МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет інженерії та енергетики
Кафедра електрифікації, автоматизації виробництва та інженерної екології

Кваліфікаційна робота
на правах рукопису
УДК 621.359.4

Любченко Сергій Олегович.

КВАЛІФІКАЦІЙНА РОБОТА

Аналіз комп'ютерного релейного захисту ліній електропередачі
(тема роботи)

141 «Електроенергетика, електротехніка та електромеханіка»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр

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

Любченко С. О.
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи

Савченко Л.Г.
(прізвище, ім'я, по батькові)
к.і.н., доцент кафедри електрифікації,
автоматизації виробництва та інженерної екології
(науковий ступінь, вчене звання)

Житомир – 2025

АНОТАЦІЯ

Любченко С. О. Аналіз комп'ютерного релейного захисту ліній електропередачі. Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 141 – Електроенергетика, електротехніка та електромеханіка – Поліський національний університет, Житомир, 2025.

Впровадження комп'ютерного релейного захисту ліній електропередачі є ключовим елементом підвищення надійності та безпеки енергосистем. Постійний аналіз та вдосконалення алгоритмів захисту, а також інтеграція з сучасними інформаційними технологіями, є необхідними для забезпечення ефективного функціонування електричних мереж. Проведено аналіз алгоритмів захисту лінії електропередачі, що є необхідною умовою для їх вдосконалення та адаптації до мінливих умов роботи енергосистеми.

Ключові слова: електрична лінія передачі, надійність та безперебійність електропостачання, алгоритми захисту електромереж.

ABSTRACT

Liubchenko S. O. Analysis of Computer-Based Relay Protection of Power Transmission Lines. Qualification work for obtaining a Master's degree in specialty 141 – Power Engineering, Electrical Engineering and Electromechanics – Polissia National University, Zhytomyr, 2025.

The implementation of computer-based relay protection for power transmission lines is a key element in enhancing the reliability and safety of power systems. Continuous analysis and improvement of protection algorithms, as well as integration with modern information technologies, are necessary to ensure the effective functioning of electrical networks. An analysis of power transmission line protection algorithms has been conducted, which is a necessary condition for their improvement and adaptation to the changing operating conditions of the power system.

Keywords: power transmission line, reliability and continuity of power supply, power grid protection algorithms.

ЗМІСТ

ВСТУП

Комп'ютерний релейний захист (КРЗ) електромереж являє собою передову технологію, що забезпечує швидке та селективне виявлення та відключення пошкоджених ділянок електричної системи. Заміна традиційних електромеханічних реле на цифрові пристрої з програмним забезпеченням значно підвищила ефективність та надійність систем захисту.

Основною перевагою КРЗ є можливість інтеграції складних алгоритмів та логік, що дозволяє реалізувати більш чутливий та точний захист. Комп'ютерні реле здатні аналізувати велику кількість даних, отриманих від датчиків струму та напруги, а також враховувати різноманітні фактори, такі як режим роботи мережі та характер пошкодження. Це забезпечує більш ефективне розрізнення між нормальними режимами роботи та аварійними ситуаціями, мінімізуючи хибні спрацьовування та пошкодження обладнання.

Крім того, КРЗ надає можливість дистанційного моніторингу та управління системою захисту, що значно полегшує експлуатацію та діагностику. Збір та аналіз даних про роботу реле дозволяє оперативно виявляти та усувати проблеми, запобігаючи виникненню серйозних аварій.

Впровадження КРЗ є важливим кроком у підвищенні надійності та ефективності електромереж, сприяючи стабільній та безперебійній роботі енергетичної системи в цілому. Постійний розвиток технологій та алгоритмів КРЗ обіцяє ще більшу ефективність та надійність у майбутньому, забезпечуючи **стабільне електропостачання для споживачів.**

Мета: Проаналізувати сучасний стан комп’ютерного релейного захисту, порівняти його з традиційними методами, висвітлити основні переваги, недоліки та практичні аспекти впровадження стратегії захисту в різних умовах.

Предмет дослідження: аналіз ефективності та обмежень комп’ютерного релейного захисту на базі мікропроцесорних систем, з акцентом на точність вимірювань, швидкість спрацьовування, інтеграцію з комунікаційними

мережами та стійкість до завад; визначення ключових факторів, що впливають на надійність системи, та розробка практичних рекомендацій щодо мінімізації ризиків та економічної обґрунтованості впровадження.

Об’єкт дослідження: комп’ютерний релейний захист на базі мікропроцесорних систем, його алгоритмічні та апаратні складові, процеси збору та аналізу сигналів, а також взаємодія з комунікаційними мережами в контексті енергопостачання.

Перелік публікацій автора за темою дослідження :

1. Ступак А. А., Любченко С. О.

АЛГОРИТМ УСУНЕННЯ НЕСПРАВНОСТЕЙ РЕЛЕЙНОГО ЗАХИСТУ НА ОСНОВІ БАЗИ ЗНАНЬ «СТУДЕНТСЬКІ ЧИТАННЯ – 2025» 30 жовтня 2025 року м. Житомир

2. Любченко С. О., Волошин В. О.

МАТЕМАТИЧНІ ОСНОВИ АЛГОРИТМІВ РЕЛЕЙНОГО ЗАХИСТУНаукові читання – 2025: збірник тез доповідей науково-практичної конференції за підсумками І-го туру Всеукраїнського конкурсу студентських наукових робіт з галузей знань і спеціальностей. 23 квітня 2025 р. Житомир: Поліський національний університет, 2025. Том 2.

3. Любченко С. О.

ПРАВИЛО КОРЕЛЯЦІЇ АГРЕГАЦІЇ ЗА ЧАСОМ ВЕНЕРГЕТИЦІ:СУТНІСТЬ ТА ЗНАЧЕННЯ «Біоенергетичні системи» IX Міжнародна науково-практична конференція, Житомир, Україна, 19-20. 11. 2025

РОЗДІЛ 1
КОМП'ЮТЕРНИЙ РЕЛЕЙНИЙ ЗАХИСТ: ПЕРЕВАГИ, ВИКЛИКИ ТА НЕДОЛІКИ У СУЧАСНИХ СИСТЕМАХ

1.1 Розвиток комп’ютерного захисту.

Галузь комп’ютерного захисту розпочалася з спроб з’ясувати, чи можуть функції захисту енергосистем здійснюватися за допомогою цифрового комп’ютера. Такі дослідження розпочалися у 1960-ті роки, період, під час якого цифровий комп’ютер повільно й системно замінював багато традиційних інструментів аналітичного інженерного забезпечення електропостачання. Проблеми короткого замикання, відпуску потоку потужності та стабільності — рішення яких було головним завданням планувальників енергосистем — вже були перетворені на комп’ютерні програми, замінюючи DC-дошки та мережеві аналізатори. Захист вважали наступною перспективною та захоплюючою областю для комп’ютеризації. Одразу було ясно, що цифрові комп’ютери того періоду не могли задовольнити технічні потреби швидкодіючих функцій захисту. Також не було економічного стимулу робити це. Комп’ютери були на порядки дорожчі. Проте перспектива розробки та випробування алгоритмів захисту була привабливою для декількох дослідників. Через таку інертну, переважно академічну цікавість ця дуже плідна галузь була започаткована. Еволюція комп’ютерів за ті роки настільки стрімко розвивалася, що алгоритмічна досконаліть, потрібна для програм захисту, зрештою знайшла відповідність у швидкості та економічності сучасних мікрокомп’ютерів; тому на сьогодні комп’ютерні реле пропонують найкраще економічне та технічне рішення для проблем захисту — у багатьох випадках єдино практичне рішення. Справді, ми стоїмо на початку ери, в якій комп’ютерний захист став повсякденністю, і він додатково вплинув на розвиток ефективних інструментів для моніторингу та керування системами живлення в реальному часі [1].

1.2 Від механіки до цифрових систем: історія комп'ютерного релейного захисту.

Одне з перших опублікованих робіт про комп'ютерний захист досліджувало досить цікаву ідею: захист усієї апаратури в підстанції мав би здійснювати один комп'ютер.1 Без сумніву це було зумовлено високою ціною комп'ютерів того часу (1960-ті роки), і не існувало жодного економічно доцільного способу використати кілька комп'ютерів як заміну звичайним реле, які були мінімум в один порядок дешевші за належний комп'ютер. Крім того, швидкість обчислень сучасних комп'ютерів була занадто повільною для високошвидкісного захисту, тоді як споживання потужності комп'ютерів — надто великим. Незважаючи на ці очевидні недоліки — які відображали тодішній стан розвитку комп'ютерів — наведене посилання досліджувало декілька алгоритмічних деталей захисту досить ретельно, і навіть сьогодні надає добру основу для новачків, що занурюються у складнощі сучасних практик захисту.

Декілька інших робіт були опубліковані приблизно в той же час і призвели до алгоритмічного розвитку захисту високовольтних ліній передач [2,3]. Рано було помітно, що функція захисту лінії передачі (зокрема відстань) — більше ніж будь-яка інша — є цільовою для інженерів з релейної справи через її широке використання в енергосистемах, відносно високу вартість та функціональну складність. Ці ранні дослідники розпочали вивчення алгоритмів захисту за відстанню, яке продовжується до сьогоднішнього дня без перерви. Ці дослідження привели до важливих нових висновків щодо фізичної природи процесів захисту та обмежень, до яких їх можна підштовхувати. Найімовірніше, що реалізація захисту за відстанню на комп'ютерах вже опанована більшістю дослідників до тепер, і будь-які нові досягнення в цій галузі, ймовірно, з'являться завдяки використанню покращеного апаратного забезпечення для реалізації добре зрозумілих алгоритмів захисту за відстанню.

Інший абсолютно інший підхід до захисту за відстанню було запропоновано в останні роки[4,5]. Він зазвичай базується на використанні біжучих хвиль, ініційованих пошкодженням, для оцінки відстані до пошкодження. Захисні реле з подорожніми хвилями вимагають відносно високих частот для відбору сигналів напруги та струму. Хоча реле на основі подорожніх хвиль не надали переконливих переваг перед іншими принципами захисту з точки зору швидкості та точності, вони застосовувалися в кількох випадках у світі з задовільною продуктивністю. Алгоритми локалізації пошкоджень за допомогою біжучих хвиль були також розроблені, і є повідомлення про хороший досвід використання цих пристроїв.

На додачу до розробки алгоритмів захисту за відстанню розпочалася рання робота з апаратурним захистом за принципом диференціального захисту[6–8]. Ці ранні посилання визнавали факт, що порівняно з завданням захисту лінії, алгоритми диференціального захисту менш вимогливі до обчислювальної потужності. Функція гармонійного обмеження додає деяку складність до задачі захисту трансформаторів, і проблеми, пов’язані з насиченням струмових трансформаторів чи інші неточності продовжують мати рішення, які не є простими у комп’ютерних системах захисту так само, як і у звичайних реле. Тим не менш, завдяки розвитку алгоритмів захисту за відстанню та диференціального захисту, можна стверджувати, що можливість комп’ютерних реле забезпечувати продуктивність не менше за звичайні реле була встановлена ще на початку 1970-х.

Значні досягнення в апаратному забезпеченні комп’ютерів з того часу відбулися. Розміри, споживання потужності та вартість комп’ютерів знизилися на порядки, водночас швидкість обчислень зросла на кілька порядків. Поява 16-розрядних (а нещодавно 32-розрядних) мікропроцесорів та комп’ютерів на їх основі зробила високошвидкісний комп’ютерний захист технічно досяжним, водночас вартість реле на базі комп’ютера стала порівнянною з вартістю звичайних реле. Ця тенденція продовжується дотепер — і, можливо, з певною меншою інтенсивністю, але продовжуватиметься й у майбутньому. Насправді

зараз уже добре встановлено, що найдешевший та технічно найбільш досконалий спосіб будівництва систем захисту майбутнього (за винятком деяких простих та недорогих функціонально реле) — це за допомогою цифрових комп'ютерів. Давня ідея об'єднати кілька функцій захисту в одному апаратному комплексі1 також частково відродилася — у сучасних багатофункціональних реле.

Зі зручними перспективами наявності доступних реле на основі комп'ютера, які можна призначати під конкретні функції захисту, увага швидко усталилася на можливостях інтеграції їх у підстанційні мережі, можливо, навіть у системну мережу з використанням швидких широкосмугових комунікаційних мереж. Ранішні роботи з цієї теми визнавали кілька переваг, які випливають з такої можливості реле для зв'язку [9,10].

1.3. Вигоди та цінність комп'ютерного релейного захисту в сучасних електромережах.

Коротко варто підсумувати переваги комп'ютерних реле та деякі особливості цієї технології, які вимагають нових операційних підходів. Серед переваг, які забезпечують комп'ютерні реле, такі:

1.3.1 Економічна ефективність комп'ютерного релейного захисту у сучасних мережах.

За інших рівних умов вартість реле є головним чинником його прийнятності. На ранніх етапах комп'ютерного захисту вартість комп'ютерного реле була у 10–20 разів більшою за вартість звичайних реле. З роками вартість цифрових комп'ютерів стабільно знижувалася; водночас їх обчислювальна потужність (за виміром часу виконання інструкцій та довжиною слова) значно зросла. Вартість звичайних (аналогових) реле постійно зростала за той самий період, головним чином через деякі конструктивні покращення, але також через інфляцію та відносно низький обсяг виробництва та продажів. Передбачається, що за однакової продуктивної

потужності вартість найскладніших цифрових реле з програмним забезпеченням буде приблизно такою ж, як у звичних систем захисту. Очевидно, існують певні звичні реле — наприклад захист лінійного струму понад струм — настільки дешеві, що дешевше замінити їх комп'ютерними реле поки не вигляє можливим, за умови, що вони не входять до багатофункціонального реле. Проте для великих систем захисту конкурентоспроможна вартість комп'ютерних реле стала важливим чинником.

1.3.2 Самодіагностика систем цифрового релейного захисту та її надійність.

Комп'ютерне реле може бути запрограмоване для постійного моніторингу кількох своїх апаратних та програмних підсистем, тим самим виявляючи будь-які збої, які можуть з'явитися. Воно може бути спроектоване так, щоб виходити з ладу в безпечному режимі — тобто само знищитися з обслуговуваної точки зору, якщо виявлено несправність — та надсилати сигнал-повідомлення до системного центру. Ця риса комп'ютерних реле, ймовірно, найістотніший технічний аргумент на користь комп'ютерного захисту. Відмова реле — не часте явище, зважаючи на велику кількість реле, що існують у енергомережі. Іншими словами, у більшості випадків катастрофічних збоїв системи причиною розгортання серії подій, що призводять до відмови, можна віднести помилкову роботу реле. У деяких випадках це є неправильне застосування реле до даної захисної задачі, але переважно причина полягає у збої компоненту реле, що веде до його неправильної роботи та збоїв у енергобезпеці. Очікується, що завдяки самодіагностиці, відбуватиметься раніше виявлення збоїв компонентів реле, і їх можна буде відремонтувати до того моменту, коли вони призведуть до неправильної роботи. У цьому сенсі, хоча комп'ютерні реле є більш складними за електромеханічні або твердотільні реле (і тому потенційно більш схильними до відмов), як система вони мають вищий рівень доступності. Зрозуміло, реле

не може виявити всі відмови компонентів — зокрема ті за периметром релейної системи.

1.3.3 Співіснування системи та цифрового середовища: перспективи інтеграції.

Цифрові комп'ютери та цифрові технології стали основою більшості систем у підстанціях. Вимірювання, зв'язок, телеметрія та керування — усе це комп'ютеризовані функції. Багато перетворювачів вимірювань (струмові та напругові трансформатори) переходять на цифрові системи. Оптоволоконні лінії завдяки своїй стійкості до електромагнітних перешкод (EMI) швидше за все стануть середовищем передачі сигналів між точками у підстанції; це технологія, що особливо підходить для цифрового середовища. У підстанціях майбутнього комп'ютерні реле будуть дуже вписуватися у загальну картину: вони зможуть приймати цифрові сигнали від новіших трансдюсерів та оптоволоконних каналів та інтегруватися з комп'ютерними системами управління та моніторингу підстанції. Власне, без комп'ютерного захисту цифрові трансдюсери та оптоволоконні системи для передачі сигналів не мали б життєздатних систем у підстанції.

1.3.4 Адаптивний захист: функційна гнучкість та динамічна адаптація.

Оскільки цифровий комп'ютер може бути запрограмований на виконання кількох функцій за умови наявності потрібних вхідних та вихідних сигналів, реле-комп'ютер може легко взяти на себе багато інших задач підстанції. Наприклад, вимірювання та моніторинг потоків і напруги у трансформаторах та лініях передач, керування відкриттям та закриттям автоматів вимикання та розмикання, надання резерву для інших пристроїв, що відмовили — це все функції, які може взяти на себе реле на базі комп'ютера. Захист потребує інтенсивної обчислювальної діяльності, коли на системі відбувається несправність. Ця інтенсивна активність, у кращому разі, займає

дуже малу частку часу експлуатації реле — менше десятої частини відсотка. Таким чином, реле-комп'ютер може виконувати ці інші задачі практично без додаткових витрат. За рахунок програмування та можливості зв'язку, комп'ютерне реле надає ще одну перевагу, яку не так легко реалізувати в традиційній системі — здатність змінювати характеристики (налаштування) реле залежно від стану системи.

Серед очікуваних переваг комп'ютерного захисту більшість з них вийшла на практиці завдяки здатності комп'ютерів до обміну даними з різними рівнями ієрархії керування. Повне розкриття можливостей комп'ютерного захисту стало можливим лише з появою широкої мережі зв'язку, що охоплює великі підстанції. Ідеальним середовищем для передавання даних вважалось би оптоволоконні мережі через його чудову стійкість до перешкод та здатність обробляти високошвидкісні потоки даних. Здається, що вигоди такої мережі зв'язку даруються у багатьох сферах, і з появою все більшої кількості таких ліній, самі комп'ютерні реле та їхні вимірювальні можливості стануть цінними самі по собі. Якщо ж розвинені мережі комунікації відсутні, багато переваг комп'ютерного захисту так і залишаться нереалізованими.

Інші питання, що стосуються технології комп'ютерного захисту, також варто згадати. Було помічено, що цифрова комп'ютерна технологія за останні двадцять років розвивалася дуже швидко. Це означає, що апаратне забезпечення комп'ютерів має відносно короткий термін служби. Апаратне забезпечення змінюється значно кожні кілька років, і питання підтримки старого обладнання стає критичним. Існуючі реле працюють добре багато років — деякі понад 30 років. Такі реле підтримувались протягом тривалого часу. Важко уявити подібну тривалість служби для обладнання на базі комп'ютера. Можливо, рішенням стане модульність апаратного забезпечення комп'ютера; комп'ютери та периферія одного сімейства можуть забезпечити довший строк служби з заміною кількох модулів кожні кілька років. За умови, що це можливо зробити без суттєвих змін у системі захисту, таке може бути прийнятним компромісом для тривалої служби. Та очевидні наслідки швидкої

зміни комп’ютерних систем очевидні виробникам та користувачам цієї технології.

Програмне забезпечення також створює свої проблеми. Програми для захисту (або критичні їх частини) зазвичай пишуться на нижчих рівнях мов програмування, таких як асемблер. Причина цього — необхідність максимально ефективно використати наявний час після виникнення несправності. Регістри захисту зазвичай обмежується обчисленнями та вводу-виводом. Вищі мови зазвичай менш ефективні для чутливих до часу застосувань. Можливо, з часом зі збільшенням швидкості виконання інструкцій у комп’ютерах більш високорівневі мови зможуть замінити значну частину програмування на асемблері в захисті. Проблема машинних мов полягає в тому, що вони не переносяться між комп’ютерами різних типів. Деякий перехід між різними моделями однієї родини може існувати, але навіть тут зазвичай бажано розробляти нове програмне забезпечення, щоб використати різні можливості різних моделей. Оскільки вартість програмного забезпечення є дуже значною частиною розробки комп’ютерного захисту, узгодженість програмного забезпечення є суттєвою проблемою.

На ранніх етапах розвитку комп’ютерного захисту існували деякі занепокоєння щодо суворого середовища електричних підстанцій, в яких реле має функціонувати. Екстремальні температури, вологість, забруднення, а також дуже сильні EMI потрібно було передбачати.

Ще одна проблема, яку часто піднімали користувачі комп’ютерних реле, стосується широкого спектру завдань, які ці реле можуть обробляти. Мало комп’ютерних реле, які не вимагали б дуже великої кількості налаштувань перед встановленням та введенням в експлуатацію. Де організація має достатній персонал для роботи з комп’ютерними реле, робота з налаштуванням не становить проблеми. Проте там, де організація мала би бути мала та спеціалізований персонал для цих застосувань не виправданий, правильне та постійне обслуговування налаштувань реле стає складним завданням. До того ж, якщо реле різного виробника використовується в одній

організації, може знадобитися експерт, який зможе працювати з пристроями різних виробників. Декілька робочих груп та технічних комітетів IEEE Power Engineering Society намагалися розробити спільний інтерфейс для реле різних виробників, але це завдання видається занадто складним і значних успіхів у цьому напрямку не досягнуто[11].

Висновки по першому розділу.

Комп'ютерний захист електросистеми, як відповідь на потребу швидкого та надійного реагування енергосистем; сучасні цифрові реле забезпечують економічно виправдані рішення навіть за рахунок високої технічної ефективності.

Історично сформувалися варіанти захисту за відстанню та диференціальний захист, що зумовили основу для впровадження комп'ютерних систем у реальному часі та розвиток багатофункціональних реле.

Основні переваги: зниження вартості при зростанні потужності обчислень, самодіагностика, інтеграція з цифровим середовищем керування, гнучкість налаштувань та адаптивний захист, можливість централізованого моніторингу та обміну даними.

Основні виклики й обмеження: швидкість та довговічність апаратного забезпечення, підтримка старого обладнання, сумісність програмного забезпечення, потреба у висококваліфікованому персоналі та відсутність універсальних стандартів між виробниками.

Перспектива: при подальшому розвитку апаратного забезпечення, мереж передачі даних (наприклад, оптоволоконні технології) та адаптивних алгоритмів комп'ютерні реле стануть нормою в сучасних підстанціях, але потребують модульності та узгодженості між виробниками.

РОЗДІЛ 2

ОСНОВНІ СКЛАДОВІ КОМП'ЮТЕРНИХ РЕЛЕ ТА ЇХ ПРИЗНАЧЕННЯ

2.1 Архітектура комп'ютерних реле.

Комп'ютерні реле складаються з підсистем із чітко визначеними функціями. Хоча конкретне реле може відрізнятися за деталями, ці підсистеми найімовірніше будуть інтегровані в його конструкцію у тій чи іншій формі. Нижче описано підсистеми реле та їхні функції.

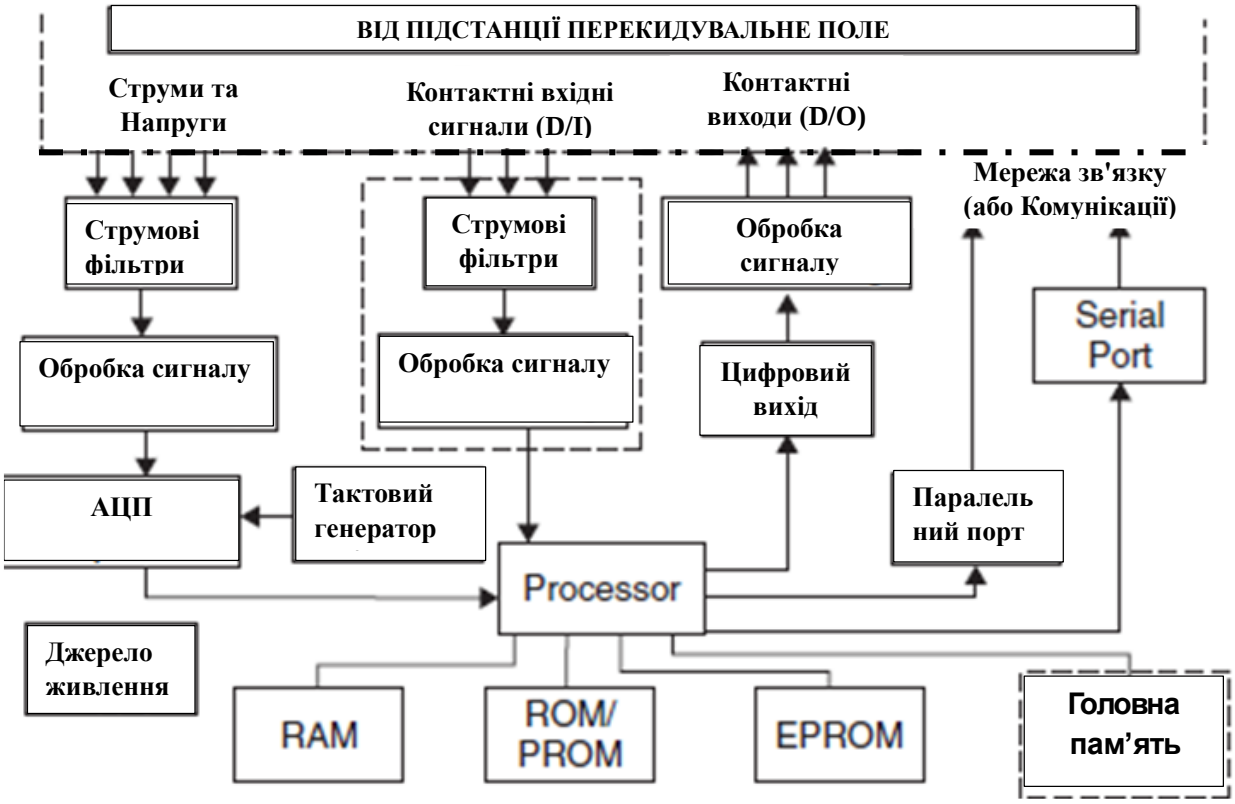

Рисунок 2.1. Підсистеми релейного комп'ютера. Пунктирна лінія зверху показує межу відкритого розподільчого пристрою. Все інше обладнання знаходиться всередині будівлі управління.

Блок-схема на Рис. 2.1 показує основні підсистеми комп'ютерного релея. Процесор є центральним у його організації. Він відповідає за виконання релейних програм, підтримку різних часових функцій та комунікацію з

периферійним обладнанням. На схемі подано кілька типів пам’яті. Доступ до пам’яті (RAM) використовується для збереження вхідних зразків даних, які надходять і обробляються. RAM також може використовуватися для буферизації даних для подальшого зберігання на більш постійному носієві. До того ж RAM потрібна як швидка тимчасове сховище під час виконання алгоритмів реле.

Пам’ять тільки для читання (ROM) або програмована пам’ять тільки для читання (PROM) використовується для постійного зберігання програм. Іноді програми можуть виконуватися безпосередньо з ROM, якщо час читання достатньо короткий. Якщо це не так, програми повинні копіюватися з ROM до RAM під час ініціалізаційного етапу, після чого реальне виконання в режимі реального часу відбувається із RAM. Ера або EPROM необхідні для збереження певних параметрів (таких як налаштування реле), які можуть змінюватися час від часу, але після встановлення повинні залишатися фіксованими, навіть якщо живлення комп’ютера перервано. Підходить або пам’ять типу Core, або RAM із підтримкою батареї для цього завдання.

Великої ємності EPROM становить бажаний елемент комп’ютерного релея. Така пам’ять була б корисною як архівний носій даних, для збереження таблиць даних про збої, часово-мічених журналів подій та аудит-логів запитів та змін налаштувань, зроблених у реле. Основний фактор тут — вартість такої пам’яті. Вартість пам’яті знизилася настільки, що архівне збереження осцилографічних даних та послідовності подій у релях великого масштабу стало можливим.

2.2 Аналогова схема входу.

Розглянемо далі аналогову входову систему. На початку варто зауважити, що Рис. 2.1 базується на використанні традиційних трансдюсерів. Якщо використовуються електронні ТТ та ТПТ (CTs та CVTs), вхідні кола можуть бути значно відмінними, і дані можуть надходити безпосередньо у пам’ять процесора. Вхідні реле — це струми та напруги, а також цифрові сигнали, які

свідчать про стан контактів. Аналогові сигнали мають бути перетворені у напруги, придатні для подальшого перетворення в цифрову форму. Це виконується за допомогою аналого-цифрового перетворювача (ADC). Зазвичай вхід ADC обмежується повзунком від ±10 В. Сигнали струму та напруги, що надходять з вторинних обмоток трансформаторів струму та напруги, повинні бути відповідним чином масштабовані. Найбільші можливі рівні сигналів мають бути передбачені, а відношення між значенням rms та піком сигналу має бути враховане. У більшості випадків не потрібно враховувати високочастотні перехідні явища, оскільки їх усувають фільтри антиаліасингу з низькою частотою відсікання. Виняток становлять волнові реле, які використовують високі частоти компонентів з високою частотою (traveling wave). Для таких реле масштабування сигналів має бути таке, щоб увесь вхідний сигнал з його найбільшим очікуваним високочастотним компонентом не перевищував діапазон вхідного ADC.

Вхідні дані струму мають перетворюватися на напруги — наприклад, за допомогою резистивних шунтів. Оскільки вторинні струми нормального ТТ можуть становити сотні ампер, потрібні шунти опором кілька міліомів для створення бажаної напруги для ADC. Альтернативна конфігурація — використати допоміжний трансформатор струму, щоб знизити струм до нижчого рівня. Проте будь-які неточності в допоміжному трансформаторі струму вноситимуться у загальну помилку перетворення, і мають бути мінімізовані. Допоміжний трансформатор струму виконує ще одну функцію: забезпечує електричну ізоляцію між вторинною ланкою основного СТ та входовою системою комп’ютера. У цьому випадку шунт може бути заземлений посередині, щоб забезпечити збалансований вхід до наступних підсилювачів та фільтрів. Такі концепції ілюстровано на Рис. 2.2(a) та (b).

З’єднання з трансформатором напруги зображено на Рис. 2.2(c). Для кожного інструмента або реле передбачена запобіжна ланка, і може бути передбачена подібна ланка для комп’ютерного релея. Нормальна напруга на вторинній обмотці трансформатора напруги становить 67 В RMS для з’єднання

фази з нейтраллю. Вона може знижуватися до бажаного рівня за допомогою опірного дільника напруги, розрахованого на забезпечення достатнього опору джерела для подальших етапів фільтрів та підсилювачів.

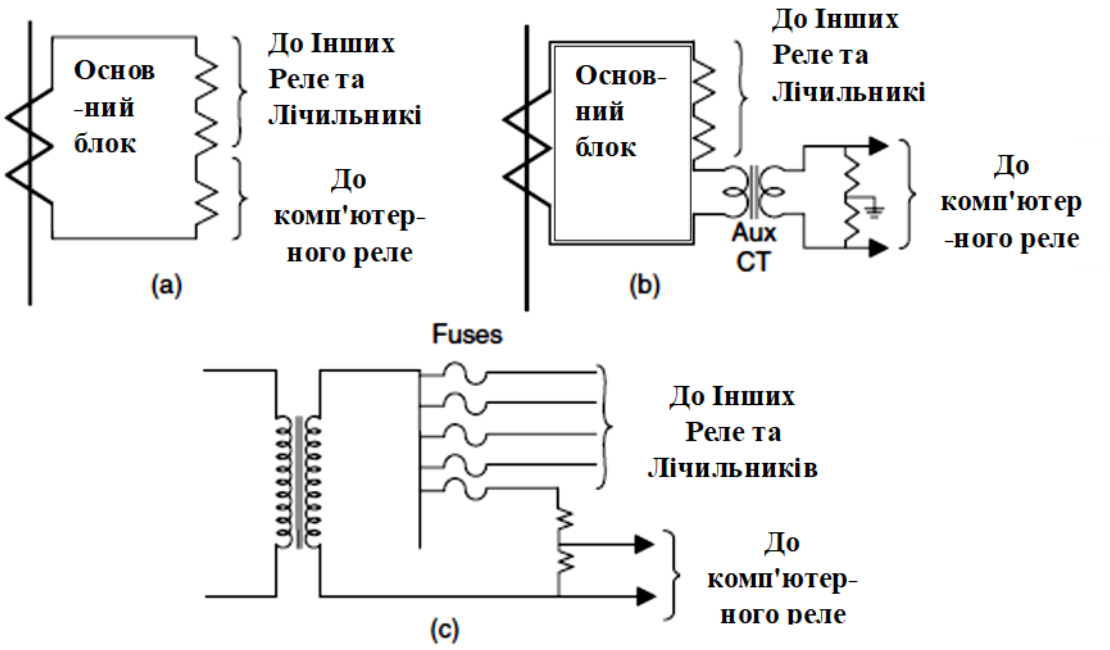

Рисунок 2.2 Масштабування сигналів струму та напруги для подачі на реле. (a) Пряме підключення у вторинній обмотці основного ТС. (b) Використання допоміжного ТС. (c) Трансформатор напруги та потенційний дільник.

Хоча допоміжний трансформатор напруги може бути використаний у цьому випадку для додаткової ізоляції, це не є обов’язковим. Цифрові входи до комп’ютерного реле зазвичай — це стан контактів, надходить від інших реле або підсистем усередині підстанції. Якщо інші підсистеми комп’ютерні, ці сигнали можуть надходити до комп’ютерного реле без спеціальної обробки. Винятком може бути оптично ізольована схема, яка забезпечує ізоляцію між двома системами. Коли цифрові входи отримуються від контактів у дворі (або у контрольному залі), необхідно застосувати фільтрацію струмопровідних імпульсів та (або) оптичну ізоляцію для ізоляції комп’ютерного реле від суворого середовища підстанції.

Придушення імпульсних перенапруг в проводці, підключеній до будь-якої системи захисту, є спеціалізованою темою з великою кількістю літератури [12,13]. Перенапруги високої напруги та з великим запасом енергії передаються в проводку, яка з'єднує струмові, напругові та цифрові входи з системою захисту.

Перенапруги виникають через пошкодження та комутаційні операції в енергосистемі, або через певні типи комутацій у приміщенні керування. Наприклад, іскріння контактів в індуктивних схемах захисту та керування всередині приміщення керування виявилось джерелом дуже значних збурень.[14] Придушення цих перенапруг вимагає ретельного заземлення та екранування провідників та обладнання, а також фільтрації нижніх частот. Нелінійні енергопоглинаючі металооксидні варистори (MOV) також можуть бути використані. Фільтри придушення перенапруг необхідні для вхідної та вихідної проводки, а також для проводів живлення.[12]

ADC та фільтр антиаліасінгу (згладжування недоліків дискретизації), пов’язані з процесом зразків. Наразі достатньо усвідомити їхню функцію у загальному процесі реле. Фільтри антиаліасінгу — це аналогові фільтри низьких частот, розроблені під конкретну частоту дискретизації. Інстанси зразків визначає такт зразкування, який повинен видавати імпульси з фіксованою частотою. На кожен момент часу, визначений тактом, відбувається перетворення з моментального значення аналогового вхідного сигналу (напруга або струм) у цифрову форму за допомогою ADC, і це доступне процесору. Оскільки реле зазвичай потребує кількох входів, під час кожного моменту зразку виконується кілька перетворень. Бажано (хоча й не обов’язково) щоб усі зразки були одночасно зафіксовані, що означає або дуже швидке перетворення та передача на процесор кожного зразка, або одночасне зразкування та утримання сигналів на однаковий момент для подальшої обробки за повільнішого режиму.

Як видно, у загальному випадку, можливе кілька входів, і кілька перетворень робляться на кожен момент зразку. Це характерно для систем із

мультиплексованим аналоговим входом. Третій варіант, технічно можливий, але дорогий — використати окремі ADC для кожного каналу. Тенденції розвитку ADC та зниження вартості вказують на те, що використання окремих ADC для кожного сигналу стане переважним. Ці варіанти проілюстровано на рисунку 1.3.

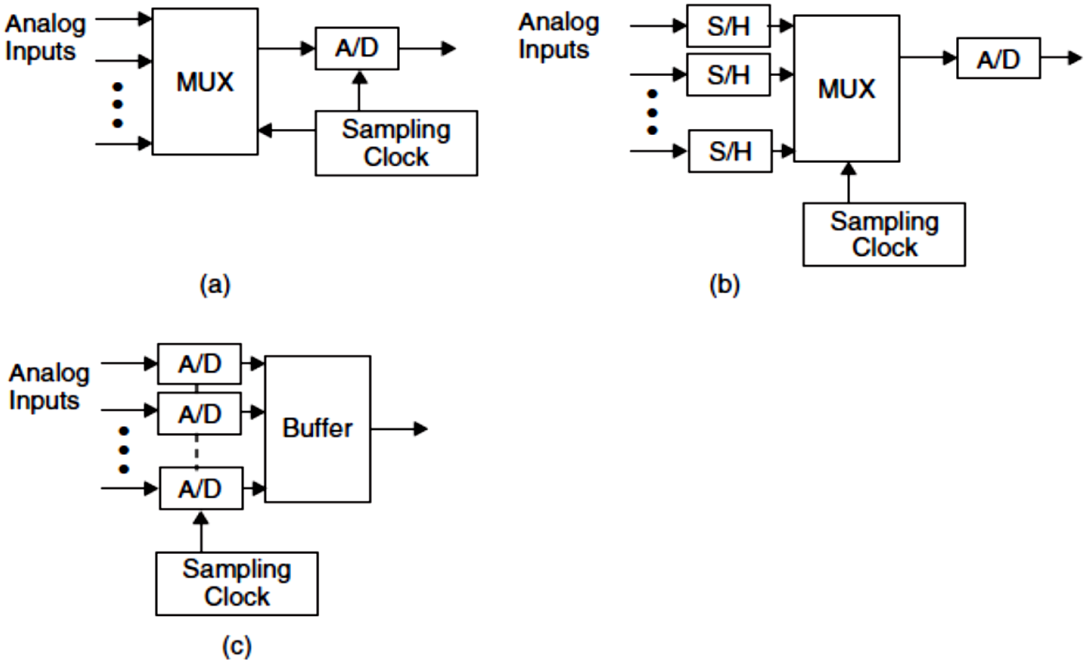

Рисунок 2.3 Процес дискретизації множинних сигналів та його організація. (a) Один АЦП з мультиплексованим входом. (b) Схема вибірки-зберігання, додана до кожного каналу. (c) Окремий АЦП для кожного каналу.

Повертаючись до Рис. 2.1, цифровий вихід від процесора використовується для забезпечення релейного виводу у формі відкритих або закритих контактів. Паралельний вихідний порт процесора надає одне слово (зазвичай дві байти) для цих виходів. Кожен біт може використовуватися як джерело для одного контакту. Вихідний біт комп’ютера є сигналом рівня TTL і буде оптично ізольований перед приведенням до високошвидкісної багатоконтактної лінії чи тиристорів, які, у свою чергу, можуть запускати зовнішні пристрої, такі як сигналізація, обмотки роз'єднувачів, контроль переносника тощо.

Наскільки відзначено на Рис. 2.3, блок живлення зазвичай являє собою один вхідний DC/DC перетворювач з кількома виходами, живлений від станційної батареї. Вхід зазвичай становить 125 В постійного струму, а вихід може бути 5 BDC та ±15 BDC. Зазвичай 5 В необхідні для живлення логіки, тоді як 15 В потрібні для аналогових коливань. Станційна батарея, звісно, постійно заряджається від станційного змінного струму.

Висновки по другому розділу.

Комп'ютерне реле побудоване з чітко визначених підсистем, основну роль виконує процесор, який виконує програми, керує часом та периферією.

Пам'ять: RAM для збереження даних та тимчасових буферів; ROM/PROM для постійних програм; EPROM/Era для збереження налаштувань; перспективи використання великих за обсягом EPROM для архівів журналів за зниження вартості.

Аналогове-цифрові входи та масштабування: ADC з зазвичай ±10 В, антиаліас-фільтри; можливе застосування допоміжних CT для ізоляції та зменшення струмів.

Цифрові входи та захист: ізоляція (оптична), фільтрація імпульсів, придушення перенапруги в лініях керування та захисту.

Обробка сигналів: варіанти з одним АЦП із мультиплексуванням, або кількома АЦП на канал; майбутнє очікувань на використання окремих ADC через зниження вартості.

Вихідні інтерфейси: TTL-виходи з оптичною ізоляцією для безпечного керування зовнішнім обладнанням.

Живлення: DC/DC з кількома виходами (5 В для логіки та ±15 В для аналогових), вхід ~125 BDC; батарея заряджається від станційного змінного струму.

Висновок: архітектура балансуватиме між вартістю, точністю та швидкістю обробки; ізоляція та захист критично важливі для надійної роботи в умовах підстанцій.

РОЗДІЛ 3

КОМП'ЮТЕРНИЙ РЕЛЕЙНИЙ ЗАХИСТ ЛІНІЙ ЕЛЕКТРОПЕРЕДАЧІ

Історично, алгоритми релейного захисту ліній представляють більшу частину ранньої діяльності в комп’ютерному релейному захисті. Дослідники вважали, що релейний захист ліній є найбільшим викликом, а також має найбільшу можливість для покращення продуктивності. Розглянемо деякі алгоритми і зробимо деякі загальні висновки про характеристики кількох типів алгоритмів.

Низку алгоритмів можна розглядати як обчислення імпедансу, в яких основні частотні компоненти як напруг, так і струмів отримуються з вибірок. Відношення відповідних напруг і струмів потім надають імпеданс до місця пошкодження. Продуктивність усіх цих алгоритмів залежить від отримання точних оцінок основних частотних компонентів сигналу на основі невеликої кількості вибірок. У межах цього класу алгоритмів для оцінки основних частотних компонентів використовуються як методи Фур'є, так і методи апроксимації кривих. Якщо б досліджуваний сигнал був чистою синусоїдою, то практично кожен запропонований алгоритм працював би ідеально. Відмінність між алгоритмами цього типу полягає в їхній поведінці, коли в напрузі та струмі присутні сигнали, відмінні від основної частоти.

Інший тип алгоритмів базується на R-L моделі лінії передачі, представленій у вигляді послідовного з'єднання. Замість використання моделі однієї частоти, такої як імпеданс, цей підхід має очевидну перевагу, дозволяючи використовувати всі сигнали, які задовольняють диференціальному рівнянню, для оцінки R та L моделі. Алгоритми релейного захисту ліній порівнювалися, виходячи з припущення, що струми та напруги складаються з основної гармоніки та певних комбінацій гармонік.[15] Ми стверджуємо, що з огляду на всі ситуації, в яких має працювати реле лінії – тобто, змінна конфігурація системи, змінний кут виникнення пошкодження

тощо – нефундаментальні частотні компоненти, які бачить реле, слід розглядати як випадковий процес. Характер цього випадкового процесу є тоді основним питанням при оцінюванні продуктивності алгоритму релейного захисту.

Наступні позначення використовуватимуться при обговоренні всіх алгоритмів:

y(t) = Миттєве значення сигналу змінного струму, напруги або струму;

y_k = k-те значення вибірки y(t);

ω_0 = Основна частота енергосистеми в радіанах на секунду;

Δt = Фіксований інтервал між вибірками, тобто;

y_k = y(kΔt);

θ = Кут основної частоти між вибірками, тобто $\theta = \omega_0 \Delta t$.

Щоб проілюструвати деякі загальні риси алгоритмів, заснованих на хвильовій моделі, припустимо, що y(t) має вигляд:

$$y(t) = Y_c \cos \omega_0 t + Y_s \sin \omega_0 t \tag{3.1}$$

де Y_c та Y_s є дійсними числами. Крім того, припустимо, що вибірки беруться в −Δt, 0, та Δt.

$$\begin{aligned} y_{-1} &= y(-\Delta t) \\ y_0 &= y(0) \\ y_1 &= y(\Delta t) \end{aligned} \tag{3.2}$$

Вибірки пов'язані з амплітудами Y_c та Y_s через

$$\begin{bmatrix} y_{-1} \\ y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} cos\theta & -sin\theta \\ 1 & 0 \\ cos\theta & -sin\theta \end{bmatrix} \begin{bmatrix} Y_c \\ Y_s \end{bmatrix} \tag{3.3}$$

де θ — кут основної частоти між вибірками. Очевидно, що двох вибірок достатньо для визначення Y_c та Y_s, якщо сигнал описується рівнянням (3.1). Наприклад, $Y_c = y_0$ та Ys = $(y_1 - y_0\ cos\theta)/\ sin\theta$ задовольняють останні два рівняння в (3.3). Використання трьох вибірок є спробою забезпечити деяку стійкість до додаткових членів (гармоніки або випадкових членів) у рівнянні (3.1). Таким чином, метод найменших квадратів для розв'язання рівняння (3.3) видається доречним тоді отримаємо розв'язок за методом найменших квадратів:

$$\begin{bmatrix} \hat{Y}_c \\ \hat{Y}_s \end{bmatrix} = \begin{bmatrix} 1 + 2cos^2\theta & 0 \\ 0 & 2sin^2\theta \end{bmatrix}^{-1} \begin{bmatrix} cos\theta & 1 & cos\theta \\ -sin\theta & 0 & sin\theta \end{bmatrix} \begin{bmatrix} y_{-1} \\ y_0 \\ y_1 \end{bmatrix}$$

$$\hat{Y}_c = \frac{[y_1 cos\theta + y_0 + y_{-1} cos\theta]}{1+2cos^2\theta} \tag{3.4}$$

$$\hat{Y}_s = \frac{y_1 - y_{-1}}{2sin\theta} \tag{3.5}$$

Більш загальним розв’язками рівняння (3.3) (не обов'язково розв’язками, отриманим методом найменших квадратів) є вираз у вигляді

$$Y_c = \hat{Y}_c + c_1[y_1 - 2y_0 cos\theta + y_{-1}] \tag{3.6}$$

$$Y_s = \hat{Y}_s + c_2[y_1 - 2y_0 cos\theta + y_{-1}] \tag{3.7}$$

де c_1 та c_2 – довільні константи. Вирази в дужках в рівняннях (3.6) та (3.7) дорівнюють нулю, якщо сигнал описується рівнянням (3.1). Два з ранніх алгоритмів відповідають певним виборам c_1 при $c_2 = 0$. Алгоритм Манна-Моррісона [16] відповідає $c_2 = 0$ та

$$c_1 = \frac{-cos\theta}{1+2cos^2\,\theta}$$

тоді як алгоритм Prodar 70 [3] відповідає c_2 = 0, і

$$c_1 = [\frac{1}{2sin^2\,\theta} - \frac{-cos\theta}{1+2cos^2\,\theta}]$$

Оригінальні версії обох алгоритмів також базуються на припущенні, що θ є достатньо малим, щоб наближення малих кутів, cosθ ≈ 1 та sinθ ≈ 0, були доречними та представляли собою апроксимації похідних членів з вибірок.

Для того, щоб дослідити деякі загальні властивості всіх подібних алгоритмів, розглянемо версію з c_1 та c_2, що дорівнюють нулю, та проаналізуємо обчислення з пливом часу та надходженням нових вибірок. Алгоритм, заснований на останніх трьох вибірках y_{k-1}, y_k, y_{k+1}, матиме наступний вигляд:

$$\hat{Y}_c^{(k)} = \frac{[y_{k+1}cos\theta + y_k + y_{k-1}cos\theta]}{1+2cos^2\,\theta} \tag{3.8}$$

$$\hat{Y}_c^{(k)} = \frac{[y_{k+1} + y_{k-1}]}{2sin^2\,\theta} \tag{3.9}$$

де верхній індекс k вказує на обчислення, зосереджені на k-му зразку. Якби y(t) була чистою синусоїдою, як у Рівнянні (3.1), тоді (фактично, для будь-якого вибору c_1 та c_2)

$$\hat{Y}_c^{(k)} = Y_c cosk\theta + Y_s sin\theta \tag{3.10}$$

$$\hat{Y}_s^{(k)} = Y_s cosk\theta + Y_c sin\theta \tag{3.11}$$

У полярній формі

$$\left|Y^{(k)}\right| = \sqrt{(Y_c^{(k)})^2 + (Y_s^{(k)})^2} \tag{3.12}$$

$$\varphi^{(k)}=tan^{-1}\left[\frac{Y_s^{(k)}}{Y_c^{(k)}}\right] = tan^{-1}\left[\frac{\mathrm{Y_s}}{\mathrm{Y_c}}\right] - k\theta \tag{3.13}$$

З рівняння (3.13) видно, що обчислений вектор має правильну амплітуду, але обертається, тобто кут $\varphi^{(k)}$ зменшується на кут θ у кожній точці відліку. Залежно від застосування, може знадобитися корекція обертання. Якщо для розрахунку імпедансу необхідно використати відношення векторів напруги та струму, то обертання взаємно знищиться при діленні.

Алгоритм, описаний рівняннями (3.8) і (3.9), має вікно даних у три відліки, тобто, коли стає доступним новий відлік, найстаріший з трьох значень відліку відкидається, а нове значення відліку включається в обчислення. Кожен відлік потім використовується в трьох обчисленнях: один раз як y_{k+1}, один раз як yk і один раз як y_{k-1}. Обчислення в рівняннях (3.8) і (3.9) повинні бути завершені мікропроцесором до того, як буде згенеровано наступний відлік. На практиці насправді потрібно обчислити значно більше, як ми побачимо далі.

На рисунку 3.1 показано рухоме вікно даних з трьох відліків для ідеальної форми сигналу напруги, дискретизованої з частотою 12 відліків на цикл. Напруга миттєво зменшується в момент виникнення пошкодження. Вікно, позначене як W1, містить три відліки даних до пошкодження, вікна W2 та W3 містять дані як до, так і після пошкодження, а вікно W4 містить лише дані після пошкодження. Обчислення за рівняннями (3.8) та (3.9) дадуть правильні фази у вікнах, що містять чисті відліки до або після пошкодження. Однак дані у вікнах W2 та W3 не можуть бути апроксимовані чистою синусоїдою, і обчислені фази мають мало сенсу. Проте, можна перевірити, що обчислені фази не відповідають трьом відлікам. Слід зазначити, що вікно з двох відліків

завжди буде відповідати даним, хоча відповідність одному відліку до пошкодження та одному після пошкодження є однаково безглуздою.

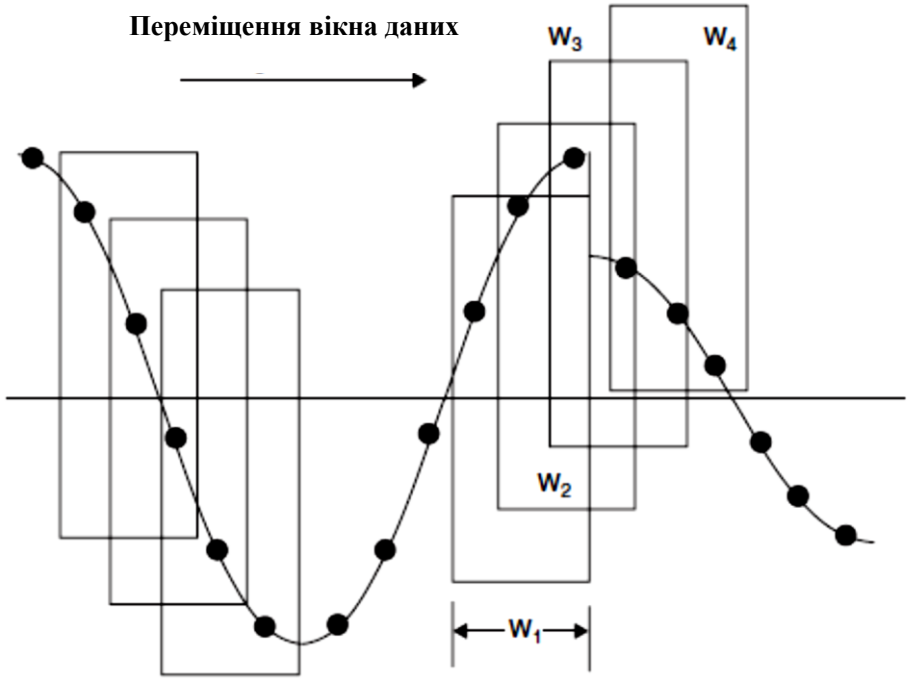

Рисунок 3.1 Переміщення трьох зразків вікна даних на формі сигналу напруги. W1 – доаварійне, W2 та W3 містять як доаварійні, так і післяаварійні зразки, а W4 – чисто післяаварійне.

З простого алгоритму з трьома зразками та рисунка можна зробити кілька висновків. Час вибірки, Δt , визначає кількість часу, яку мікропроцесор має на виконання обчислень. У прикладі з 12 зразками на цикл, Δt = 1,3889 мс для системи 60 Гц. У системі 50 Гц 20 зразків на цикл дають Δt = 1 мс. Існуючі алгоритми використовують частоту вибірки від чотирьох до 64 зразків на цикл. Очевидно, що висока частота вибірки вимагає більш потужних процесорів або особливо простих алгоритмів[17].

Друга проблема стосується довжини вікна даних. Враховуючи, що результати, отримані коли вікно містить як зразки до збою, так і після збою, є ненадійними, видається доцільним чекати до того часу, коли результати стануть надійними (коли вікно містить лише пост збійні дані) перед

ухваленням релейних рішень. Важливо розробити методику, яка виявлятиме цю перехідну ділянку. Відповідь прикладного алгоритму на цій перехідній ділянці залежить від параметрів C_1 та C_2 в рівняннях (3.6) і (3.7). Оскільки довше вікно потребує більше часу, щоб пройти через момент збою, очевидно, що швидші рішення можна приймати за допомогою алгоритмів з коротким вікном. На жаль здатність алгоритму відкидати сигнали з частотою, що відрізняється від фундаментальної, залежить від довжини вікна даних. Іншими словами, існує вроджений обернений зв'язок між швидкістю релейної дії та її точністю. Хоча алгоритм, представлений рівняннями (3.8) і (3.9), дає правильну фазу, якщо сигнал y(t) задається рівнянням (3.1), ми повинні визнати, що сигнал, який підлягає вибірку, точніше задається так:

$$y(t) = \mathrm{Y_c} cos\omega_0 t + \mathrm{Y_s} sin\omega_0 t + \varepsilon(t) \qquad (3.14)$$

Для оцінки продуктивності лінійного реле необхідно розуміти природу сигналу ε(t) е рівнянні (3.14).

3. 1 Джерела похибок.

Струм та напруга після виникнення пошкодження не мають форми чистої синусоїди основної частоти з багатьох причин. Найбільш передбачуваним негармонійним компонентом є експоненціально затухаюча складова, яка може бути присутня у формі хвилі струму. Для послідовної R-L моделі лінії, зображеної на рисунку 3.2, припускаючи нульовий струм до пошкодження та усталений струм пошкодження у вигляді $I cos\ (\omega_0 t - \varphi)$, миттєвий струм при пошкодженні в момент часу t_0 задається виразом

$$i(t) = Icos(\omega_0 t - \varphi) - [Icos(\omega_0 t_0 - \varphi] e^{-(t-t_0)R/L} \qquad (3.15)$$

Другий член в рівнянні (3.15) експоненціально згасає з часовою константою лінії. Цей член є основною причиною тимчасового пере відкриття у швидкодіючих реле, і його необхідно усунути, якщо необхідно досягти комп'ютерного релейного захисту на швидкості частки циклу. Для типової лінії надвисокої напруги (EHV) часова константа знаходиться в діапазоні 30–50 мс. Початкова амплітуда експоненціальної складової може бути такою ж великою, як пік струму короткого замикання, як показано на Рисунку 3.3. Ситуація може бути ще складнішою поблизу великого генератора. Експоненціальний член не є помилкою для алгоритмів, заснованих на описі лінії диференціальним рівнянням, оскільки експонента задовольняє диференціальне рівняння. Якщо відома часова константа лінії, то згасання можна усунути за допомогою зовнішнього фільтра або навіть програмно (для алгоритмів, які розглядають експоненціальне згасання як помилку). Залежність часової константи від опору короткого замикання робить видалення менш ефективним для коротких замикань з високим опором.

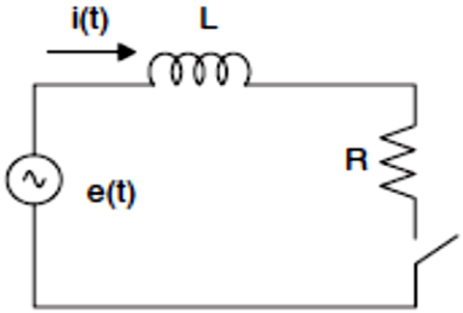

Рисунок 3.2. Послідовна R-L модель лінії передачі

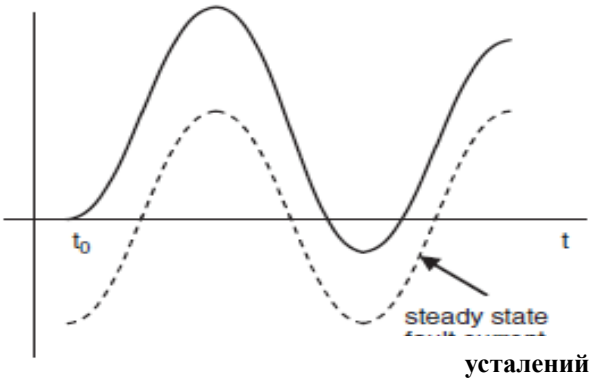

Рисунок 3.3 Струм короткого замикання. Пунктирна крива - усталений струм короткого замикання.

Інші нефундаментальні частотні компоненти не так легко видалити, оскільки їх не так легко передбачити. Перетворювачі струму та напруги додають деякі з цих сигналів. Наприклад, ємнісний трансформатор напруги має перехідну характеристику на різку зміну напруги, показану на рисунку 3.1. Можуть бути присутні високочастотні сигнали, пов'язані з відбиттям хвильових форм між шиною та місцем пошкодження. Нелінійна поведінка дуги замикання може генерувати гармонічні сигнали. Крім того АЦП (аналого-цифровий перетворювач) вносить похибки, зумовлені найменш значущим бітом при перетворенні та через похибки синхронізації, тобто вибірки не є точно Δt секунд одна від одної. Більшість цих сигналів мають значний високочастотний вміст і можуть бути зменшені за допомогою фільтра захисту від перекриття спектру (anti-aliasing filter).

Оскільки форма хвилі дискретизується з частотою f_s= 1/Δt Гц, теорема Найквіста про дискретизацію передбачає, що сигнал має бути відфільтрований фільтром із частотою зрізу f_s/2, щоб уникнути накладання спектрів (аліасингу). Такий фільтр усуне високочастотні сигнали похибок, описані вище, але внесе власну перехідну характеристику; крім того, дрейф значень компонентів з часом у таких фільтрах (особливо в активних реалізаціях таких фільтрів) є джерелами помилок.

Нарешті, сама енергосистема є джерелом сигналів не основної частоти. Розглянемо однофазну модель трьох ліній і двох генераторів, показану на рисунку 3.4. Припускається, що лінії ідентичні, але одне джерело є сильним, а інше – слабким. Вважається, що лінії – це 100 миль типової лінії 765 кВ. Якщо пошкодження виникає на 60% захищеної лінії, напруга, що бачить реле, показана на рисунку 3.5. Плавна крива – це напруга, яка була б, якщо б конденсатори були видалені з рисунку 3.5. Видно, що включення конденсаторів створило щонайменше два сигнали не основної частоти. Ці не основні частоти є власними частотами системи, які збуджуються застосуванням пошкодження. Оскільки мережа є фіксованою, якщо місце

розташування пошкодження залишається постійним, з цього випливає, що власні частоти визначаються місцем розташування пошкодження.

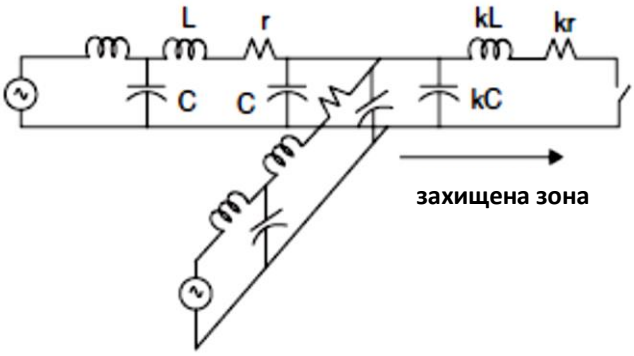

Рисунок 3.4 Модель однофазної системи електропостачання

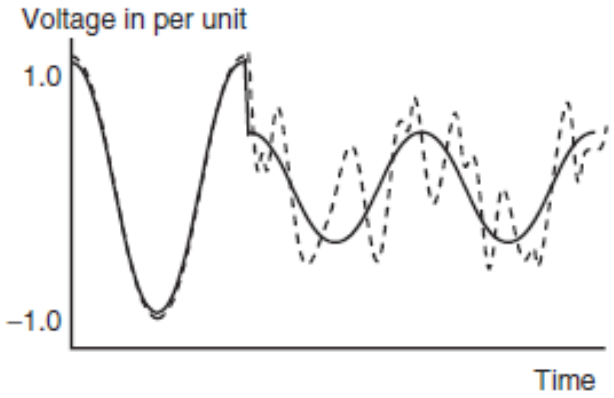

Рисунок 3.5. Криві напруги для пошкодження на 60% довжини лінії

На рисунку 3.6 зображено сімейство кривих напруги, отриманих шляхом зміни кута виникнення пошкодження. Видно, що фаза не основних частотних компонент є функцією кута виникнення пошкодження. Як показано на рисунку 3.7, при зміні місця розташування пошкодження змінюється частота не основних частотних компонент. Подібний ефект може бути отриманий шляхом зміни структури мережі за місцем пошкодження. В літературі описано експерименти на моделі енергосистеми, що поєднують вплив зміни структури мережі, що живить пошкодження, а також типу і місця пошкодження.[18] Висновок полягає в тому, що значна частина сигналу не основної частоти ε(t) в рівнянні (3.14), принаймні для ліній високої напруги, зумовлена самою

мережею. Ці сигнали залежать від місця пошкодження та характеру системи, що живить місце пошкодження, і, як такі, не є передбачуваними.

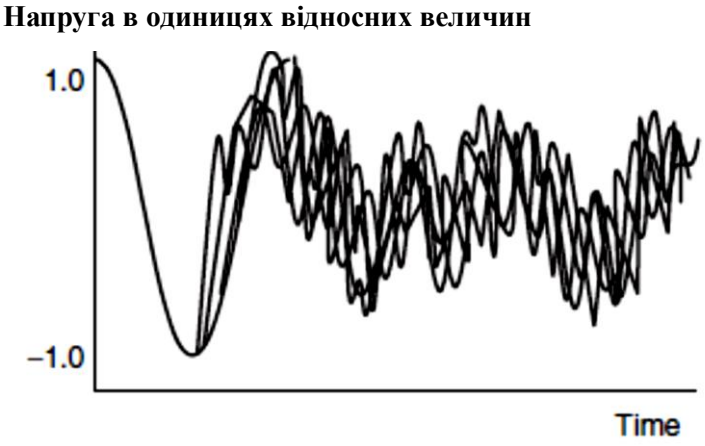

Рисунок 3.6. Сімейство кривих напруги для пошкоджень на 60% довжини лінії

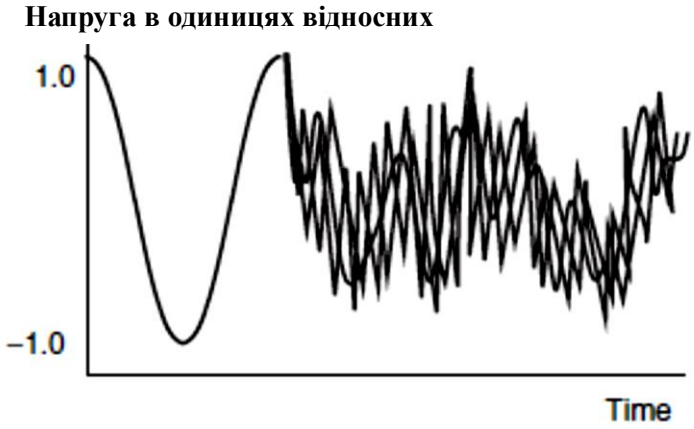

Рисунок 3.7 Сімейство кривих напруги для різних місць пошкодження

Якщо змоделювати кут падіння пошкодження як випадкову фазу, а місце розташування пошкодження та структуру мережі як механізм, що генерує випадкову частоту, то ми можемо розглядати спектр потужності як спектр потужності сигналу в ε(t) в рівнянні (314). Слід зазначити, що кожна реалізація такого процесу є досить детермінованим на вигляд сигналом, як, наприклад, показано на рисунку 3.5. (Це суперечить інтуїції, якщо очікується, що реалізація випадкового процесу виглядатиме зашумленою.) Випадковість

присутня тому, що, враховуючи ансамбль моментів часу, коли реле має спрацювати, частоту та фазу сигналу передбачити неможливо.

Розглядаючи ε(t) в як випадковий процес, цілком бажано розглядати анти-елайзинговий фільтр та алгоритм разом як фільтрацію цього випадкового процесу. Частотна характеристика алгоритму, таким чином, є важливою частиною процесу фільтрації. Щоб отримати частотну характеристику алгоритму, нам слід обчислити відгук алгоритму (фаза для рівнянь (3.6) та (3.7), наприклад) коли вхідний сигнал має вигляд $e^{j\omega t}$.

3.2 Алгоритми захисту електромереж реалізовані на цифрових реле.

Ефективний захист електромереж є критично важливим для забезпечення надійності та стабільності електропостачання. В основі багатьох захисних пристроїв лежать алгоритми, що аналізують поточні значення напруги та струму для виявлення аномальних режимів, таких як короткі замикання. Якщо узагальнити рівняння (3.14), щоб включити ряд відомих сигналів, в тому числі компоненти основної частоти, можна сформулювати загальну задачу оцінювання коефіцієнтів відомих сигналів. Отримане рішення охоплює ряд алгоритмів релейного захисту. Важливою складовою цих алгоритмів є апроксимація кривих, що описують зміни електричних параметрів.

Сучасні релейні пристрої еволюціонували від електромеханічних до цифрових, що дозволило значно розширити функціональність та гнучкість реалізованих алгоритмів. Цифрові реле здатні обробляти складніші сигнали, реалізовувати логічні функції, аналізувати параметри електромережі та приймати рішення на основі заданих критеріїв. Це дозволяє реалізовувати адаптивні алгоритми захисту, які враховують зміни в режимі роботи мережі та навантаження.

3.3.1 Алгоритми апроксимації кривих.

Забезпечення надійного та ефективного захисту електромереж є критично важливим завданням, яке потребує точного і швидкого реагування захисних

пристроїв на аварійні ситуації. Ключовим елементом налаштування цих пристроїв є крива захисту, що визначає час спрацювання захисту залежно від величини струму короткого замикання. Оскільки точне відтворення теоретичної кривої захисту на практиці часто неможливе або недоцільне, виникає необхідність у застосуванні алгоритмів апроксимації[19,20].

Апроксимація кривих захисту передбачає заміну складної математичної залежності простішою, яка дозволяє з достатньою точністю відтворити необхідну характеристику спрацювання захисту, водночас мінімізуючи обчислювальні витрати та полегшуючи реалізацію. Для апроксимації часто використовуються поліноми, кусково-лінійні функції, а також сплайни. Вибір конкретного алгоритму залежить від вимог до точності, швидкодії та складності реалізації.

Поліноміальна апроксимація, хоча і проста у реалізації, може призводити до значних похибок на краях діапазону значень струму. Кусково-лінійна апроксимація, у свою чергу, дозволяє досягти високої точності за рахунок збільшення кількості лінійних сегментів, що ускладнює обчислення. Сплайни, зокрема кубічні, забезпечують гладку апроксимацію з меншою кількістю точок, що робить їх привабливим варіантом для застосування у мікропроцесорних пристроях захисту.

Удосконалення алгоритмів апроксимації кривих захисту електромереж є актуальним напрямком досліджень, спрямованим на підвищення ефективності та надійності захисних пристроїв. Пошук оптимального балансу між точністю апроксимації, обчислювальною складністю та вартістю реалізації є ключовим фактором для забезпечення стабільної та безпечної роботи електроенергетичної системи.

3.3.2 Алгоритми Фур'є.

Алгоритми, засновані на перетворенні Фур'є, відіграють ключову роль у сучасних системах захисту електромереж. Їх використання дозволяє

виокремити з часового сигналу компоненти різних частот, що є критично важливим для виявлення та класифікації аномальних режимів роботи.

Основна перевага алгоритмів Фур'є полягає у їхній здатності виявляти гармоніки та міжгармоніки, які можуть вказувати на наявність несправностей, таких як нелінійне навантаження, коротке замикання, або дефекти ізоляції.

Аналіз частотного спектру струму та напруги дає можливість оперативно ідентифікувати тип пошкодження та розробити відповідні заходи захисту.
Існують різні варіації алгоритмів Фур'є, що використовуються для захисту електромереж. До них належать дискретне перетворення Фур'є (Discrete Fourier Transform, DFT) та його швидкі версії, такі як швидке перетворення Фур'є (Fast Fourier Transform, FFT). Останні забезпечують значно більшу швидкість обчислень, що є критичним для реального часу реагування системи захисту.

Не зважаючи на численні переваги, алгоритми Фур'є мають певні обмеження. Зокрема, вони чутливі до змін частоти вхідного сигналу та можуть вимагати значного обчислювального ресурсу. Тому, сучасні розробки направлені на вдосконалення алгоритмів Фур'є, адаптацію їх до умов роботи електромереж та інтеграцію з іншими методами захисту для забезпечення більш ефективного та надійного захисту.

Отже, алгоритми Фур'є є потужним інструментом у арсеналі інженерів-енергетиків, що дозволяє підвищити надійність та безпеку функціонування сучасних електроенергетичних систем.

3.3.3 Алгоритми Фур’є з коротшими вікнами.

Класичні алгоритми Фур'є вимагають аналізу значного обсягу даних, що призводить до відносно довгого часу затримки перед спрацюванням захисту. Це може мати критичні наслідки при виникненні серйозних пошкоджень, таких як короткі замикання, які потребують негайного відключення пошкодженої ділянки мережі[21].

Розробка та впровадження алгоритмів Фур'є з коротшими вікнами стає все більш актуальною тенденцією. Ці алгоритми використовують різноманітні методи, такі як зважене вікно, адаптивні фільтри, та вдосконалені методи обробки сигналів, що дозволяють отримувати достовірні результати аналізу, використовуючи менший обсяг даних.

Переваги використання алгоритмів Фур'є з коротшими вікнами очевидні: зменшення часу затримки спрацювання захисту, підвищення чутливості системи до швидкозмінних процесів, та покращення загальної стабільності електромережі. Проте, слід зазначити, що скорочення вікна аналізу може призвести до зниження точності визначення частотних компонентів сигналу та збільшення впливу шумів. Тому, розробка таких алгоритмів вимагає ретельного балансування між швидкістю реагування та точністю аналізу.

Враховуючи зростаючу складність та інтелектуалізацію сучасних електромереж, подальші дослідження та вдосконалення алгоритмів Фур'є з коротшими вікнами є перспективним напрямком для підвищення надійності та безпеки енергопостачання. Це, безумовно, сприятиме стабільному розвитку енергетичної галузі та забезпеченню безперебійної роботи критичної інфраструктури.

3.3.4 Алгоритми рекурсивних форм.

Рекурсивні алгоритми, характеризуючись здатністю до самовідтворення та обчислення на основі менших підзадач, демонструють значний потенціал для оперативного аналізу складних сигналів у електромережах. Їх застосування дозволяє ефективно виявляти аномалії, швидко оцінювати масштаби пошкодження та ініціювати захисні дії. Зокрема, рекурсивні фільтри Калмана, завдяки своїй адаптивній природі, здатні придушувати шум та точно оцінювати параметри мережі, навіть в умовах нелінійних спотворень.

Крім того, рекурсивні форми обчислень можуть бути використані для створення децентралізованих систем захисту. Кожен вузол мережі, оснащений рекурсивним алгоритмом, здатний локально аналізувати інформацію та

приймати рішення про захист, мінімізуючи залежність від централізованого управління та підвищуючи стійкість системи до відмов.

Втім, реалізація рекурсивних алгоритмів потребує врахування обчислювальних витрат та забезпечення їхньої стабільності. Незважаючи на це, подальші дослідження та розвиток обчислювальної потужності відкривають широкі можливості для впровадження рекурсивних форм захисту електромереж, сприяючи підвищенню їхньої надійності та безпеки.

3.3.5 Алгоритми диференціальних рівнянь.

Основною перевагою використання алгоритмів диференціальних рівнянь є їхня здатність реагувати на зміни в електромережі більш швидко та адаптивно, ніж традиційні методи. Це дозволяє мінімізувати час впливу несправності на систему та зменшити потенційні збитки. Крім того, ці алгоритми можуть бути застосовані для виявлення різних типів несправностей, включаючи короткі замикання, обриви та міжфазні перенапруги.

Проте, використання алгоритмів диференціальних рівнянь у захисті електромереж також має певні виклики. Точність та швидкість алгоритму значною мірою залежить від точності математичної моделі електромережі та обчислювальної потужності пристрою захисту. Крім того, необхідність розв'язання диференціальних рівнянь в реальному часі вимагає використання високопродуктивних процесорів та оптимізованих алгоритмів розв'язання[21].

Незважаючи на ці виклики, алгоритми диференціальних рівнянь представляють собою перспективний напрямок розвитку систем захисту електромереж. Їхня здатність до швидкої та адаптивної реакції робить їх важливим інструментом для забезпечення надійності та безпеки сучасних енергосистем. Подальші дослідження та розробки у цій області спрямовані на підвищення точності моделей, оптимізацію алгоритмів та розробку нових методів застосування диференціальних рівнянь у захисті електромереж.

3.3.6 Алгоритми фільтра Калмана.

Фільтр Калмана – це рекурсивний алгоритм, який використовує серію вимірювань, що містять статистичні шуми, для отримання оптимальної оцінки стану системи. Він успішно застосовується для прогнозування та згладжування даних у різних областях, включаючи системи управління, навігацію та економіку. У сфері електроенергетики, фільтр Калмана може використовуватися для оцінки стану мережі, зокрема, для прогнозування напруги, струму та частоти в різних точках мережі[22].

Застосування фільтра Калмана для захисту електромереж дає змогу:

1. Підвищити точність оцінки стану мережі: Алгоритм комбінує інформацію з різних датчиків, враховуючи похибки вимірювання, що дозволяє отримати більш точну картину поточного стану мережі;
2. Виявляти аномалії та передбачати аварійні ситуації: На основі історичних даних та прогнозованого стану, фільтр Калмана може виявляти відхилення від нормального режиму роботи, сигналізуючи про потенційні проблеми;
3. Покращити ефективність роботи захисних пристроїв: Знаючи поточний стан мережі з високою точністю, можна більш ефективно налаштовувати захисні пристрої, мінімізуючи наслідки можливих аварій.

Висновки по третьому розділу.

У главі розглянуто алгоритми лінійного релейного захисту. Виявили, що фундаментальним обмеженням усіх розглянутих алгоритмів є наявність непередбачуваних нефундаментальних частотних складових у напрузі та струмі одразу після виникнення короткого замикання. Чи намагається алгоритм оцінити фундаментні частотні складові напруги та струму для визначення імпедансу, використовуючи послідовну R–L модель лінії, ці немоделювані сигнали спричинюють помилки в оцінці місця пошкодження. Роль експоненційного зсуву в струмі при пошкодженні є важливим фактором

при розрізненні алгоритмів. Якщо зсув видаляють до подачі на релейний алгоритм за допомогою аналогового фільтрування або окремої підпрограми, то алгоритми типу Фур'є мають значні переваги з погляду простоти та якості роботи. Алгоритми на основі диференціальних рівнянь не вимагають видалення зсуву, але мають певні обмеження продуктивності для довгих високовольтних ліній, якщо структура системи в шині джерела ускладнена. Якщо припустити, що похибки в вимірюваних струмі та напрузі зазнають істотних змін у своїх статистичних характеристиках протягом інтервалу релейної дії, може бути доцільним підхід з фільтром Калмана. Слід враховувати збільшене обчислювальне навантаження разом із проблемою потреби в детальнішій моделі похибок.

Необхідно також враховувати додаткові властивості релейних алгоритмів, такі як їх здатність визначати тип пошкодження. Використання перетворення Кларка або симетричних компонент забезпечує метод визначення типу пошкодження для наведених алгоритмів. Наслідки неправильної класифікації пошкодження є додатковим фактором при виборі алгоритму.

Нарешті, у всіх відстаневих релейних характеристиках існує вроджене обмеження швидкості досяжності. Враховуючи непередбачувану природу нефундаментальних частотних складових післяпошкодного струму та напруги, близькі до джерела пошкодження можуть бути надійно оброблені коротко-віконними алгоритмами, але дальній захват реле вимагає довшого обробного вікна даних. Дальність дії фіксованих віконних цифрових релейних алгоритмів має встановлюватися з урахуванням цих обмежень. Адаптивна характеристика «швидкість—досяжність» є важливою властивістю будь-якої релейної програми.

ЗАГАЛЬНІ ВИСНОВКИ

У даній роботі розглянуто принципи, методи та перспективи аналізу комп'ютерного релейного захисту ліній електропередачі. Виявлено, що сучасні релейні системи, які інтегрують цифрові сигнальні процесори, алгоритми захисту та комунікаційні протоколи, забезпечують значно вищу швидкість реагування, точність селекції та надійність енергосистеми порівняно з традиційними аналоговими рішеннями. Основні висновки можна узагальнити так:

Точність і швидкість: цифрові реле дозволяють адаптивно налаштовувати пороги спрацьовування, використовуючи детекцію фазових та струмових відхилень в режимах короткого замикання й диференційного режиму, що зменшує ймовірність ізольованих помилок та знижує час вимкнення пошкоджених ділянок.

Гнучкість та масштабованість: програмно визначені функції дозволяють швидко адаптовуватися до зміни топології мережі, інтеграції віддалених джерел енергії та збільшення потужностей без значних переобладнань апаратних засобів.

Надійність та відмовостійкість: використання багатокрокових алгоритмів верифікації та резервування вузлів релейного захисту підвищує відмовостійкість систем, зменшуючи ризик неправильної ізоляції ділянок мережі.

Комунікаційні вимоги: надійна й захищена передача діагностичної та сигналізаційної інформації між пристроями є критичною для координації захисту в розподілених і розгалужених мережах. Приділено увагу протоколам з низьким споживанням ширини каналу та криптографічним засобам захисту.

Вплив на кібербезпеку: цифровий захист релейних систем вимагає застосування багатогранних заходів (моделі threat-аналітики, аутентифікація, шифрування та моніторинг трафіку), щоб мінімізувати ризики віддаленого втручання та маніпуляцій даними.

Перспективи розвитку: перспективи зосереджені на впровадженні штучного інтелекту для прогнозування відмов, самодіагностики пристроїв та оптимізації режимів захисту, а також на подальшому інтегруванні зю системами управління енергетичними потоками в рамках концепції умних мереж (Smart Grid).

Обмеження дослідження та напрямки майбутніх робіт також варто відзначити: потреба в більш повному моделюванні взаємодії між захистом і системами управління для оцінки впливу різних схем координації, необхідність стандартизації інтерфейсів та протоколів для забезпечення сумісності між пристроями від різних виробників, а також потреба в довготривалих експериментальних випробуваннях у реальних умовах експлуатації.

Загалом, використання комп’ютеризованих релейних систем з цифровою обробкою сигналів значно підсилює безпеку та надійність ліній електропередачі, забезпечуючи більш ефективну координацію захисту при збереженні гнучкості та можливостей для майбутніх покращень у складі енергетичних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rockefeller, G. D. (1969) Fault protection with a digital computer, IEEE Transactions on Power Apparatus and Systems (IEEE Trans. on PAS), vol. 88, no. 4, pp. 438–461.

2. Mann B. J. and Morrison, I. F. (1971) Digital calculation of impedance for transmission line protection, IEEE Trans. on PAS, vol. 90, no. 1, pp. 270–279.

3. Poncelet, R. (1972) The use of digital computers for network protection, CIGR′E Paper no. 32-08.

4. Takagi, T., Baba, J., Uemura K., and Sakaguchi, T. (1977) Fault protection based on traveling wave theory − Part I: Theory, IEEE Summer Power Meeting, Mexico City, paper no. A77 750-3.

5. Dommel, H. W. and Michels, J. M. (1978) High speed relaying using travelling wave transient analysis, IEEE PES Winter Power Meeting, New York, January 1978, Paper No. A78 214-9.

6. Cory B. J. and Moont, J. F. (1970) Application of digital computers to busbar protection, IEEE Conference on the Application of Computers to Power System Protection and Metering, Bournemouth, England, May 1970, pp. 201−209.

7. Sykes, J. A. and Morrison, I. F. (1972) A proposed method of harmonic restraint differential protection of transformers by digital computers, IEEE Trans. on PAS, vol. 91, no. 3, pp. 1266−1272.

8. Sachdev, M. S. and Wind, D. W. (1973) Generator differential protection using a hybrid computer, IEEE Trans. on PAS, vol. 92, no. 6, pp. 2063−2072.

9. Phadke, A. G., Horowitz, S. H., Thorp, J. S. (1983) Integrated computer system for protection and control of high voltage substations, CIGR′E Colloquium, Tokyo, Japan, November 1983.

10. Deliyannides J. S. and Udren, E. A. (1985) From concepts to reality:

the implementation of an integrated protection and control system, *Developments in Power System Protection*, IEE Conference Publication no. 249, London, April 1985, pp. 24–28.

11. North American Reliability Council, System Disturbance, 1983, 1984 etc. Research Park, Terhune Road, Princeton, New Jersey.

12. Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems, P472/D9, C37.90.1-198x. Draft Document of the Power System Relaying Committee, June 8, 1987.

13. Surge Withstand Capability (SWC) Tests, ANSI C37.90a, 1974.

14. Kotheimer W. C. and Mankoff, L. L. (1977) Electromagnetic interference and solid-state protective relays, IEEE Trans. on PAS, vol. PAS-96, no. 4, pp. 1311–1317.

15. Gilbert, J.C., Udren, E.A. and Sackin, M. (1977) Evaluation of algorithms for computer relaying, IEEE Publication no. 77CH1193 PWR, Paper no. A77-520-0, IEEE PES Summer Meeting, Mexico City, pp. 1–8.

16. B.J. Mann, and I.F. Morrison (1971) Digital calculation of impedance for transmission line protection, IEEE Trans. on PAS, vol. 90, no. 1, pp. 270–279.

17. Gilchrist, G.B., Rockefeller G.D. and Udren, E.A. (1972) High-speed distance relaying using a digital computer, Part I: System description, IEEE Trans. on PAS, vol. 91, no. 3, pp. 1235–1243.

18. Thorp, J.S., Phadke, A.G., Horowitz S.H. and Beehler, J.E. (1979) Limits to impedance relaying, IEEE Trans. on PAS, vol. 98, no. 1, pp. 246–260.

19. Sachdev M.S. and Baribeau, M.A. (1979) A Digital computer relay for impedance protection of transmission lines, Trans. of Engineering and Operating Division Canadian Electrical Association, vol. 18, Part 3, no. 79-SP-158, pp. 1–5. References 187

20.] Luckett, R.G., Munday, P.J. and Murray, B.E. (1975) A substation-based computerfor control and protection, Developments in Power System Protection, IEE ConferencePublication No. 125, pp. 252–260.

21. Phadke, A.G., Hlibka, T., Ibrahim, M. and Adamiak, M.G. (1979) A microprocessorbased symmetrical component distance relay, Proceedings of PICA, Cleveland.

22. Swift, G.W. (1979) The spectra of fault induced transients, IEEE Trans. on PAS, vol. 98, no. 3, pp. 940–947.