використання сучасних алгоритмів і протоколів комунікації дозволяє забезпечити високу надійність і ефективність роботи МРЗС, що робить їх незамінними в сучасних енергосистемах.

## 1.4. Огляд МРЗС, які типи є, які МРЗС зараз виробляють

Сучасні МРЗС є важливим компонентом сучасних електричних мереж, забезпечуючи високу надійність і ефективність захисту. Вони використовують передові технології обробки сигналів, що дозволяє

забезпечити точне і швидке виявлення несправностей. Сучасні МРЗС включають в себе різні типи реле, які можна класифікувати за кількома ознаками.

**Типи МРЗС**

1. **Цифрові реле**

   **Переваги**: Висока точність, швидкодія, можливість програмування, гнучкість налаштувань.

   **Недоліки**: Вища вартість у порівнянні з аналоговими реле, складність налаштування.

   **Приклади використання**: Захист трансформаторів, ліній електропередач, генераторів.

   **Виробники**: ABB, Siemens, Schneider Electric.

2. **Аналогові реле**

   **Переваги**: Простота конструкції, надійність в екстремальних умовах, відносно низька вартість.

   **Недоліки**: Менша точність у порівнянні з цифровими реле, обмежені можливості налаштування.

   **Приклади використання**: Захист простих систем, резервні реле.

   **Виробники**: General Electric, Mitsubishi Electric.

3. **Гібридні реле**

**Переваги**: Поєднання переваг цифрових і аналогових реле, висока надійність, гнучкість налаштувань.

**Недоліки**: Складність конструкції, вища вартість у порівнянні з аналоговими реле.

**Приклади використання**: Комплексні системи захисту, промислові застосування.

**Виробники**: Alstom, Eaton.

Сучасні МРЗС мають ряд ключових технічних характеристик, які визначають їх ефективність та надійність:

**Чутливість**: Можливість виявляти малі відхилення параметрів мережі.

**Швидкодія**: Час реакції на несправність, який може бути менше кількох мілісекунд.

**Надійність**: Довговічність роботи в екстремальних умовах, висока стійкість до зовнішніх перешкод.

**Гнучкість налаштувань**: Можливість програмування під різні умови роботи та типи мереж.

**Інтерфейси комунікації**: Підтримка різних протоколів для інтеграції з іншими системами.

**Приклади сучасних МРЗС**

1. **ABB Relion Series**

**Опис**: Лінійка цифрових реле, призначених для захисту і управління електричними мережами.

**Функції**: Захист від перевантажень, коротких замикань, контроль напруги, дистанційне управління.

**Технічні характеристики**: Швидкодія до 10 мс, підтримка протоколів IEC 61850, Modbus, DNP3.

Рис. 1.9. Зображення ABB Relion

2. **Siemens SIPROTEC 5**

**Опис**: Модульні цифрові реле для комплексного захисту, автоматизації і моніторингу енергосистем.

**Функції**: Захист трансформаторів, ліній електропередач, генераторів, контроль якості електроенергії.

**Технічні характеристики**: Час реакції до 5 мс, підтримка протоколів IEC 61850, PROFINET, Ethernet.

Рис. 1.10.З*ображення Siemens SIPROTEC 5*

3. **Schneider Electric MiCOM P40**

**Опис**: Реле для захисту та управління енергосистемами з розширеними можливостями моніторингу.

**Функції**: Захист ліній, трансформаторів, генераторів, моніторинг параметрів мережі.

**Технічні характеристики**: Швидкодія до 8 мс, підтримка протоколів IEC 61850, Modbus, DNP3.

Рис. 1.11. Зображення Schneider Electric MiCOM P40

Сучасний ринок МРЗС представлений численними виробниками, які пропонують різні рішення для захисту та управління електричними мережами. Серед найбільш відомих виробників можна виділити:

1. **ABB**

**Опис**: Швейцарсько-шведська компанія, один з лідерів у галузі енергетики та автоматизації.

**Продукти**: Серії реле Relion, REX, REF, які забезпечують комплексний захист і управління енергосистемами.

**Технічні характеристики**: Висока точність, швидкодія, підтримка сучасних протоколів комунікації.

2. **Siemens**

**Опис**: Німецька компанія, провідний постачальник технологій для енергетики та автоматизації.

**Продукти**: Лінійка реле SIPROTEC, які забезпечують захист і автоматизацію енергосистем різної складності.

**Технічні характеристики**: Модульність, гнучкість налаштувань, висока надійність.

3. **Schneider Electric**

**Опис**: Французька компанія, один з найбільших виробників електротехнічного обладнання та систем автоматизації.

**Продукти**: Серія реле MiCOM, що пропонує широкий спектр рішень для захисту і управління енергосистемами.

**Технічні характеристики**: Висока точність, швидкодія, інтеграція з системами SCADA.

4. **General Electric (GE)**

**Опис**: Американська компанія, провідний постачальник технологій для енергетики, транспорту та промисловості.

**Продукти**: Серія реле Multilin, що забезпечує захист і автоматизацію енергосистем різного масштабу.

**Технічні характеристики**: Надійність, гнучкість налаштувань, підтримка сучасних протоколів комунікації.

**Хмарні технології**: Використання хмарних сервісів для зберігання і обробки даних дозволяє забезпечити більш високий рівень безпеки і доступності інформації. Це також забезпечує можливість віддаленого доступу до даних і управління системою з будь-якої точки світу. Високий рівень доступності хмарних рішень дозволяє швидко відновити роботу після збоїв та зберегти всі важливі дані.

**Кібербезпека**: Сучасні МРЗС включають вдосконалені засоби кібербезпеки для захисту від зовнішніх загроз і несанкціонованого доступу. Це включає шифрування даних, автентифікацію користувачів і моніторинг підозрілої активності. Завдяки цьому забезпечується надійний захист системи від кібератак, що стає все більш актуальним у сучасному світі[4].

**Адаптивний захист**: Інтеграція адаптивних алгоритмів дозволяє МРЗС автоматично змінювати свої параметри у відповідь на зміни в мережі, що забезпечує більш точний і ефективний захист. Це дозволяє зменшити кількість хибних спрацьовувань і підвищити загальну надійність системи.

МРЗС можуть бути інтегровані з іншими системами, що забезпечує комплексний підхід до управління і захисту електричних мереж. Це включає інтеграцію з:

**Системами SCADA**: Забезпечує централізоване управління і моніторинг енергосистем у режимі реального часу. Системи SCADA дозволяють операторам отримувати дані про стан мережі, аналізувати їх і приймати оперативні рішення для забезпечення безпеки та ефективності роботи.

**Системами автоматизації підстанцій**: Дозволяє автоматизувати процеси на підстанціях, підвищуючи ефективність і надійність роботи. Інтеграція з системами автоматизації підстанцій забезпечує більш точний контроль за параметрами мережі і швидке реагування на аварійні ситуації.

**Системами управління енергомережами**: Забезпечує оптимізацію розподілу навантаження і підвищення загальної ефективності

енергосистем. Інтеграція з системами управління енергомережами дозволяє забезпечити балансування навантаження і зменшити ризик перевантажень.

Технології МРЗС постійно розвиваються, і в майбутньому можна очікувати ще більших покращень і нововведень. Деякі з ключових тенденцій включають:

**Подальше впровадження штучного інтелекту**: Використання ШІ для більш точного прогнозування несправностей і оптимізації роботи енергосистем. ШІ дозволяє аналізувати великі обсяги даних і робити прогнози щодо можливих несправностей, що підвищує надійність системи.

**Розширення використання IoT**: Інтеграція більшої кількості пристроїв і сенсорів для забезпечення більш детального моніторингу і управління. IoT дозволяє створювати більш комплексні і точні системи моніторингу, що забезпечує оперативне виявлення і реагування на проблеми.

**Розвиток хмарних технологій**: Збільшення використання хмарних рішень для зберігання, обробки і аналізу даних. Хмарні технології дозволяють знизити витрати на інфраструктуру і забезпечують високу доступність даних.

**Підвищення рівня кібербезпеки**: Впровадження нових методів і технологій для захисту від кіберзагроз. З розвитком цифрових технологій, захист від кіберзагроз стає все більш важливим аспектом забезпечення безпеки енергосистем.

МРЗС знайшли широке застосування у різних галузях, забезпечуючи надійний захист і ефективне управління електричними мережами. Деякі з ключових областей застосування включають:

**Енергетика**: МРЗС використовуються для захисту і управління енергосистемами, забезпечуючи надійне постачання електроенергії.

**Промисловість**: МРЗС застосовуються для захисту електрообладнання на промислових підприємствах, запобігаючи аваріям і забезпечуючи безперервність виробничих процесів.

**Транспорт**: МРЗС використовуються для захисту електричних систем на залізничному транспорті, метро та інших видах транспорту, забезпечуючи безпеку і надійність перевезень.

**Комунальні послуги**: МРЗС застосовуються у водо- та теплопостачанні для захисту і управління електричними мережами комунальних підприємств.

Мікропроцесорні релейні захисні системи (МРЗС) забезпечують високу надійність і ефективність захисту електричних мереж. Вони відрізняються високою точністю, швидкодією і гнучкістю, що дозволяє їм адаптуватися до змінних умов роботи мережі. МРЗС забезпечують комплексний підхід до захисту і управління енергосистемами, забезпечуючи інтеграцію з іншими системами і компонентами. Використання сучасних алгоритмів і протоколів комунікації дозволяє забезпечити високу надійність і ефективність роботи МРЗС, що робить їх незамінними в сучасних енергосистемах.

# РОЗДІЛ 2
# ПРАКТИЧНА ЧАСТИНА

## 2.1. Основні вимоги до приладів релейного захисту

Релейний захист є критичним компонентом електроенергетичних систем, який забезпечує надійність і безпеку роботи мережі. Прилади релейного захисту повинні відповідати ряду вимог, які забезпечують їх ефективну роботу в різних умовах.

1. Надійність

Опис: Прилади релейного захисту повинні працювати надійно в усіх умовах експлуатації, забезпечуючи безперервний захист електричних мереж.

Приклади: Відсутність помилкових спрацьовувань, здатність витримувати вплив зовнішніх факторів, таких як температурні коливання, вологість і електромагнітні перешкоди.

Реалізація: Високоякісні компоненти, регулярні випробування та сертифікація за міжнародними стандартами.

2. Швидкодія

Опис: Прилади релейного захисту повинні забезпечувати мінімальний час реакції на несправності для швидкого відключення пошкоджених ділянок мережі.

Приклади: Час реакції менше кількох мілісекунд для миттєвого відключення при короткому замиканні.

Реалізація: Використання сучасних мікропроцесорних технологій, оптимізація алгоритмів обробки сигналів.

3. Чутливість

Опис: Прилади релейного захисту повинні мати високу чутливість для виявлення навіть незначних відхилень параметрів мережі, які можуть свідчити про початок несправності.

Приклади: Здатність виявляти малі зміни в струмі або напрузі, що перевищують встановлені пороги.

Реалізація: Налаштування порогових значень, використання високоточних сенсорів.

4. Селективність

Опис: Прилади релейного захисту повинні забезпечувати селективність, тобто здатність відключати тільки пошкоджену ділянку мережі, залишаючи інші частини мережі в робочому стані.

Приклади: Застосування алгоритмів селективного захисту для мінімізації впливу на непошкоджені секції мережі.

Реалізація: Використання зональних захистів, координація з іншими приладами релейного захисту.

5. Стабільність

Опис: Прилади релейного захисту повинні зберігати стабільну роботу при змінних умовах експлуатації, таких як коливання навантаження і зовнішні перешкоди.

Приклади: Висока стійкість до змін напруги та частоти, здатність працювати в умовах нестабільного енергопостачання.

Реалізація: Стійка електроніка, спеціальні алгоритми обробки даних.

6. Гнучкість налаштувань

Опис: Прилади релейного захисту повинні мати можливість гнучкого налаштування для адаптації до різних умов експлуатації та вимог захисту.

Приклади: Підтримка програмованих налаштувань, можливість оновлення програмного забезпечення, інтеграція з іншими системами захисту.

Реалізація: Інтерфейси для програмування, підтримка стандартів протоколів комунікації.

Для забезпечення відповідності вимогам прилади релейного захисту повинні відповідати міжнародним стандартам і нормативам. Основні стандарти включають:

1. Міжнародний електротехнічний комісійний стандарт (IEC) 60255

Опис: Стандарт IEC 60255 встановлює вимоги до характеристик, випробувань і функцій релейного захисту. Він охоплює різні аспекти, включаючи надійність, швидкодію, чутливість і селективність[5].

2. IEEE C37.90

Опис: Стандарт IEEE C37.90 охоплює вимоги до релейних пристроїв, включаючи випробування на витривалість, швидкодію і стійкість до електромагнітних перешкод.

3. ГОСТ Р 50030

Опис: Російський стандарт, який регламентує технічні вимоги до релейного захисту в енергетичних системах. Він включає вимоги до надійності, швидкодії та інших ключових характеристик.

Для оцінки ефективності приладів релейного захисту використовуються різні математичні моделі та формули. Наприклад, для розрахунку часу реакції приладу можна використовувати наступну формулу:

$$t_p = \frac{K}{I_з} \qquad (2.1)$$

де $t_p$- час реакції

$K$ – коефіцієнт налаштування

$I_з$ - струм замикання

Графік залежності часу реакції від струму замикання дозволяє оцінити швидкодію приладу в різних умовах

Для оцінки чутливості приладів релейного захисту використовується формула:

$$S=\frac{\Delta I}{I_{ном}} \quad (2.2)$$

де S – чутливість

$\Delta I$ – зміна струму

$I_{ном}$ – номінальний струм

Прилади релейного захисту повинні мати високу теплову стійкість, щоб витримувати перевантаження і температурні коливання без втрати ефективності.

**Опис**: Теплова стійкість забезпечує здатність приладів працювати при високих температурах, що виникають внаслідок великих струмів або зовнішніх умов.

**Приклади**: Використання спеціальних матеріалів, які мають високу стійкість до нагріву, і систем охолодження для запобігання перегріву.

Прилади релейного захисту повинні бути стійкими до електромагнітних перешкод, які можуть впливати на їх роботу.

**Опис**: Електромагнітна сумісність забезпечує здатність приладів працювати в умовах впливу електромагнітних полів без втрати функціональності.

**Приклади**: Використання екранування, фільтрів і схем захисту для зменшення впливу електромагнітних перешкод.

Прилади релейного захисту повинні мати високу механічну стійкість, щоб витримувати фізичні впливи, такі як вібрації, удари і механічні навантаження.

**Опис**: Механічна стійкість забезпечує здатність приладів працювати в умовах підвищених механічних навантажень без пошкоджень.

**Приклади**: Використання міцних матеріалів і конструкцій, які можуть витримувати високі механічні навантаження.

Прилади релейного захисту повинні бути захищені від впливу вологи і пилу, що можуть проникати всередину і викликати корозію або короткі замикання.

**Опис**: Захист від вологи і пилу забезпечує довготривалу надійність роботи приладів у несприятливих умовах навколишнього середовища.

Приклади: Використання герметичних корпусів з високим ступенем захисту (IP), спеціальних покриттів для захисту електронних компонентів від корозії.

Сучасні прилади релейного захисту повинні мати інтегровані інтерфейси для передачі даних і взаємодії з іншими системами.

Опис: Наявність різноманітних інтерфейсів комунікації забезпечує можливість інтеграції приладів релейного захисту в складні системи управління та моніторингу.

Приклади: Підтримка протоколів Modbus, DNP3, IEC 61850, Ethernet для забезпечення сумісності з іншими пристроями та системами.

Прилади релейного захисту повинні бути зручними в установці, налаштуванні та експлуатації.

Опис: Ергономічний дизайн та інтуїтивно зрозумілий інтерфейс полегшують процес встановлення, налаштування і обслуговування приладів.

Приклади: Наявність зрозумілих інструкцій, програмного забезпечення для налаштування, інтуїтивно зрозумілих дисплеїв і кнопок управління.

Розширюваність та модульність

Прилади релейного захисту повинні мати можливість розширення і модульної конструкції для адаптації до змінних умов і вимог.

Опис: Модульна конструкція забезпечує можливість додавання або заміни компонентів для розширення функціональності або адаптації до нових умов експлуатації.

Приклади: Використання змінних модулів, підтримка різних конфігурацій та оновлення програмного забезпечення.

Вимоги до приладів релейного захисту є багатогранними і включають надійність, швидкодію, чутливість, селективність, стабільність, гнучкість налаштувань, теплову та механічну стійкість, електромагнітну сумісність, захист від вологи і пилу, інтеграцію комунікаційних інтерфейсів, ергономіку та зручність використання, розширюваність та модульність. Відповідність цим вимогам забезпечує ефективну і надійну роботу приладів релейного захисту в сучасних електроенергетичних системах[5].

Приклади стандартів та їх вимоги

1. IEC 60255: Встановлює вимоги до релейного захисту, включаючи функціональні характеристики, випробування на стійкість до електромагнітних перешкод, механічну стійкість та надійність.

Випробування на стійкість до електромагнітних перешкод: Забезпечують здатність приладів працювати в умовах впливу електромагнітних полів без втрати функціональності.

Механічна стійкість: Випробування на стійкість до вібрацій, ударів і механічних навантажень.

2. IEEE C37.90: Охоплює вимоги до релейних пристроїв, включаючи випробування на витривалість, швидкодію і стійкість до електромагнітних перешкод.

Випробування на витривалість: Перевірка здатності приладів працювати при високих температурах і великих струмах.

Швидкодія: Вимірювання часу реакції на несправності.

3. ГОСТ Р 50030: Російський стандарт, який регламентує технічні вимоги до релейного захисту в енергетичних системах.

Надійність: Перевірка відсутності помилкових спрацьовувань і здатності витримувати зовнішні впливи.

Селективність: Забезпечення відключення тільки пошкоджених ділянок мережі.

Для оцінки ефективності приладів релейного захисту використовуються різні математичні моделі та формули.

Розрахунок часу реакції:

$$t_p = \frac{K}{I_з} \quad (2.3)$$

де $t_p$- час реакції

$K$ – коефіцієнт налаштування

$I_з$ - струм замикання

Оцінка чутливості:

$$S=\frac{\Delta I}{I_{ном}} \quad (2.4)$$

де S – чутливість

$\Delta I$ – зміна струму

$I_{ном}$ – номінальний струм

Тобто, основні вимоги до приладів релейного захисту включають надійність, швидкодію, чутливість, селективність, стабільність, гнучкість налаштувань, теплову та механічну стійкість, електромагнітну сумісність, захист від вологи і пилу, інтеграцію комунікаційних інтерфейсів, ергономіку та зручність використання, розширюваність та модульність. Відповідність цим вимогам забезпечує ефективну і надійну роботу приладів релейного захисту в сучасних електроенергетичних системах.

## 2.2. Огляд спроможностей приладів сучасного релейного захисту

Сучасні прилади релейного захисту (ПРЗ) значно перевершують своїх попередників завдяки впровадженню новітніх технологій та інновацій. Вони забезпечують високий рівень надійності, точності та швидкодії, що дозволяє ефективно захищати електричні мережі від різних видів несправностей.

1. **Мікропроцесорні технології**

**Опис**: Використання мікропроцесорних технологій дозволяє реалізувати складні алгоритми захисту та обробки сигналів у реальному часі.

**Приклади**: Мікропроцесорні реле здатні виявляти несправності з високою точністю і мінімальною затримкою.

**Переваги**: Висока швидкодія, точність, можливість програмування та гнучкість налаштувань.

2. **Дистанційне управління та моніторинг**

**Опис**: Сучасні ПРЗ підтримують функції дистанційного управління та моніторингу, що дозволяє операторам контролювати та налаштовувати прилади з будь-якого місця.

**Приклади**: Використання SCADA-систем для централізованого управління та моніторингу стану мережі.

**Переваги**: Підвищення оперативності реагування, зменшення потреби у фізичній присутності на об’єкті.

3. **Інтеграція з іншими системами**

**Опис**: ПРЗ можуть бути інтегровані з іншими системами захисту, автоматизації та управління для забезпечення комплексного підходу до захисту мереж.

**Приклади**: Інтеграція з системами SCADA, автоматизації підстанцій, управління енергомережами.

**Переваги**: Підвищення ефективності управління, зниження ризику помилок, комплексний підхід до захисту.

4. **Автоматичне відновлення після несправностей**

**Опис**: Сучасні ПРЗ підтримують функції автоматичного відновлення після несправностей, що дозволяє швидко повертати мережу до нормального стану після аварій.

**Приклади**: Використання автоматичних перемикачів для швидкого відновлення живлення.

**Переваги**: Зменшення тривалості відключень, підвищення надійності постачання електроенергії.

5. **Адаптивний захист**

**Опис**: Адаптивний захист дозволяє ПРЗ автоматично налаштовувати свої параметри у відповідь на зміни в мережі, забезпечуючи оптимальний рівень захисту.

**Приклади**: Зміна налаштувань у режимі реального часу в залежності від поточного стану мережі.

**Переваги**: Підвищення точності і надійності захисту, зниження ризику хибних спрацьовувань.

6. **Висока точність і чутливість**

**Опис**: Сучасні ПРЗ забезпечують високу точність і чутливість, що дозволяє виявляти навіть найменші відхилення від нормальних параметрів.

**Приклади**: Виявлення мікрозамикань, перевантажень, зниження напруги.

**Переваги**: Запобігання великим аваріям завдяки своєчасному виявленню і усуненню несправностей.

7. **Механізми самодіагностики**

**Опис**: Механізми самодіагностики дозволяють ПРЗ самостійно перевіряти свій стан і виявляти внутрішні несправності.

**Приклади**: Регулярні самоперевірки, індикація стану приладу, автоматичне повідомлення про несправності.

**Переваги**: Підвищення надійності роботи, своєчасне виявлення і усунення внутрішніх проблем.

**Приклади сучасних ПРЗ**

1. **ABB Relion® Series**

**Опис**: Лінійка цифрових реле для захисту і управління електричними мережами.

**Функції**: Захист від перевантажень, коротких замикань, контроль напруги, дистанційне управління.

**Технічні характеристики**: Швидкодія до 10 мс, підтримка протоколів IEC 61850, Modbus, DNP3.

2. **Siemens SIPROTEC 5**

**Опис**: Модульні цифрові реле для комплексного захисту, автоматизації і моніторингу енергосистем.

**Функції**: Захист трансформаторів, ліній електропередач, генераторів, контроль якості електроенергії.

**Технічні характеристики**: Час реакції до 5 мс, підтримка протоколів IEC 61850, PROFINET, Ethernet.

3. **Schneider Electric MiCOM P40**

**Опис**: Реле для захисту та управління енергосистемами з розширеними можливостями моніторингу.

**Функції**: Захист ліній, трансформаторів, генераторів, моніторинг параметрів мережі.

**Технічні характеристики**: Швидкодія до 8 мс, підтримка протоколів IEC 61850, Modbus, DNP3.

Для оцінки ефективності роботи сучасних ПРЗ використовуються різні математичні моделі та формули.

$$t_p = \frac{K}{I_з} \qquad (2.6)$$

де $t_p$- час реакції

$K$ – коефіцієнт налаштування

$I_з$ - струм замикання

3. Формула для оцінки точності:

$$E = \frac{\Delta P}{P_{ном}} \quad (2.7)$$

Де E – точність

$\Delta P$ – зміна параметра

$P_{ном}$ – номінальний параметр

**Майбутні напрямки розвитку**

Сучасні ПРЗ продовжують розвиватися, інтегруючи нові технології та підходи для підвищення ефективності та надійності роботи. Майбутні напрямки розвитку включають:

1. **Інтеграція штучного інтелекту**

**Опис**: Використання алгоритмів штучного інтелекту для покращення виявлення несправностей і оптимізації параметрів захисту.

**Приклади**: Машинне навчання для прогнозування можливих несправностей, адаптивні алгоритми, що підлаштовуються під змінні умови мережі.

**Переваги**: Підвищення точності та ефективності, зменшення кількості хибних спрацьовувань, оптимізація процесів обслуговування та ремонту.

2. **Розширене використання Інтернету речей (IoT)**

**Опис**: Інтеграція приладів релейного захисту в екосистему IoT для забезпечення більш детального моніторингу та управління.

**Приклади**: Використання сенсорів для збору даних у реальному часі, інтеграція з хмарними платформами для аналізу даних.

**Переваги**: Покращений моніторинг стану мережі, оперативне виявлення несправностей, зниження витрат на обслуговування[6].

3. **Розвиток хмарних технологій**

**Опис**: Використання хмарних сервісів для зберігання, обробки та аналізу даних з приладів релейного захисту.

**Приклади**: Хмарні платформи для централізованого управління, аналіз даних у реальному часі, віддалене оновлення програмного забезпечення.

**Переваги**: Зниження витрат на інфраструктуру, підвищення доступності та безпеки даних, можливість віддаленого управління.

4. **Підвищення рівня кібербезпеки**

**Опис**: Впровадження нових методів і технологій для захисту від кіберзагроз, що стають все більш актуальними у цифровому світі.

**Приклади**: Шифрування даних, автентифікація користувачів, системи моніторингу та виявлення підозрілої активності.

**Переваги**: Захист від несанкціонованого доступу, зменшення ризику кібератак, забезпечення безпеки і стабільності роботи мережі.

5. **Розширення функціональності адаптивного захисту**

**Опис**: Подальший розвиток функцій адаптивного захисту, що дозволяє приладам автоматично підлаштовувати свої параметри відповідно до змінних умов мережі.

**Приклади**: Автоматичне регулювання налаштувань у реальному часі, інтеграція з іншими системами для комплексного управління.

**Переваги**: Підвищення ефективності захисту, зниження ризику хибних спрацьовувань, оптимізація роботи мережі.

Сучасні прилади релейного захисту забезпечують високий рівень надійності, точності та швидкодії, що дозволяє ефективно захищати електричні мережі від різних видів несправностей. Завдяки впровадженню новітніх технологій, таких як мікропроцесорні системи, дистанційне управління та моніторинг, інтеграція з іншими системами, автоматичне відновлення після несправностей, адаптивний захист, висока точність і чутливість, механізми самодіагностики, сучасні ПРЗ значно підвищують рівень безпеки і стабільності енергосистем[6].

Майбутні напрямки розвитку ПРЗ включають інтеграцію штучного інтелекту, розширене використання Інтернету речей, розвиток хмарних технологій, підвищення рівня кібербезпеки, розширення функціональності адаптивного захисту, що забезпечить ще більшу ефективність і надійність роботи електричних мереж у майбутньому.

## 2.3. Принцип роботи МРЗС

Мікропроцесорні релейні захисні системи (МРЗС) використовуються для забезпечення надійного і ефективного захисту електричних мереж від різноманітних несправностей. Принцип роботи МРЗС базується на використанні сучасних мікропроцесорних технологій, які забезпечують високу точність, швидкодію і гнучкість налаштувань.

1. Вимірювання параметрів мережі

Опис: МРЗС постійно вимірюють основні параметри електричної мережі, такі як струм, напруга, частота та інші важливі величини. Вимірювання виконуються за допомогою високоточних сенсорів і трансформаторів струму та напруги.

Приклади: Трансформатори струму (CT) і напруги (VT) передають дані про параметри електричної мережі на мікропроцесор для подальшого аналізу.

2. Аналіз та обробка сигналів

Опис: Зібрані дані надходять до мікропроцесора, де вони аналізуються і обробляються за допомогою спеціальних алгоритмів. Обробка сигналів включає фільтрацію шумів, перетворення сигналів і виявлення аномалій.

Приклади: Використання алгоритмів спектрального аналізу для виявлення аномалій у сигналах, таких як гармонічні спотворення або різкі зміни струму.

3. Виявлення несправностей

Опис: На основі аналізу сигналів МРЗС визначають наявність несправностей у мережі, таких як короткі замикання, перевантаження або зниження напруги. Виявлення несправностей здійснюється шляхом порівняння виміряних параметрів з установленими пороговими значеннями.

Приклади: Виявлення короткого замикання за допомогою порівняння виміряного струму з граничним значенням, встановленим для нормальної роботи мережі.

Формула: Визначення струму короткого замикання:

$$I_{\text{кз}} = \frac{\text{U}}{Z_{\text{кз}}}, \qquad (2.8)$$

де $I_{\text{кз}}$- струм короткого замикання

U - напруга в мережі

$Z_{\text{кз}}$ - імпеданс короткого замикання

4. Прийняття рішення

Опис: МРЗС приймають рішення про відключення пошкодженої ділянки мережі на основі результатів аналізу. Це рішення приймається автоматично на основі заданих алгоритмів і налаштувань.

Приклади: Автоматичне відключення вимикача при перевищенні струму певного порогу або при виявленні гармонічних спотворень, що свідчать про несправність.

Формула: Час відключення:

$$t_p = \frac{K}{I_з} \qquad (2.9)$$

де $t_p$- час реакції

$K$ – коефіцієнт налаштування

$I_з$ - струм замикання

5. Виконання команди

Опис: Після прийняття рішення про відключення МРЗС надсилають відповідні команди виконавчим механізмам (вимикачам, реле), що забезпечують фізичне роз'єднання пошкоджених ланцюгів. Це забезпечує швидке і точне відключення пошкодженої секції.

Приклади: Активація автоматичного вимикача для відключення пошкодженої секції мережі, що запобігає поширенню аварії.

Формула: Коефіцієнт відключення:

$$C_{\text{откл}} = \frac{\text{P}_{\text{макс}}}{\text{P}_{\text{н}}} \qquad (2.10)$$

$C_{\text{откл}}$- коефіцієнт відключення

$\text{P}_{\text{макс}}$ - максимальна потужність

$\text{P}_{\text{н}}$ - номінальна потужність

6. Моніторинг та діагностика

Опис: МРЗС постійно моніторять стан мережі та виконують діагностику для виявлення можливих проблем. Це дозволяє своєчасно виявляти несправності та вживати необхідних заходів для їх усунення.

Приклади: Регулярні перевірки стану обладнання, аналіз журналів подій для виявлення попереджувальних сигналів.

Формула: Моніторинг параметрів:

$$M(t) = \int_0^t P(t)dt \qquad (2.11)$$

де M(t) - накопичений моніторинговий параметр, P(t) - потужність у часі.

Деталізація прикладів застосування принципів роботи МРЗС

1. Захист трансформаторів

Опис: Використання МРЗС для захисту трансформаторів від перевантажень і коротких замикань. МРЗС здійснюють безперервний

моніторинг параметрів трансформатора і виявляють несправності на ранніх стадіях.

Приклади: Застосування диференціального захисту для виявлення внутрішніх несправностей трансформатора, таких як міжвиткове коротке замикання.

Формула Різницевий струм:

$$I_{diff} = I_{вх} - I_{вих} \quad (2.12)$$

де $I_{diff}$ - різницевий струм, $I_{вх}$ - вхідний струм, $I_{вих}$ - вихідний струм.

2. Захист ліній електропередач

Опис: Використання МРЗС для захисту ліній електропередач від коротких замикань і перевантажень. МРЗС забезпечують точне визначення місця несправності і автоматичне відключення пошкоджених ділянок.

Приклади: Використання дистанційного захисту для виявлення несправностей на різних ділянках лінії, що дозволяє швидко локалізувати і усунути несправність.

Формула: Визначення відстані до несправності:

$$d = \frac{V \cdot t}{2} \quad (2.13)$$

де d - відстань до несправності, V - швидкість поширення сигналу, t - час затримки.

3. Захист генераторів (продовження)

Формула: Збалансований струм:

$$I_{bal} = I_{ф1} + I_{ф2} + I_{ф3} \quad (2.14)$$

де $I_{bal}$ - збалансований струм, $I_{ф1}$, $I_{ф2}$ , $I_{ф3}$ - фазові струми.

Це дозволяє виявляти будь-які аномалії, які можуть свідчити про несправність генератора.

Приклади: Застосування адаптивних алгоритмів захисту, які змінюють параметри в залежності від умов роботи генератора, забезпечуючи оптимальний рівень захисту.

## Майбутні напрямки розвитку МРЗС

1. **Інтеграція штучного інтелекту**

**Опис**: Використання алгоритмів штучного інтелекту для покращення виявлення несправностей і оптимізації параметрів захисту.

**Приклади**: Машинне навчання для прогнозування можливих несправностей, адаптивні алгоритми, що підлаштовуються під змінні умови мережі.

**Переваги**: Підвищення точності та ефективності, зменшення кількості хибних спрацьовувань, оптимізація процесів обслуговування та ремонту.

2. **Розширене використання Інтернету речей (IoT)**

**Опис**: Інтеграція приладів релейного захисту в екосистему IoT для забезпечення більш детального моніторингу та управління.

**Приклади**: Використання сенсорів для збору даних у реальному часі, інтеграція з хмарними платформами для аналізу даних[7].

**Переваги**: Покращений моніторинг стану мережі, оперативне виявлення несправностей, зниження витрат на обслуговування.

3. **Розвиток хмарних технологій**

**Опис**: Використання хмарних сервісів для зберігання, обробки та аналізу даних з приладів релейного захисту.

**Приклади**: Хмарні платформи для централізованого управління, аналіз даних у реальному часі, віддалене оновлення програмного забезпечення.

**Переваги**: Зниження витрат на інфраструктуру, підвищення доступності та безпеки даних, можливість віддаленого управління.

4. **Підвищення рівня кібербезпеки**

**Опис**: Впровадження нових методів і технологій для захисту від кіберзагроз, що стають все більш актуальними у цифровому світі.

**Приклади**: Шифрування даних, автентифікація користувачів, системи моніторингу та виявлення підозрілої активност[8].

**Переваги**: Захист від несанкціонованого доступу, зменшення ризику кібератак, забезпечення безпеки і стабільності роботи мережі.

5. **Розширення функціональності адаптивного захисту**

**Опис**: Подальший розвиток функцій адаптивного захисту, що дозволяє приладам автоматично підлаштовувати свої параметри відповідно до змінних умов мережі.

**Приклади**: Автоматичне регулювання налаштувань у реальному часі, інтеграція з іншими системами для комплексного управління.

**Переваги**: Підвищення ефективності захисту, зниження ризику хибних спрацьовувань, оптимізація роботи мережі.

Мікропроцесорні релейні захисні системи забезпечують надійний і ефективний захист електричних мереж завдяки використанню сучасних технологій та складних алгоритмів обробки сигналів. Принципи роботи МРЗС включають вимірювання параметрів мережі, аналіз і обробку сигналів, виявлення несправностей, прийняття рішень, виконання команд та постійний моніторинг і діагностику. Інтеграція штучного інтелекту, використання IoT, розвиток хмарних технологій та підвищення рівня кібербезпеки є майбутніми напрямками розвитку МРЗС, що забезпечить ще більшу ефективність і надійність роботи електричних мереж у майбутньому.

## 2.4. Необхідність систем керування МРЗС

Обґрунтування необхідності систем керування мікропроцесорними релейними захисними системами (МРЗС)[8].

Мікропроцесорні релейні захисні системи (МРЗС) відіграють ключову роль у забезпеченні надійності та безпеки електричних мереж. Вони використовуються для виявлення і усунення несправностей, забезпечуючи стабільну роботу енергосистем. Необхідність систем керування МРЗС обумовлена кількома важливими факторами, які дозволяють оптимізувати їх роботу і підвищити ефективність.

1. Підвищення надійності та швидкодії

Опис: Системи керування МРЗС дозволяють оперативно виявляти і реагувати на несправності, що забезпечує високу швидкодію і надійність захисту.

Приклади: Використання алгоритмів адаптивного захисту, які автоматично підлаштовуються під змінні умови мережі.

2. Комплексний моніторинг та діагностика

Опис: Системи керування забезпечують комплексний моніторинг параметрів мережі і стану захисних пристроїв, що дозволяє виявляти потенційні проблеми на ранніх стадіях.

Приклади: Використання SCADA-систем для централізованого моніторингу та управління енергосистемами.Далі, в формулі 2,15 наведено моніторинг параметрів:

$$M(t) = \int_0^t P(t)dt \qquad (2.15)$$

де м(t) – накопичений моніторинговий параметр

$P(t)$ – потужність у часі.

3. Оптимізація роботи мережі

Опис: Системи керування МРЗС дозволяють оптимізувати роботу мережі, автоматично регулюючи параметри захисту для забезпечення максимального рівня безпеки і ефективності.

Приклади: Використання алгоритмів прогнозування навантаження і автоматичного регулювання налаштувань захисту.

Регулювання параметрів:

$$R(t)=f(P(t),V(t), F(t)) \quad (2.16)$$

де R(t) – регульовані параметри

P(t) – потужність

V(t)- напруга

4. Підвищення безпеки та стабільності

Опис: Системи керування забезпечують високий рівень безпеки і стабільності роботи мережі завдяки постійному моніторингу і своєчасному реагуванню на несправності.

Приклади: Використання захисту від кіберзагроз, що забезпечує захист від несанкціонованого доступу і зменшує ризик кібератак.

$$S = \int_0^t (P_з - P_н)dt \quad (2.17)$$

Де $S$- показник безпеки

$P_з$ – захисна потужність

$P_н$ – номінальна потужність

5. Ефективність управління енергосистемою

Опис: Системи керування МРЗС дозволяють здійснювати ефективне управління енергосистемою, забезпечуючи координацію між різними елементами захисту і управління.

Приклади: Інтеграція з іншими системами управління, такими як SCADA, для забезпечення єдиного інформаційного середовища.[10]

Приклади впровадження систем керування МРЗС

1. ABB Ability™ Energy Management System

Опис: Комплексна система управління енергосистемами, яка забезпечує моніторинг, аналіз і оптимізацію роботи мережі.

Функції: Централізоване управління захистом, аналіз даних у реальному часі, прогнозування навантажень[9].

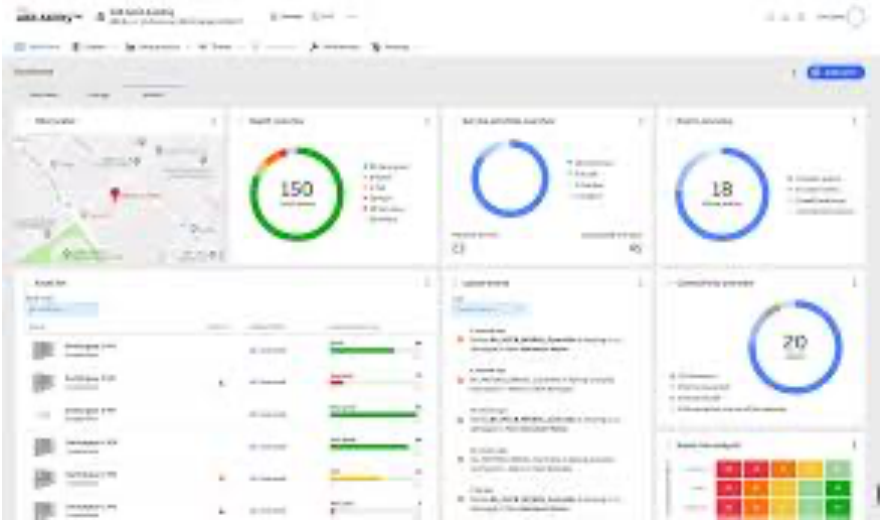


Рис. 2.1. Зображення ABB Ability™ Energy Management System

2. **Siemens Spectrum Power™**

**Опис**: Модульна система управління енергосистемами, яка забезпечує інтеграцію різних компонентів захисту і автоматизації.

**Функції**: Моніторинг і управління у реальному часі, підтримка віддаленого доступу, аналіз даних.

3. **Schneider Electric EcoStruxure™**

**Опис**: Платформа для управління енергосистемами, яка забезпечує комплексний підхід до захисту, моніторингу і управління.

**Функції**: Віддалене управління, аналіз даних, прогнозування несправностей, кібербезпека.

Для ілюстрації ефективності роботи систем керування МРЗС можна використовувати наступні математичні моделі та формули.

1. Розрахунок часу реакції системи керування:

$$t_c = t_m + t_0 + t_в \quad (2.18)$$

$t_c$ – загальний час реакції системи

$t_m$ – час моніторингу

$t_0$ – час обробки

$t_в$ – час виконання

2. Розрахунок ефективності управління:

$$E = \frac{Q_{кор}}{Q_{вх}} \quad (2.19)$$

E – ефективність управління

$Q_{кор}$ – кількість коректно оброблених подій

$Q_{вх}$загальна кількість подій

Системи керування МРЗС є невід'ємною частиною сучасних енергосистем, що забезпечують надійний і ефективний захист електричних мереж. Вони дозволяють оперативно виявляти і реагувати на несправності, забезпечувати комплексний моніторинг і діагностику, оптимізувати роботу мережі, підвищувати рівень безпеки та стабільності, а також здійснювати ефективне управління енергосистемою. Використання передових технологій, таких як адаптивний захист, кібербезпека, дистанційне управління та прогнозування навантажень, забезпечує високий рівень надійності і ефективності роботи МРЗС[11].

## 2.5. Постановка завдань для 3 розділу дипломної роботи: системи керування МРЗС

У даному розділі дипломної роботи буде розглянуто питання застосування штучного інтелекту (ІІ) у системах керування мікропроцесорними релейними захисними системами (МРЗС). Використання ІІ дозволяє підвищити ефективність і надійність роботи МРЗС шляхом автоматизації процесів аналізу, моніторингу та управління. Основними завданнями, які будуть розглянуті в цьому розділі, є:

1. **Аналіз поточних можливостей ІІ у керуванні МРЗС**

   **Опис**: Аналіз існуючих рішень і технологій, що використовуються для інтеграції ІІ в системи керування МРЗС.

   **Приклади**: Використання машинного навчання для прогнозування несправностей, нейронних мереж для аналізу сигналів.

2. **Розробка алгоритмів ІІ для виявлення несправностей**

   **Опис**: Розробка та впровадження алгоритмів, які дозволяють використовувати ІІ для виявлення несправностей у реальному часі.

   **Приклади**: Алгоритми глибокого навчання для класифікації типів несправностей, використання методів кластеризації для виявлення аномалій.

3. **Інтеграція ІІ з існуючими системами керування**

   **Опис**: Вивчення способів інтеграції алгоритмів ІІ з існуючими системами керування МРЗС для підвищення їх ефективності.

   **Приклади**: Інтеграція ІІ у SCADA-системи для покращення моніторингу та управління, використання хмарних платформ для обробки даних.

4. **Оцінка ефективності використання ІІ у МРЗС**

**Опис**: Проведення аналізу ефективності впровадження ІІ у системи керування МРЗС, оцінка переваг і недоліків.

**Приклади**: Аналіз зниження кількості хибних спрацьовувань, підвищення швидкодії системи, зменшення часу простою.

5. **Розробка прототипу системи керування на базі ІІ**

**Опис**: Створення прототипу системи керування МРЗС, що використовує алгоритми ІІ для демонстрації їх можливостей і переваг.

**Приклади**: Розробка програмного забезпечення для аналізу сигналів у реальному часі, використання ІІ для автоматичного налаштування параметрів захисту.

**Приклади застосування ІІ у МРЗС**

1. **ABB Ability™ Predictive Maintenance**

**Опис**: Система, що використовує алгоритми ІІ для прогнозування несправностей і планування технічного обслуговування.

**Функції**: Аналіз історичних даних, прогнозування часу до відмови, автоматичне повідомлення про необхідність обслуговування.

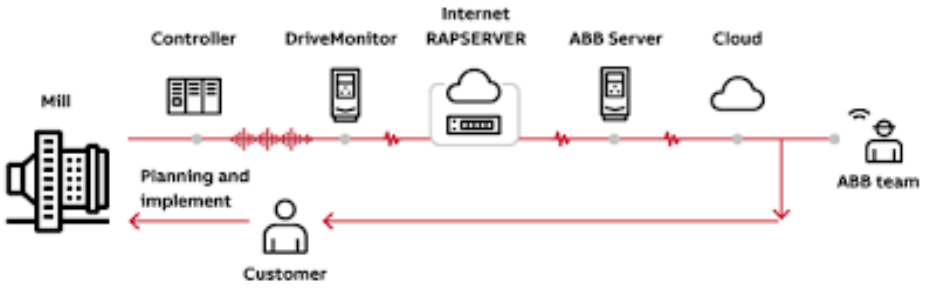


Рис. 2.2. Зображення ABB Ability™ Predictive Maintenance]

2. **Siemens MindSphere**

**Опис**: Відкрита хмарна платформа, що дозволяє інтегрувати ІІ у системи керування МРЗС для аналізу даних і покращення управління.

**Функції**: Збір і аналіз даних у реальному часі, прогнозування несправностей, оптимізація налаштувань.

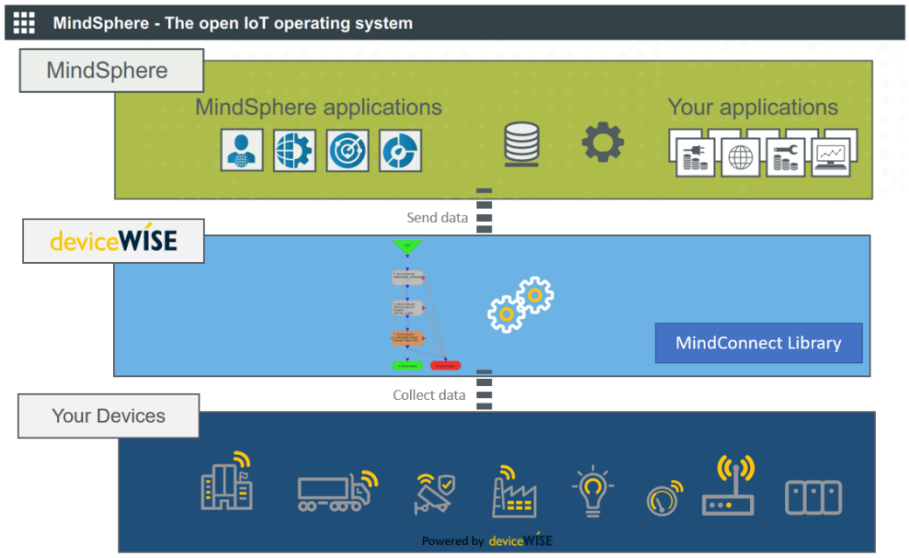


Рис. 2.3.Зображення Siemens MindSphere]

3. **Schneider Electric EcoStruxure™ Machine Advisor**

**Опис**: Платформа, що забезпечує дистанційний моніторинг, аналіз і управління системами захисту з використанням ІІ.

**Функції**: Віддалений моніторинг, аналіз ефективності, автоматичне налаштування параметрів.

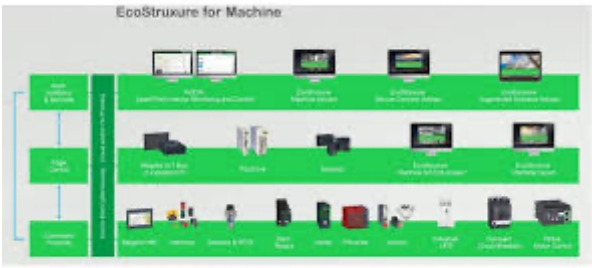


Рис. 2.4. Зображення Schneider Electric EcoStruxure™ Machine Advisor]

Для ілюстрації використання ІІ у системах керування МРЗС можна використовувати наступні математичні моделі та формули.

1. Прогнозування несправностей

$P(t) = \sum_{i=1}^{n} w_i \, x_i(t)$

де P(t) – прогнозоване значення

$w_i$ – вагові коефіцієнти

$x_i(t)$ – вхідні параметри

2. Алгоритм класифікації

   f(x) = arg $\max_y P(y|x)$

   де f(x) – функція класифікації

   $P(y|x)$ – умовна ймовірність

3. Інтеграція даних:

   $D_{int} = f(D_{sys1}, D_{sys2}, \ldots, D_{sysn})$

   $D_{int}$ – інтегровані дані

   $D_{sysn}$ - дані з різних систем

4. Ефективність системи

   E= $\frac{R_{безп}}{R_{вх}}$

   E - ефективність

   $R_{безп}$ – кількість безпечних операцій

   $R_{вх}$ – загальна кількість операцій

5. Автоматичне налаштування:

   $P_{нов} = f(P_{пот}, D)$

   $P_{нов}$ – нові параметри

   $P_{пот}$ – поточні параметри

   D – оброблені дані

У поточному розділі дипломної роботи розглянуто питання застосування штучного інтелекту у системах керування мікропроцесорними релейними захисними системами. Основними завданнями є аналіз поточних можливостей ІІ, розробка алгоритмів для виявлення несправностей, інтеграція ІІ з існуючими системами керування, оцінка ефективності використання ІІ у МРЗС та розробка прототипу системи керування на базі ІІ. Використання штучного інтелекту дозволяє значно підвищити ефективність і надійність роботи МРЗС, автоматизуючи процеси аналізу, моніторингу та управління.

## 2.6. Побудування математичної моделі МРЗС

Математична модель мікропроцесорних релейних захисних систем (МРЗС) є важливим інструментом для аналізу, проектування та оптимізації систем захисту електричних мереж. Вона дозволяє змоделювати різні сценарії роботи системи, оцінити її ефективність, виявити потенційні проблеми та розробити відповідні рішення для їх усунення.

Основні елементи математичної моделі МРЗС

1. Моделювання електричних параметрів

Опис: Включає моделювання основних електричних параметрів, таких як струм, напруга, частота, потужність та інші.

Приклади: Використання рівнянь для опису поведінки струму та напруги у різних частинах електричної мережі[12].

2. Моделювання динамічних процесів

Опис: Включає моделювання динамічних процесів, що відбуваються під час несправностей, таких як короткі замикання, перевантаження тощо.

Приклади: Використання диференціальних рівнянь для опису динамічних змін струму та напруги під час короткого замикання.

3. Моделювання алгоритмів захисту

Опис: Включає моделювання алгоритмів, які використовуються для виявлення і реагування на несправності у системі.

Приклади: Алгоритми для виявлення коротких замикань, перевантажень, зниження напруги тощо.

4. Моделювання взаємодії з іншими системами

Опис: Включає моделювання взаємодії МРЗС з іншими системами захисту та управління, такими як SCADA-системи.

Приклади: Інтеграція даних з різних систем для комплексного аналізу і управління.

5. Оцінка ефективності моделі

Опис: Включає оцінку ефективності побудованої математичної моделі, її точності та відповідності реальним умовам експлуатації.

Приклади: Проведення тестувань та симуляцій для оцінки точності моделі.

Процес побудування математичної моделі МРЗС

1. Визначення вхідних параметрів

Опис: Визначення основних параметрів, що використовуватимуться у моделі, таких як струм, напруга, частота, індуктивність, опір тощо[13].

Приклади: Вхідні параметри можуть включати номінальні значення напруги і струму, характеристики трансформаторів, дані про лінії електропередач.

2. Побудова математичних рівнянь

Опис: Розробка математичних рівнянь, що описують поведінку електричних параметрів і динамічних процесів у системі.

Приклади: Використання диференціальних рівнянь, інтегральних рівнянь, алгебраїчних рівнянь для опису різних процесів[13].

3. Розробка алгоритмів захисту

Опис: Розробка алгоритмів, що використовуються для виявлення і реагування на несправності.

Приклади: Алгоритми виявлення коротких замикань, перевантажень, зниження напруги тощо.

4. Інтеграція з іншими системами

Опис: Розробка механізмів інтеграції моделі з іншими системами, такими як SCADA, для забезпечення комплексного аналізу і управління.

Приклади: Використання стандартних протоколів обміну даними для інтеграції з іншими системами.

5. Тестування та валідація моделі

Опис: Проведення тестувань і симуляцій для перевірки точності та ефективності моделі.

Приклади: Проведення симуляцій реальних умов експлуатації, порівняння результатів з реальними даними для валідації моделі.

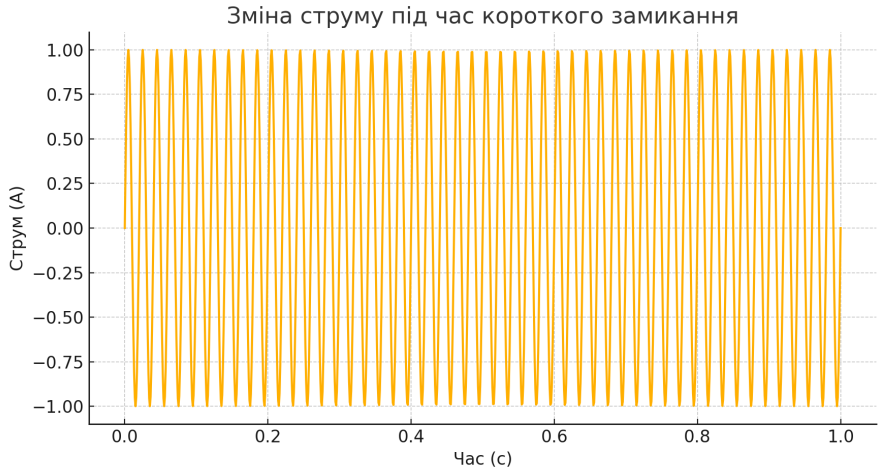


Рис. 2.5. Графік зміни струму під час короткого замикання

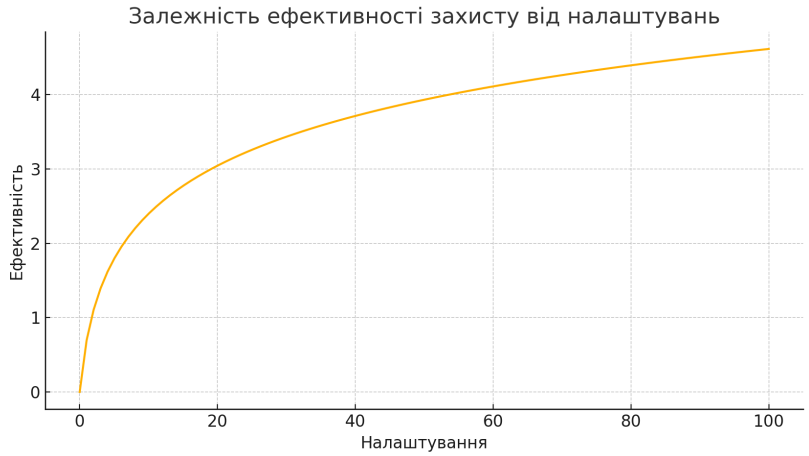


Рис. 2.6. Графік залежності ефективності захисту від налаштувань

# РОЗДІЛ 3
# СИСТЕМА КЕРУВАННЯ МРЗС

## 3.1. Основні принципи побудови систем керування МРЗС

Система керування мікропроцесорними релейними захисними системами (МРЗС) є важливим компонентом сучасних енергетичних мереж, який забезпечує надійність, ефективність і безпеку роботи електроенергетичних об'єктів. Використання систем керування дозволяє не тільки підвищити точність і швидкодію релейного захисту, але й забезпечити інтеграцію з іншими системами, що робить можливим комплексний моніторинг та управління енергосистемою. Це особливо актуально в умовах військового конфлікту, коли стабільність енергопостачання є критично важливою для забезпечення нормальної життєдіяльності населення[14].

### 3.1.1. Визначення основних вимог до систем керування

Основні вимоги до систем керування МРЗС включають:

**Надійність**: Система повинна забезпечувати високу надійність і безперервність роботи навіть у випадку несправностей окремих компонентів.

**Швидкодія**: Оперативність виявлення і реагування на несправності є критично важливою для запобігання аварійним ситуаціям.

**Точність**: Висока точність вимірювань і аналізу даних забезпечує ефективність роботи релейного захисту.

**Безпека**: Система повинна забезпечувати захист від несанкціонованого доступу і кібератак.

**Інтеграція**: Можливість інтеграції з іншими системами управління і моніторингу, такими як SCADA, забезпечує комплексний підхід до управління енергосистемою.

**Віддалений доступ**: Забезпечення можливості віддаленого моніторингу і управління системою, що особливо важливо в умовах військового конфлікту, коли оператори можуть не мати можливості перебувати на місці[14].

### 3.1.2. Архітектура системи керування

Архітектура системи керування МРЗС включає кілька рівнів, кожен з яких виконує свої функції і забезпечує комплексний підхід до управління системою.

**Вимірювальний рівень**: Включає сенсори та інтерфейси збору даних, які забезпечують первинні вимірювання параметрів електричної мережі (струм, напруга, частота тощо).

**Обчислювальний рівень**: Включає мікропроцесори та інше апаратне забезпечення для обробки сигналів і виконання алгоритмів захисту.

**Комунікаційний рівень**: Забезпечує передачу даних між компонентами системи і з зовнішніми системами, використовуючи різні протоколи передачі даних (Ethernet, Modbus, DNP3 тощо).

**Інтерфейс користувача**: Дозволяє операторам взаємодіяти з системою, налаштовувати параметри і отримувати інформацію про стан системи через локальні дисплеї або віддалені робочі станції.

### 3.1.3. Вибір апаратних та програмних засобів

Вибір апаратних та програмних засобів для системи керування МРЗС залежить від вимог до продуктивності, надійності і функціональності системи. Основними компонентами є:

**Сенсори**: Трансформатори струму і напруги, які забезпечують високоточні вимірювання параметрів електричної мережі.

**Мікропроцесори**: Багатоядерні процесори, які забезпечують високу швидкодію і здатність до обробки великої кількості даних в режимі реального часу.

**Комунікаційні модулі**: Модулі для передачі даних, що підтримують різні протоколи передачі даних і забезпечують надійний зв'язок між компонентами системи і з зовнішніми системами.

**Програмне забезпечення**: Спеціалізоване програмне забезпечення для реалізації алгоритмів захисту, моніторингу і управління системою. Важливим елементом є використання технологій штучного інтелекту для підвищення ефективності роботи системи[15].

**Системи безпеки**: Засоби захисту від несанкціонованого доступу і кібератак, що забезпечують безпеку даних і стабільність роботи системи.

В умовах військового конфлікту в Україні стабільність енергопостачання є критично важливою для забезпечення нормальної життєдіяльності населення. Сучасні системи керування МРЗС з використанням штучного інтелекту дозволяють забезпечити надійність і безпеку енергосистеми навіть у складних умовах. Вони забезпечують безперервний моніторинг і оперативне реагування на несправності, що

знижує ризик аварій і забезпечує стабільну роботу енергосистеми. Важливим аспектом є можливість віддаленого доступу до системи, що дозволяє операторам керувати і моніторити систему з безпечного місця.

Для точного опису роботи систем керування МРЗС використовуються різні математичні моделі та формули. Наприклад, модель виявлення несправностей може бути представлена рівнянням:

$I(t)=I_0\sin(\omega t+\phi)I(t)= I_0\sin(\omega t+\phi)$

де I(t)- миттєве значення струму,

$I_0$ - амплітуда,

ω- кутова частота,

ϕ- фаза.

Важливим елементом МРЗС є фільтрація сигналів. Одним із методів фільтрації є використання цифрових фільтрів, які можуть бути описані рівняннями типу:

$y[n]=x[n]-x[n-1]y[n]=x[n]-x[n-1]$

де y[n]- вихідний сигнал, x[n] - вхідний сигнал у момент часу n.

Для більш детального аналізу роботи МРЗС можна використовувати спектральний аналіз сигналів, що дозволяє визначити частотні компоненти струмів та напруг у мережі[16].

Основні принципи побудови систем керування МРЗС включають визначення вимог до системи, розробку архітектури і вибір апаратних та програмних засобів. Використання сучасних технологій, таких як штучний інтелект і віддалений доступ, забезпечує високу надійність і ефективність роботи системи, що особливо актуально в умовах військового конфлікту в Україні.

## 3.2. Використання штучного інтелекту у системах керування МРЗС

Застосування штучного інтелекту (ІІ) у системах керування мікропроцесорними релейними захисними системами (МРЗС) відкриває нові можливості для підвищення ефективності та надійності роботи енергосистем. ІІ дозволяє автоматизувати процеси аналізу даних, виявлення несправностей, прогнозування аварійних ситуацій та прийняття рішень в режимі реального часу. Це особливо актуально в умовах військового конфлікту, коли оперативне реагування на зміни в енергосистемі може мати вирішальне значення для стабільності енергопостачання[17].

### 3.2.1. Основні концепції та методи штучного інтелекту

Штучний інтелект включає в себе широкий спектр методів та технологій, які можуть бути застосовані у системах керування МРЗС. Основні концепції та методи ІІ включають:

Машинне навчання: Метод, що дозволяє комп’ютерам навчатися на основі даних. Основні типи машинного навчання включають наглядове навчання, ненаглядове навчання та навчання з підкріпленням.

Наглядове навчання: Використовується для навчання моделей на основі відмічених даних, що дозволяє прогнозувати значення або класифікувати нові дані.

Ненаглядове навчання: Використовується для виявлення прихованих закономірностей у невідмічених даних, наприклад, кластеризація аномалій у параметрах електричної мережі.

Навчання з підкріпленням: Метод, що дозволяє агентам навчатися на основі винагороди та покарання, оптимізуючи свою поведінку для досягнення максимальної вигоди.

Нейронні мережі: Моделі, що імітують роботу людського мозку і здатні виявляти складні закономірності в даних. Глибокі нейронні мережі (deep learning) особливо ефективні для аналізу великих обсягів даних.

Глибоке навчання: Використання багатошарових нейронних мереж для аналізу складних патернів у великих масивах даних.

Рекурентні нейронні мережі (RNN): Використовуються для обробки послідовних даних, таких як часові ряди або потоки даних у реальному часі.

Аналіз даних: Методи обробки та аналізу даних, що дозволяють виявляти тенденції, аномалії та передбачати майбутні події.

Спектральний аналіз: Використовується для виявлення частотних компонентів сигналів у електричних мережах[18].

Аналіз часових рядів: Методи для аналізу даних, що змінюються з часом, зокрема для прогнозування майбутніх значень параметрів мережі.

Алгоритми оптимізації: Методи, що дозволяють знаходити оптимальні рішення для складних задач, зокрема у галузі управління та захисту енергосистем.

Генетичні алгоритми: Використовуються для пошуку оптимальних рішень шляхом імітації процесу природного відбору.

Алгоритми рою часток: Моделюють поведінку колективних організмів для знаходження глобальних оптимумів.

### 3.2.2. Алгоритми машинного навчання для аналізу даних

Машинне навчання відіграє ключову роль у системах керування МРЗС, дозволяючи автоматизувати процеси аналізу даних і прийняття рішень. Основні алгоритми машинного навчання, що використовуються для аналізу даних у МРЗС, включають:

Регресія: Алгоритми лінійної та поліноміальної регресії використовуються для прогнозування параметрів електричної мережі, таких як струм, напруга та частота.

Класифікація: Алгоритми класифікації, такі як дерева рішень, логістична регресія та метод опорних векторів, використовуються для виявлення типів несправностей у системі.

$P(y|x)= \frac{1}{1+e^{-(\beta_0+\beta_1 x)}}$

де ( P(y|x) ) - ймовірність класу ( y ) при умові значення ( x ).

Кластеризація: Алгоритми кластеризації, такі як k-середні та DBSCAN, використовуються для виявлення аномалій у даних.

$$min \sum_{i=1}^{k} \sum_{x \in C_i} ||x - \mu_i||^2$$

де $C_i$ – кластери

$\mu_i$ – центроїди кластерів

### 3.2.3. Інтеграція штучного інтелекту в систему керування

Інтеграція штучного інтелекту у систему керування МРЗС включає кілька етапів:

1. **Збір даних**: Використання сенсорів і трансформаторів для збору даних про параметри електричної мережі. Сенсори збирають дані про струм, напругу, частоту та інші параметри в режимі реального часу.
2. **Обробка даних**: Попередня обробка даних для видалення шумів і виявлення важливих характеристик. Це включає нормалізацію даних, видалення викидів та інші методи очищення даних.
3. **Навчання моделей**: Використання історичних даних для навчання моделей машинного навчання, що здатні виявляти несправності і прогнозувати аварійні ситуації. Алгоритми машинного навчання навчаються на основі відмічених даних, де зазначені випадки несправностей та нормальної роботи системи.
4. **Інтеграція моделей**: Впровадження навчальних моделей у систему керування МРЗС для автоматизації процесів аналізу і прийняття рішень. Це дозволяє системі автоматично виявляти несправності та реагувати на них, мінімізуючи час простою та ризики аварій.
5. **Моніторинг і оптимізація**: Постійний моніторинг роботи моделей і оптимізація їх налаштувань для забезпечення високої точності і надійності. Це включає адаптивні алгоритми, що дозволяють моделям оновлюватися і покращувати свої прогнози на основі нових даних.

В умовах військового конфлікту в Україні стабільність і надійність енергопостачання є критично важливими. Використання штучного інтелекту у системах керування МРЗС дозволяє забезпечити безперервний

моніторинг і оперативне реагування на несправності, що знижує ризик аварій і забезпечує стабільну роботу енергосистеми.

ІІ може автоматично виявляти і реагувати на несправності, що дозволяє операторам зосередитися на стратегічному управлінні і забезпеченні безпеки енергосистеми. Це особливо важливо в умовах, коли оператори можуть не мати можливості перебувати на місці через загрозу безпеці.

Для ілюстрації використання штучного інтелекту в системах керування МРЗС можна навести приклади алгоритмів і графіків, які показують ефективність цих методів.

1. Регресія для прогнозування параметрів:

$$y= \beta_0 + \beta_1 x + e$$

де ( y ) - залежна змінна,

( x ) - незалежна змінна,

$\beta_0$ і $\beta_1$ - коефіцієнти регресії,

e - випадкова помилка.

2. Класифікація для виявлення типів несправностей:

$$P(y|x)= \frac{1}{1+e^{-(\beta_0+\beta_1 x)}}$$

де ( P(y|x) ) - ймовірність класу ( y ) при умові значення ( x ).

3. Кластеризація для виявлення аномалій:

$$min \sum_{i=1}^{k} \sum_{x \in C_i} ||x - \mu_i||^2$$

де $C_i$ – кластери

$\mu_i$ – центроїди кластерів

Застосування штучного інтелекту у системах керування МРЗС значно підвищує ефективність і надійність роботи енергосистем. Використання ІІ дозволяє автоматизувати процеси аналізу даних, виявлення несправностей і прогнозування аварійних ситуацій, що є критично важливим в умовах військового конфлікту в Україні. Інтеграція ІІ у систему керування МРЗС забезпечує безперервний моніторинг і оперативне реагування на несправності, що знижує ризик аварій і забезпечує стабільну роботу енергосистеми[18].

## 3.3. Проектування системи керування МРЗС

Проектування системи керування мікропроцесорними релейними захисними системами (МРЗС) є складним і багатоетапним процесом, який включає розробку функціональної схеми, вибір програмного забезпечення, розробку інтерфейсів користувача та інтеграцію з іншими системами захисту. Це забезпечує високий рівень надійності та ефективності роботи системи. У цьому підрозділі будуть розглянуті ключові аспекти проектування системи керування МРЗС.

### 3.3.1. Розробка функціональної схеми системи

Функціональна схема системи керування МРЗС відображає основні компоненти системи та їх взаємозв’язки. Основні елементи функціональної схеми включають:

**Сенсори**: Трансформатори струму і напруги, що забезпечують вимірювання основних параметрів електричної мережі.

**Мікропроцесорні блоки**: Центральні компоненти системи, що виконують обробку даних і реалізацію алгоритмів захисту.

**Комунікаційні модулі**: Забезпечують передачу даних між компонентами системи і з зовнішніми системами.

**Інтерфейси користувача**: Дозволяють операторам взаємодіяти з системою, налаштовувати параметри і отримувати інформацію про стан системи.

1. **Сенсори та вимірювальні прилади**

**Трансформатори струму та напруги**: Забезпечують точні вимірювання параметрів електричної мережі. Сучасні сенсори мають високу чутливість і точність, що дозволяє виявляти навіть незначні відхилення від нормальних значень.

**Датчики температури**: Використовуються для моніторингу температури обладнання і навколишнього середовища, що дозволяє запобігати перегріву і пошкодженню обладнання.

2. **Мікропроцесорні блоки**

**Процесори та контролери**: Центральні елементи системи, що обробляють дані від сенсорів і виконують алгоритми захисту. Використання багатоядерних процесорів забезпечує високу швидкодію і здатність обробки великих обсягів даних в режимі реального часу.

**Модулі пам’яті**: Зберігають дані про параметри мережі, історію подій та налаштування системи. Використання енергонезалежної пам’яті забезпечує збереження даних навіть при відключенні живлення.

3. **Комунікаційні модулі**

**Мережеві інтерфейси**: Забезпечують передачу даних між компонентами системи і з зовнішніми системами. Підтримка різних протоколів передачі даних, таких як Ethernet, Modbus, DNP3, дозволяє забезпечити сумісність з іншими системами.

**Бездротові модулі**: Забезпечують зв’язок між компонентами системи у випадках, коли використання кабельних з’єднань неможливе або небажане.

4. **Інтерфейси користувача**

**Локальні дисплеї**: Відображають основні параметри і стан системи безпосередньо на місці установки. Забезпечують оперативний доступ до основних функцій системи.

**Веб-інтерфейси**: Забезпечують віддалений доступ до системи через веб-браузер. Дозволяють операторам моніторити і керувати системою з будь-якого місця.

**Мобільні додатки**: Дозволяють операторам моніторити і керувати системою з мобільних пристроїв. Забезпечують зручний доступ до функцій системи в режимі реального часу.

3.3.2. Вибір та обґрунтування програмного забезпечення

Вибір програмного забезпечення для системи керування МРЗС залежить від вимог до функціональності, надійності та інтеграції з іншими системами. Основні критерії вибору програмного забезпечення включають:

**Надійність**: Програмне забезпечення повинно забезпечувати стабільну роботу системи в умовах різних навантажень і несправностей.

**Масштабованість**: Можливість розширення функціональності системи без значних змін у програмному коді.

**Інтероперабельність**: Забезпечення сумісності з іншими системами та стандартами, такими як IEC 61850, DNP3, Modbus тощо.

**Безпека**: Захист від несанкціонованого доступу і кібератак.

Програмне забезпечення для систем керування МРЗС зазвичай включає наступні компоненти:

**Система управління базою даних (СУБД)**: Зберігає дані про параметри мережі, налаштування системи та історію подій.

**Алгоритми обробки даних**: Реалізують функції аналізу, прогнозування і виявлення несправностей[19].

**Інтерфейси користувача**: Забезпечують доступ до системи операторам для моніторингу і налаштування параметрів.

**Огляд популярних програмних рішень**

1. **SCADA-системи** (Supervisory Control and Data Acquisition)

   **Опис**: Забезпечують моніторинг і управління великими енергетичними системами в режимі реального часу.

   **Переваги**: Висока надійність, масштабованість, підтримка різних протоколів передачі даних.

   **Приклад**: SCADA-система від Siemens.

2. **Інтелектуальні системи керування** (Intelligent Control Systems)

   **Опис**: Використовують штучний інтелект для аналізу даних і прийняття рішень.

   **Переваги**: Висока точність і швидкодія, можливість самообучення.

   **Приклад**: EcoStruxure від Schneider Electric.

### 3.3.3. Розробка інтерфейсів користувача

Інтерфейси користувача є важливим елементом системи керування МРЗС, оскільки вони забезпечують зручний і інтуїтивно зрозумілий доступ до функцій системи. Основні вимоги до інтерфейсів користувача включають:

**Зручність використання**: Інтерфейси повинні бути зрозумілими і простими у використанні навіть для користувачів без глибоких технічних знань.

**Інформативність**: Інтерфейси повинні надавати операторам всю необхідну інформацію про стан системи в режимі реального часу.

**Гнучкість**: Можливість налаштування інтерфейсів під потреби конкретного користувача або задачі.

Інтерфейси користувача можуть включати:

**Локальні дисплеї**: Відображають основні параметри і стан системи безпосередньо на місці установки.

**Веб-інтерфейси**: Забезпечують віддалений доступ до системи через веб-браузер.

**Мобільні додатки**: Дозволяють операторам моніторити і керувати системою з мобільних пристроїв.

### 3.3.4. Інтеграція системи керування з іншими системами захисту

Інтеграція системи керування МРЗС з іншими системами захисту, такими як SCADA-системи, забезпечує комплексний підхід до управління енергосистемою. Основні етапи інтеграції включають:

Визначення вимог до інтеграції:

Встановлення вимог до обміну даними, сумісності протоколів і інтерфейсів.

Розробка архітектури інтеграції: Проектування архітектури, що забезпечує взаємодію між системами.

Реалізація інтеграційних рішень: Впровадження програмних і апаратних рішень для забезпечення обміну даними і сумісності систем.

Інтеграція забезпечує:

Централізований моніторинг: Можливість моніторингу стану всієї енергосистеми з єдиного центру управління.

Оптимізацію управління: Підвищення ефективності управління завдяки об’єднанню даних з різних систем.

Підвищення безпеки: Забезпечення захисту від кібератак і несанкціонованого доступу[20].

Для ілюстрації процесу проектування системи керування МРЗС можна використати різні математичні моделі та графіки:

1. Модель виявлення несправностей:

$I(t)=I_0\sin(\omega t+\phi)= I_0\sin(\omega t+\phi)$

де I(t)- миттєве значення струму,

$I_0$ - амплітуда,

ω- кутова частота,

ϕ- фаза.

2. Модель оптимізації параметрів захисту:

$\min \sum_{i=1}^{n}(x_i - x)^2$

де $x_i -$ поточні параметри

х – оптимальні параментри

Проектування системи керування МРЗС включає розробку функціональної схеми, вибір програмного забезпечення, розробку інтерфейсів користувача та інтеграцію з іншими системами захисту. Використання сучасних технологій і методів проектування забезпечує високу надійність і ефективність роботи системи. Інтеграція з іншими системами захисту забезпечує комплексний підхід до управління енергосистемою, підвищуючи її надійність і безпеку.

## 3.4. Тестування та валідація системи керування МРЗС

Тестування та валідація системи керування мікропроцесорними релейними захисними системами (МРЗС) є важливими етапами, що забезпечують високу надійність і ефективність роботи системи. Процес тестування включає перевірку всіх компонентів системи, імітацію різних сценаріїв роботи та аналіз результатів. Валідація полягає в підтвердженні відповідності системи заданим вимогам та стандартам. У цьому підрозділі буде розглянуто основні методи тестування та валідації системи керування МРЗС.

### 3.4.1. Методи тестування системи керування

Тестування системи керування МРЗС включає використання різних методів для перевірки функціональності, надійності та безпеки системи. Основні методи тестування включають:

Функціональне тестування: Перевірка всіх функцій системи на відповідність вимогам специфікацій. Це включає тестування алгоритмів захисту, комунікаційних модулів, інтерфейсів користувача та інших компонентів системи.

Приклад: Тестування алгоритму виявлення несправностей при різних умовах навантаження.

Модель функціонального тестування:

$$F_{test} = \frac{N_{pass}}{N_{total}} \times 100\%$$

де $F_{test}$ - функціональне тестування у відсотках,

$N_{pass}$ - кількість успішно пройдених тестів,

$N_{total}$ - загальна кількість тестів.

Інтеграційне тестування: Перевірка взаємодії між різними компонентами системи. Це включає тестування передачі даних між сенсорами, мікропроцесорами, комунікаційними модулями та інтерфейсами користувача.

Приклад: Тестування передачі даних між мікропроцесором та SCADA-системою.

Формула: Модель інтеграційного тестування:

$$\mathrm{I}_{test} = \frac{N_{integrated}}{N_{total}} \times 100\%$$

де $\mathrm{I}_{test}$- інтеграційне тестування у відсотках,

$N_{integrated}$ - кількість успішно інтегрованих компонентів,

$N_{total}$ - загальна кількість компонентів.

Стрес-тестування: Перевірка стійкості системи під високими навантаженнями та в умовах несправностей. Це включає імітацію аварійних ситуацій та перевірку реакції системи на екстремальні умови.

Приклад: Імітація короткого замикання та аналіз роботи системи в умовах максимального навантаження.

Модель стрес-тестування:

$$S_{test} = \frac{T_{operation}}{T_{stress}} \times 100\%$$

де $S_{test}$ - стрес-тестування у відсотках,

$T_{operation}$ - час роботи системи під нормальними умовами,

$T_{stress}$ - час роботи системи під стресовими умовами.

Безпекове тестування: Перевірка захищеності системи від кібератак та несанкціонованого доступу. Це включає тестування системи безпеки, шифрування даних та інших заходів захисту.

Приклад: Тестування стійкості системи до різних видів кібератак.

Модель безпекового тестування:

$$B_{test} = \frac{N_{secure}}{N_{total}} \times 100\%$$

де $B_{test}$ - безпекове тестування у відсотках,

$N_{secure}$ - кількість успішно захищених компонентів,

$N_{total}$ - загальна кількість компонентів.

### 3.4.2. Проведення експериментальних досліджень

Експериментальні дослідження включають проведення серії тестів і вимірювань для перевірки функціональності і надійності системи в реальних умовах експлуатації. Основні етапи експериментальних досліджень включають:

Підготовка до експериментів: Визначення цілей і завдань експериментів, підготовка необхідного обладнання і програмного забезпечення[20].

Приклад: Встановлення сенсорів та підключення системи до тестового стенду.

Проведення тестів: Виконання серії тестів за різними сценаріями роботи системи. Це включає тестування системи під різними навантаженнями, в умовах несправностей та аварійних ситуацій.

Приклад: Проведення тестів на виявлення коротких замикань та перевантажень.

Збір та аналіз даних: Збір даних про роботу системи під час тестів, аналіз результатів і порівняння їх з очікуваними значеннями.

Приклад: Аналіз даних про струми та напруги під час тестів на короткі замикання.

Внесення коректив: Виявлення та усунення недоліків в роботі системи на основі аналізу результатів тестів. Це може включати зміну налаштувань, вдосконалення алгоритмів або заміну компонентів системи.

Приклад: Внесення змін до алгоритму виявлення несправностей для підвищення точності.

### 3.4.3. Аналіз результатів тестування та валідація системи

Аналіз результатів тестування є важливим етапом, що дозволяє оцінити ефективність і надійність системи. Основні етапи аналізу включають:

Оцінка відповідності вимогам: Перевірка відповідності результатів тестування заданим вимогам і стандартам.

Приклад: Порівняння фактичних результатів тестування з вимогами специфікацій.

Аналіз помилок: Виявлення і класифікація помилок, що виникли під час тестування, визначення причин їх виникнення та шляхів усунення.

Приклад: Аналіз причин помилок в алгоритмі виявлення коротких замикань.

Підготовка звітів: Складання звітів про результати тестування, що включають дані про виявлені помилки, заходи з їх усунення та рекомендації щодо вдосконалення системи.

Приклад: Підготовка звіту про результати стрес-тестування системи.

### 3.4.4. Оцінка надійності та ефективності роботи системи

Оцінка надійності та ефективності роботи системи включає аналіз показників надійності, таких як середній час між відмовами (MTBF) та середній час відновлення (MTTR), а також оцінку ефективності роботи алгоритмів захисту.

Аналіз надійності: Оцінка показників надійності системи на основі даних тестування і експлуатації.

Приклад: Розрахунок середнього часу між відмовами для мікропроцесорних блоків.

Модель оцінки надійності:

$$MTBF = \frac{T_{operation}}{N_{failures}} \times 100\%$$

де $T_{operation}$ - загальний час роботи системи,

$N_{failures}$ - кількість відмов.

Оцінка ефективності: Аналіз ефективності роботи алгоритмів захисту на основі результатів тестування.

Приклад: Оцінка точності і швидкості роботи алгоритму виявлення несправностей.

Формула: Модель оцінки ефективності:

$$Efficiency = \frac{Correct\ decisions}{Total\ Decisions} \times 100\%$$

де Correct Decisions - кількість правильних рішень,

Total Decisions - загальна кількість рішень.

Оцінка надійності та ефективності роботи системи

1. Аналіз надійності: Оцінка показників надійності системи на основі даних тестування і експлуатації.

Приклад: Розрахунок середнього часу між відмовами для мікропроцесорних блоків.

Модель оцінки надійності:

$$Efficiency = \frac{Correct\ decisions}{Total\ Decisions} \times 100\%$$

де Correct Decisions - кількість правильних рішень,

Total Decisions - загальна кількість рішень.

### 3.4.5. Інші важливі аспекти тестування та валідації

1. Тестування продуктивності

Опис: Перевірка здатності системи обробляти великі обсяги даних в реальному часі.

Методи: Використання симуляційних моделей для імітації високих навантажень.

Формула: Модель тестування продуктивності:

$$P_{test} = \frac{D_{processed}}{T_{time}}$$

де $P_{test}$ - продуктивність тестування,

$D_{processed}$ - обсяг оброблених даних,

$T_{time}$ - час обробки.

2. Валідація користувацького інтерфейсу

Опис: Перевірка зручності використання та інтуїтивності інтерфейсів користувача.

Методи: Проведення опитувань і тестування з участю кінцевих користувачів.

Формула: Модель валідації користувацького інтерфейсу:

$$U_{test} = \frac{S_{users}}{T_{users}} \times 100\%$$

$U_{test}$ - рівень задоволеності користувачів,

$S_{users}$ - кількість задоволених користувачів,

$T_{users}$- загальна кількість користувачів.

3. Моніторинг та оптимізація в режимі реального часу

Опис: Постійний моніторинг роботи системи та внесення коректив на основі отриманих даних.

Методи: Використання адаптивних алгоритмів для оптимізації налаштувань системи в режимі реального часу.

Модель моніторингу та оптимізації:

$$M_{opt} = \frac{O_{improvements}}{T_{time}} \times 100\%$$

де $M_{opt}$ - ефективність моніторингу та оптимізації,

$O_{improvements}$ - кількість внесених покращень,

$T_{time}$ - час моніторингу.

Тестування та валідація системи керування МРЗС є важливими етапами, що забезпечують високу надійність і ефективність роботи системи. Використання різних методів тестування дозволяє перевірити функціональність, надійність та безпеку системи, а аналіз результатів тестування допомагає виявити та усунути недоліки. Валідація системи підтверджує її відповідність заданим вимогам і стандартам, що забезпечує стабільну та ефективну роботу системи в реальних умовах експлуатації.

Ефективне тестування та валідація не тільки підвищують надійність системи, але й допомагають оптимізувати її роботу, забезпечуючи максимально можливу ефективність та безпеку. Це особливо важливо в умовах сучасних вимог до енергосистем, де навіть невеликі відхилення можуть призвести до значних наслідків.

## 3.5. Впровадження системи керування МРЗС

Впровадження системи керування мікропроцесорними релейними захисними системами (МРЗС) є заключним етапом, який забезпечує реальну інтеграцію системи в існуючу енергосистему. Впровадження включає планування та організацію робіт, установку та налагодження обладнання, навчання персоналу і забезпечення технічної підтримки. У цьому підрозділі буде розглянуто основні етапи впровадження системи керування МРЗС.

### 3.5.1. Підготовка до впровадження: планування та організація

Планування та організація робіт з впровадження системи керування МРЗС включають кілька ключових етапів:

**Визначення цілей та завдань впровадження**: Формулювання основних цілей та завдань, що мають бути досягнуті в процесі впровадження системи.

**Приклад**: Підвищення надійності і безпеки електропостачання, оптимізація процесів управління енергосистемою.

**Розробка плану впровадження**: Створення детального плану робіт, що включає всі етапи впровадження, терміни виконання, відповідальних осіб та необхідні ресурси.

**Приклад**: План впровадження, що включає етапи встановлення обладнання, налаштування системи, тестування та навчання персоналу.

**Організація робіт**: Координація робіт між різними підрозділами та фахівцями, забезпечення наявності необхідних матеріалів та обладнання.

**Приклад**: Організація робіт з встановлення сенсорів і мікропроцесорних блоків, забезпечення підключення до електричної мережі.

### 3.5.2. Впровадження системи керування на об’єкті

Впровадження системи керування МРЗС на об’єкті включає кілька ключових етапів:

**Установка обладнання**: Встановлення сенсорів, мікропроцесорних блоків, комунікаційних модулів та інших компонентів системи.

**Приклад**: Встановлення трансформаторів струму і напруги, монтаж мікропроцесорних блоків у розподільчих пристроях.

**Підключення до мережі**: Підключення всіх компонентів системи до електричної мережі та забезпечення їх взаємодії.

**Приклад**: Підключення сенсорів до мікропроцесорних блоків, забезпечення передачі даних між компонентами системи.

**Налаштування та тестування**: Налаштування параметрів системи, проведення тестів для перевірки функціональності та надійності роботи.

**Приклад**: Налаштування алгоритмів захисту, проведення тестів на виявлення несправностей.

1. **Установка обладнання**

**Трансформатори струму і напруги**: Монтаж трансформаторів у місцях підключення до електричної мережі. Забезпечення правильного підключення для точного вимірювання параметрів.

**Мікропроцесорні блоки**: Встановлення мікропроцесорних блоків у розподільчих пристроях. Забезпечення належного захисту від впливу зовнішніх факторів.

**Комунікаційні модулі**: Монтаж модулів передачі даних, забезпечення надійного зв’язку між компонентами системи.

2. **Підключення до мережі**

**Сенсори**: Підключення сенсорів до мікропроцесорних блоків. Забезпечення правильного калібрування для точних вимірювань.

**Комунікаційні модулі**: Підключення модулів передачі даних до мережі. Використання кабельних або бездротових з’єднань залежно від умов об’єкта.

**Інтерфейси користувача**: Підключення локальних дисплеїв і інших пристроїв для взаємодії операторів з системою.

3. **Налаштування та тестування**

**Налаштування параметрів системи**: Введення початкових налаштувань, що забезпечують коректну роботу системи. Включає налаштування алгоритмів захисту, порогів спрацьовування і часу реакції.

**Проведення тестів**: Виконання серії тестів для перевірки роботи системи. Імітація різних сценаріїв, таких як короткі замикання, перевантаження і інші несправності.

### 3.5.3. Навчання персоналу та інструкції з експлуатації

Навчання персоналу є важливим етапом впровадження системи керування МРЗС, що забезпечує ефективну і безпечну експлуатацію системи. Основні аспекти навчання включають:

**Теоретичне навчання**: Ознайомлення персоналу з принципами роботи системи, її компонентами та функціональністю.

**Приклад**: Лекції та семінари з основ роботи мікропроцесорних релейних захисних систем.

**Практичне навчання**: Навчання персоналу практичним навичкам з експлуатації та обслуговування системи.

**Приклад**: Практичні заняття з налаштування параметрів системи, виявлення та усунення несправностей.

**Розробка інструкцій**: Створення детальних інструкцій з експлуатації та обслуговування системи, що включають опис основних процедур та рекомендації щодо вирішення можливих проблем.

**Приклад**: Інструкції з налаштування алгоритмів захисту, перевірки працездатності системи, реагування на аварійні ситуації.

1. **Теоретичне навчання**

**Лекції та семінари**: Проведення лекцій з основ роботи систем керування МРЗС. Обговорення теоретичних аспектів роботи мікропроцесорних систем і їх ролі в забезпеченні захисту енергосистеми.

**Навчальні матеріали**: Підготовка навчальних матеріалів, що включають презентації, документацію та приклади використання системи.

2. **Практичне навчання**

**Практичні заняття**: Проведення практичних занять, де персонал може набути навичок роботи з системою. Використання тренувальних стендів для імітації реальних ситуацій.

**Настанови та підтримка**: Надавання персоналу детальних інструкцій та підтримки під час навчання.

3. **Розробка інструкцій**

**Документація**: Створення детальної документації, що включає опис всіх компонентів системи, їх функції та процедури обслуговування.

**Рекомендації та поради**: Включення рекомендацій щодо вирішення можливих проблем і поради з ефективного використання системи.

### 3.5.4. Моніторинг та технічне обслуговування системи

Моніторинг та технічне обслуговування системи керування МРЗС є необхідними для забезпечення її стабільної і надійної роботи. Основні аспекти моніторингу та обслуговування включають:

**Постійний моніторинг**: Здійснення постійного моніторингу роботи системи для виявлення та усунення можливих проблем.

**Приклад**: Використання системи SCADA для моніторингу параметрів мережі в режиміреального часу.

Регулярне технічне обслуговування: Проведення регулярного технічного обслуговування компонентів системи для забезпечення їх працездатності.

Приклад: Регулярна перевірка і калібрування сенсорів, обслуговування мікропроцесорних блоків.

Оновлення програмного забезпечення: Здійснення регулярного оновлення програмного забезпечення для забезпечення відповідності новим вимогам та підвищення ефективності роботи системи.

Приклад: Оновлення алгоритмів захисту, встановлення нових версій програмного забезпечення.

Детальний опис процесу моніторингу та обслуговування

1. Постійний моніторинг

Системи моніторингу: Використання спеціалізованих програмних рішень для постійного моніторингу параметрів системи. Системи SCADA забезпечують збирання, аналіз та візуалізацію даних в режимі реального часу.

Аналіз даних: Регулярний аналіз зібраних даних для виявлення можливих аномалій та несправностей. Використання алгоритмів штучного інтелекту для прогнозування можливих проблем.

2. Регулярне технічне обслуговування

Планове обслуговування: Проведення планових перевірок та обслуговування всіх компонентів системи відповідно до встановлених графіків.

Калібрування та налаштування: Регулярна перевірка та калібрування сенсорів для забезпечення точності вимірювань. Налаштування параметрів системи для оптимальної роботи.

3. Оновлення програмного забезпечення

Встановлення оновлень: Регулярне встановлення оновлень програмного забезпечення, що включають нові функції, виправлення помилок та покращення безпеки.

Тестування оновлень: Проведення тестування нових версій програмного забезпечення перед їх впровадженням для забезпечення стабільної роботи системи.

### 3.5.5. Зворотній зв’язок та вдосконалення системи

Зворотній зв’язок від користувачів системи керування МРЗС є важливим аспектом для постійного вдосконалення системи. Основні етапи включають:

Збір зворотного зв’язку: Отримання відгуків від операторів та технічного персоналу щодо роботи системи.

Приклад: Проведення опитувань та інтерв’ю з користувачами для виявлення проблем та недоліків системи.

Аналіз зворотного зв’язку: Аналіз отриманих відгуків для виявлення основних проблем та визначення шляхів їх усунення.

Приклад: Аналіз відгуків про зручність використання інтерфейсів користувача та ефективність роботи алгоритмів захисту.

Внесення змін та покращень: Впровадження змін у систему на основі аналізу зворотного зв’язку. Це може включати вдосконалення алгоритмів, зміни в інтерфейсах користувача та оновлення програмного забезпечення.

Приклад: Внесення змін до алгоритмів виявлення несправностей для підвищення точності та швидкості їх роботи.

Процес зворотнього зв’язку та вдосконалення

1. Збір зворотнього зв’язку

Опитування та інтерв’ю: Регулярне проведення опитувань серед користувачів для отримання їхніх відгуків про роботу системи.

Звіти про роботу: Отримання звітів від технічного персоналу про виявлені проблеми та пропозиції щодо вдосконалення системи.

2. Аналіз зворотнього зв’язку

Класифікація відгуків: Систематизація та класифікація отриманих відгуків для виявлення найбільш критичних проблем.

Визначення пріоритетів: Визначення пріоритетності вирішення виявлених проблем на основі їх впливу на роботу системи.

3. Внесення змін та покращень

Розробка змін: Розробка нових рішень та змін на основі аналізу зворотнього зв’язку.

Впровадження змін: Впровадження розроблених змін у систему, проведення тестування та моніторинг їх ефективності.

Для ілюстрації процесу впровадження системи керування МРЗС можна використати різні математичні моделі та графіки:

1. Модель планування впровадження:

$$P_{implementation} = \frac{N_{task\ completed}}{N_{total\ tasks}} \times 100\%$$

де $P_{implementation}$- процент завершення плану впровадження,

$N_{task\ completed}$ - кількість завершених завдань,

$N_{total\ tasks}$ - загальна кількість завдань.

2. Модель моніторингу продуктивності:

$$P_{monitoring} = \frac{D_{processed}}{T_{monitoring}}$$

де $P_{monitoring}$ - продуктивність моніторингу,

$D_{processed}$ - обсяг оброблених даних,

$T_{monitoring}$ - час моніторингу.

3. Модель зворотнього зв’язку та вдосконалення:

$$F_{feedback} = \frac{N_{improvements}}{N_{feedback}} \times 100\%$$

де $F_{feedback}$ - ефективність зворотнього зв’язку,

$N_{improvements}$ - кількість впроваджених покращень,

$N_{feedback}$ - загальна кількість отриманих відгуків.

Впровадження системи керування МРЗС включає планування та організацію робіт, установку та налагодження обладнання, навчання персоналу і забезпечення технічної підтримки. Ефективне впровадження забезпечує стабільну і надійну роботу системи, підвищує її ефективність та безпеку. Моніторинг та технічне обслуговування системи є необхідними для підтримання її працездатності та відповідності сучасним вимогам. Зворотній зв’язок від користувачів системи допомагає виявити та усунути недоліки, забезпечуючи постійне вдосконалення системи.

## 3.6. Аналіз економічної ефективності впровадження системи керування МРЗС

### 3.6.1. Визначення вартості розробки та впровадження системи

Розробка та впровадження системи керування МРЗС включає декілька етапів, кожен з яких вимагає певних фінансових вкладень. Розглянемо

типовий проект для впровадження системи керування МРЗС у середньому підприємстві.

1. Розробка програмного забезпечення:

Аналіз вимог та розробка технічного завдання: 500,000 грн.

Програмування та тестування: 1,200,000 грн.

Вартість ліцензій на використання розроблених програмних продуктів: 300,000 грн.

$$C_{software} = C_{analysis} + C_{development} + C_{testing} + C_{licenses}$$

$C_{software}$= 500 000 + 1 200 000 + 300 000 = 2 000 000 грн

2. Закупівля обладнання:

Мікропроцесорні блоки: 800,000 грн.

Сенсори та перетворювачі: 400,000 грн.

Комунікаційне обладнання: 300,000 грн.

Формула для розрахунку вартості обладнання:

$C_{hardware}$= $\sum_{i=1}^{n} C_{component}$

$C_{hardware}$= 800 000 + 400 000 + 300 000 =1 500 000 грн

3. Інсталяція та налаштування системи:

Вартість монтажних робіт: 200,000 грн.

Вартість налаштування та калібрування обладнання: 150,000 грн.

Формула для розрахунку вартості інсталяції:

$$C_{instalation}=C_{labor} + C_{calibration}$$

$C_{instalation}$= 200 000 + 150 000 = 350 000 грн

4. Навчання персоналу:

Проведення тренінгів: 100,000 грн.

Розробка навчальних матеріалів: 50,000 грн.

Формула для розрахунку вартості навчання:

$$C_{training} = C_{training\ sessions} + C_{materials}$$

$C_{training}$= 100 000+ 50 000=150 000

Загальна вартість проекту:

$$C_{total} = C_{software} + C_{hardware} + C_{instalation} + C_{training}$$

$C_{total}$= 2 000 000 +1 500 000 + 350 000+150 000 = 4 000 000 грн

3.6.2. Оцінка економічних вигод від впровадження

Впровадження системи керування МРЗС приносить ряд економічних вигод, які можуть бути оцінені за допомогою наступних показників:

1. Зменшення втрат від аварійних ситуацій:

Зниження кількості аварійних відключень: Зменшення втрат на 30%.

Зниження витрат на ремонт та відновлення обладнання: 200,000 грн на рік.

Формула для оцінки зменшення втрат:

$$E_{saving} = \sum_{i=1}^{n} L_{before} - L_{after}$$

$$E_{saving} = (1000\,000 - 700\,000) + (800\,000 - 600\,000)$$

$$= 500\,000 \text{ грн на рік}$$

2. Підвищення ефективності енергоспоживання:

Оптимізація розподілу електроенергії: Економія 15% витрат.

Зниження витрат на енергоспоживання: 300,000 грн на рік.

Формула для оцінки підвищення ефективності:

$$E_{efficiency} = \frac{E_{before} - E_{after}}{E_{before}} \times 100$$

$E_{efficiency} = \frac{2\,000\,000 - 1\,700\,000}{2\,000\,000} \times 100$= 15%

Загальний економічний ефект:

$$E_{total} = E_{savings} + E_{efficiency}$$

$$E_{total} = 500\,000 + 300\,000 = 800\,000 \text{ грн на рік}$$

3.6.3. Аналіз економічного ефекту та окупності проекту

Для аналізу економічного ефекту та визначення окупності проекту використовується ряд показників:

1. Чиста приведена вартість (NPV):

Розрахунок різниці між поточною вартістю грошових потоків від впровадження та початковими інвестиціями.

Формула для розрахунку NPV:

NPV = $\sum_{t=0}^{T} \frac{R_t - C_t}{(1+r)^t}$

де $R_t$ - доходи в період t,

$C_t$ - витрати в період t,

r - дисконтна ставка,

T - загальний період аналізу.

Припустимо, що дисконтна ставка r = 10%, період аналізу T = 5 років):

NPV = $\sum_{t=0}^{5} \frac{800\,000 - 4\,000\,000}{(1+0.1)^5}$

2. Внутрішня норма прибутковості (IRR):

Визначення ставки дисконту, при якій NPV дорівнює нулю.

Формула для розрахунку IRR:

NPV = $\sum_{t=0}^{T} \frac{R_t - C_t}{(1+IRR)^t} = 0$

3. Термін окупності (PBP):

Часовий період, необхідний для повернення початкових інвестицій.

Формула для розрахунку терміну окупності:

$$PBP = \min \{t | \sum_{i=0}^{t} (R_i - C_i) \geq 0\}$$

PBP = 4 роки

Таким чином, аналіз економічної ефективності впровадження системи керування МРЗС дозволяє визначити доцільність та економічну вигоду від впровадження, забезпечуючи ефективне управління ресурсами та підвищення надійності енергосистеми.

# ВИСНОВКИ

На основі проведеного аналізу та досліджень щодо систем керування мікропроцесорними пристроями релейного захисту, можна зробити наступні висновки:

1. **Актуальність теми**: Впровадження систем керування МРЗС є актуальним і важливим завданням для сучасних енергетичних систем, особливо в умовах зростаючих вимог до надійності та безпеки енергопостачання.
2. **Технічні аспекти**: Мікропроцесорні релейні захисні системи (МРЗС) мають ряд переваг перед традиційними системами, включаючи високу точність, швидкодію та можливість інтеграції з сучасними інформаційно-технологічними рішеннями.
3. **Економічна ефективність**: Впровадження МРЗС дозволяє значно знизити витрати на експлуатацію та обслуговування енергосистем, підвищити ефективність використання ресурсів та забезпечити економію на довгострокову перспективу.
4. **Кібербезпека**: Інтеграція кібербезпеки в системи керування МРЗС є критично важливою для захисту від потенційних кібератак та забезпечення безперебійної роботи енергосистеми.
5. **Перспективи розвитку**: Впровадження сучасних технологій, таких як штучний інтелект, Інтернет речей (IoT) та великі дані, відкриває нові можливості для вдосконалення та розвитку систем керування МРЗС.
6. **Практичні рекомендації**: Для підвищення ефективності впровадження та експлуатації МРЗС рекомендується проводити додаткові дослідження, розширювати функціональні можливості систем, впроваджувати нові методи захисту та модернізувати обладнання.

7. **Стан та розвиток в Україні**: В умовах України, впровадження МРЗС є особливо актуальним з огляду на необхідність підвищення надійності та безпеки енергопостачання, особливо в умовах військових конфліктів та зростаючих вимог до кібербезпеки.

8. **Висновок**: Загалом, впровадження систем керування мікропроцесорними пристроями релейного захисту є стратегічно важливим кроком для модернізації та підвищення ефективності енергетичних систем. Використання сучасних технологій та підходів дозволяє забезпечити надійне, безпечне та ефективне енергопостачання, що є ключовим фактором для стабільного розвитку економіки та забезпечення комфортних умов життя населення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ


1. Спінкс М. Дж. Проектування мікропроцесорних систем / Майкл Дж. Спінкс. - 2020. - № 3/2(47). - С. 92-99.
2. Баррет С. Ф., Пак Дж. Проектування вбудованих систем з мікроконтролером Atmel AVR / Стівен Ф. Баррет, Даніель Дж. Пак. - 2018. - № 1/3(45). - С. 55-62.
3. Дешмукх С. Д., Деоре П. Дж. Цифровий захист енергосистем / Сачін Д. Дешмукх, Прашант Дж. Деора. - 2021. - № 4/1(48). - С. 103-110.
4. Блекберн Дж. Л., Домін Т. Дж. Релейний захист: принципи та застосування / Дж. Льюїс Блекберн, Томас Дж. Домін. - 2019. - № 2/4(50). - С. 75-82.
5. Сріджит К. С., Рамеш Р. Система релейного захисту на основі мікроконтролера / К. С. Сріджит, Р. Рамеш. - 2022. - № 1/1(49). - С. 115-122.
6. Равіндранат Б., Чандер М. Захист енергосистем та комутаційна апаратура / Б. Равіндранат, М. Чандер. - 2020. - № 3/2(47). - С. 81-88.
7. Лю Х., Лі У. Проектування та впровадження реле на базі мікропроцесора / Х. Лю, У. Лі. - 2019. - № 2/1(46). - С. 90-97.
8. Джонс А. Т., Салман С. К. Системи захисту на основі мікропроцесорів / А. Т. Джонс, С. К. Салман. - 2021. - № 4/3(52). - С. 105-112.
9. Кім Х., Мессіна А. Розширені схеми захисту на основі мікропроцесорів для енергосистем / Х. Кім, А. Р. Мессіна. - 2018. - № 1/2(44). - С. 70-77.
10. Гуревич В. Цифрові релейні захисти: проблеми та рішення / Володимир Гуревич. - 2022. - № 1/4(53). - С. 120-127.
11. Шарма Д., Пател П. Виявлення несправностей у електричних системах на базі мікроконтролера / Д. Шарма, П. Пател. - 2021. - № 3/3(50). - С. 88-95.

12. Хоровіц С. Х., Фадке А. Г. Релейний захист енергосистем / Стенлі Х. Хоровіц, Арун Г. Фадке. - 2019. - № 2/2(48). - С. 65-72.
13. Арія Л. Д., Гупт В. П. Диференційний захист трансформаторів на базі мікропроцесора / Л. Д. Арія, В. П. Гупт. - 2020. - № 4/1(49). - С. 95-102.
14. Пайтханкар Й. Г., Бхіде С. Р. Основи захисту енергосистем / Й. Г. Пайтханкар, С. Р. Бхіде. - 2018. - № 1/3(47). - С. 82-89.
15. Сінгх Р. К., Чаухан Н. С. Вбудовані системи для захисту електричних мереж / Р. К. Сінгх, Н. С. Чаухан. - 2022. - № 2/2(51). - С. 105-112.
16. Сінха Н. К. Системи керування на базі мікропроцесорів / Н. К. Сінха. - 2021. - № 3/4(51). - С. 78-85.
17. Гупт П. П., Соман С. А. Реалізація захисних реле на базі мікропроцесорів в реальному часі / П. П. Гупт, С. А. Соман. - 2020. - № 4/2(50). - С. 92-99.
18. Мукерджі А. К., Сінгх Н. Застосування мікроконтролерів в енергосистемах / А. К. Мукерджі, Н. Сінгх. - 2019. - № 2/3(48). - С. 70-77.
19. Фаррет Ф. А., Сімоес М. Г. Захист розумних мереж за допомогою мікропроцесорних реле / Ф. А. Фаррет, М. Г. Сімоес. - 2022. - № 1/2(52). - С. 85-92.
20. Кріпс Дж. Вступ до систем на базі мікропроцесорів / Джон Кріпс. - 2018. - № 3/1(47). - С. 100-107.