НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2025 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Оцінювання часозатримних атак на PSS методом фазових різниць

Виконав: здобувач вищої освіти **IV** курсу, групи ФБ-12

Слєпий Роман Юрійович _____

Керівник доцент кафедри ІБ, к.т.н., доцент Гальчинський Леонід Юрійович _____
(підпис)

Рецензент доцент кафедри ММАД, к.т.н.,старш. досл. Хайдуров Владислав Володимирович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2025 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2025 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Слєпому Роману Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Оцінювання часозатримних атак на PSS методом фазових різниць»

керівник роботи: Гальчинський Леонід Юрійович к.т.н., доцент, доцент кафедри інформаційної безпеки, затверджені наказом по університету від 26 травня 2025 р. №1761-с.

2. Термін подання здобувачем вищої освіти роботи 13 червня 2025 р.

3. Вихідні дані до роботи : літературні джерела, опис архітектури та принципів роботи стабілізатора PSS, характеристики та призначення PMU, типові моделі кібератак на енергосистему, наукові публікації про існуючі підходи до виявлення аномалій у фазових сигналах.

4. Зміст роботи: здійснити огляд літературних джерел пов'язаних із проблематикою кібератак на стабілізатори енергетичну інфраструктуру, PSS та пристрої вимірювання фаз PMU, порівняння методів виявлення аномалій у сигнальному просторі PSS, побудова алгоритму виявлення часозатримних атак, симуляція поведінки системи під час атаки та оцінка ефективності запропонованого методу.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація.

6. Дата видачі завдання 02 грудня 2024 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання завдання та тематики дипломної роботи	02.12.2024-23.12.2024	Виконано
2	Пошук та опрацювання літературних джерел	23.12.2024-23.01.2025	Виконано
3	Аналіз проблематики атак на енергетичну інфраструктуру	23.01.2025-12.02.2025	Виконано
4	Дослідження типових атак на PSS	12.02.2025-15.03.2025	Виконано
5	Ознайомлення з двоконтурною системою Кундура	15.03.2025-20.03.2025	Виконано
6	Аналіз алгоритмів виявлення атак	20.03.2025-13.04.2025	Виконано
7	Написання оглядових розділів дипломної роботи	13.04.2025-27.04.2025	Виконано
8	Впровадження методу в тестову мережу	27.04.2025-13.05.2025	Виконано
9	Написання практичного розділу дипломної роботи	13.05.2025-30.05.2025	Виконано
10	Оформлення дипломної роботи відповідно до методичних вказівок	30.05.2025-05.06.2025	Виконано
11	Створення презентації для передзахисту дипломної роботи	05.06.25-10.06.25	Виконано
12	Передзахист дипломної роботи	13.06.2025	Виконано
13	Захист дипломної роботи	20.06.2025	Виконано

Здобувач вищої освіти Роман СЛЄПИЙ
(підпис) (Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи Леонід ГАЛЬЧИНСЬКИЙ
(підпис) (Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг дипломної роботи : 67 сторінок, 35 ілюстрацій, 25 формул та 49 джерел літератури

Об’єкт дослідження: вразливість стабілізатора енергосистеми(PSS) до кібератак.

Предмет дослідження: модель виявлення часозатримних атак на PSS, що базується на крос-кореляції фазових показників.

Мета дослідження: Аналіз типових векторів кібератак на стабілізатори енергосистеми (PSS), зокрема атак із затримкою сигналу, а також вивчення підходів до виявлення таких атак за допомогою даних з PMU. Розробка методу автоматизованого виявлення часозатримних атак на основі крос-кореляції незалежних сигналів у режимі реального часу.

Методи дослідження: Аналіз літературних джерел, моделювання алгоритму, побудова практичної моделі на тестовій мережі.

Отримані результати: Реалізовано метод виявлення часозатримних атак на PSS на основі крос-кореляційного аналізу сигналів від незалежних PMU. Сформульовано математичні моделі часозатримних атак. Проведено моделювання поведінки системи під впливом атак, що підтвердило здатність методу виявляти приховані спотворення з високою чутливістю. Отримані результати узгоджуються з висновками попередніх досліджень проведених іншими авторами.

Результати роботи були представлені на XXIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених.

Ключові слова: виявлення атак, PSS, PMU, часозатримні атаки

ABSTRACT

The volume of the tesis is 67 pages, 35 illustrations, 25 formulas and 49 references

Research object: vulnerability of the power system stabilizer (PSS) to cyber attacks.

The subject of the research: a model for detecting time-delay attacks on PSS based on cross-correlation of phase indicators.

The purpose of the work: Analysis of typical vectors of cyber attacks on power system stabilizers (PSS), in particular, attacks with time-delay, as well as studying approaches to detecting such attacks using data from PMU. Development of a method for automated detection of time-consuming attacks based on cross-correlation of independent signals in real time.

Research methods: Analysis of literary sources, modeling of the algorithm, building a practical model on the test network.

Obtained results: A method for detecting time-consuming attacks on PSS based on cross-correlation analysis of signals from independent PMUs has been implemented. Mathematical models of time-consuming attacks are formulated. A simulation of the behavior of the system under the influence of attacks was carried out, which confirmed the ability of the method to detect hidden distortions with high sensitivity. The results obtained are consistent with the conclusions of previous studies conducted by other authors.

The results of the work were presented at the XXIII All-Ukrainian Scientificand Practical Conference of Students, Postgraduates and Young Scientists.

Keywords: attack detection, PSS, PMU, Time-delay attack

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DDoS (Distributed Denial of Service) – Тип кібератаки, при якій зловмисники використовують множину пристроїв для одночасного надсилання великої кількості запитів, що призводить до його перевантаження та недоступності для легітимних користувачів.

OT (Operational Technology) – Технології та системи, призначені для моніторингу та управління фізичними процесами, обладнанням та інфраструктурою в промислових та критичних системах.

PMU (Phasor Measurement Units) – Пристрої високоточного вимірювання електричних параметрів в енергосистемах, що забезпечують синхронізовані за часом вимірювання фазорів напруги та струму для моніторингу стану електричної мережі.

PSS (Power System Stabilizer) – Додатковий регулятор збудження синхронного генератора, призначений для покращення стійкості енергосистеми шляхом демпфірування коливань ротора генератора та підвищення стабільності перехідних процесів.

SCADA (Supervisory Control and Data Acquisition) – Комп'ютерна система диспетчерського управління та збору даних, призначена для централізованого моніторингу, управління та контролю розподілених промислових процесів та інфраструктури в реальному часі.

SVM (Support Vector Machine) – Алгоритм машинного навчання для задач класифікації та регресії, що знаходить оптимальну гіперплощину для розділення класів даних шляхом максимізації відстані між найближчими точками різних класів.

ВСТУП

Актуальність роботи. Сучасні енергетичні системи дедалі більше інтегрують інформаційно-комунікаційні технології, що забезпечують ефективне керування, моніторинг та автоматизацію виробництва й розподілу електроенергії. Проте разом із перевагами цифровізації зростає і кількість потенційних векторів кібератак, що можуть бути спрямовані на виведення з ладу критичних елементів інфраструктури. Зокрема, атаки на Power System Stabilizer можуть спричинити порушення синхронності генераторів і навіть повне відключення енергоблоків.

Phasor Measurement Units забезпечують точний моніторинг динаміки енергосистем у реальному часі, однак залишаються вразливими до кібератак, особливо часозатримних. Тому дослідження методів виявлення таких атак є критично важливим для кібербезпеки енергетичної інфраструктури. Вчасне виявлення загроз для PSS та розробка методів виявлення прихованих атак є ключовими для забезпечення надійності та стійкості сучасних електроенергетичних мереж.

Метою дослідження: аналіз типових векторів кібератак на стабілізатори енергосистеми (PSS), зокрема атак із затримкою сигналу, а також вивчення підходів до виявлення таких атак за допомогою даних з PMU. Розробка методу автоматизованого виявлення часозатримних атак на основі крос-кореляції незалежних сигналів у режимі реального часу.

Завдання дослідження. Для досягнення мети необхідно виконати завдання, які наведені нижче.

1. Проаналізувати принципи роботи стабілізатора PSS та пристроїв PMU, а також визначити їхню вразливість до типових кібератак, зокрема time-delay.

2. Сформулювати математичні моделі атак із часовою затримкою сигналів у контексті впливу на роботу PSS.

3. Розробити метод виявлення часозатримних атак на основі аналізу крос-кореляційної залежності між сигналами PMU.

4. Провести комп’ютерне моделювання впливу часозатримних атак на стабільність системи та оцінити ефективність запропонованого методу виявлення.

Об’єкт дослідження – вразливість стабілізатора енергосистеми(PSS) до кібератак.

Предмет дослідження – модель виявлення часозатримних атак на PSS, що базується на крос-кореляції фазових показників.

Методи дослідження – аналіз літературних джерел, моделювання алгоритму, побудова практичної моделі на тестовій мережі.

Новизна одержаних результатів. У роботі пов’язано теоретичну модель виявлення часозатримної атаки з розрахованим практичним методом порогом виявлення таких атак.

Практичне значення одержаних результатів. Дослідження спрямоване на забезпечення практичних варіантів реалізації методу виявлення атак на стабілізатор енергосистеми(PSS) для операторів критичної інфраструктури, що мають на меті підвищити захищеність системи в умовах цифровізації і впровадження розумних мереж.

Апробація результатів роботи. Результати дослідження були представлені на XXIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (14–17.05.2025 р., м. Київ, Україна).

Публікації. Здійснено опублікування наукової статті на базі даної роботи у збірнику тез XXIII Всеукраїнської науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики».

1 БЕЗПЕКА ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Мета кібератак на енергетичну інфраструктуру

Кібератака – будь-який вид зловмисної діяльності, який намагається зібрати, порушити, заперечити, погіршити або знищити ресурси інформаційної системи або саму інформацію [1].

Також кібератака визначається як будь-яка навмисна діяльність, спрямована на крадіжку, розкриття, зміну, виведення з ладу або знищення даних, програм чи інших цифрових активів через несанкціонований доступ до мережі, комп'ютерної системи або цифрового пристрою [2]. У деяких випадках метою кібератак є не стільки крадіжка інформації, скільки порушення роботи інформаційних систем або IT-інфраструктури, що завдає шкоди бізнесу, урядовим установам та іншим об'єктам [2].

У зв’язку з впровадженням більшої кількості інформаційних технологій у всі сфери життя глобальний енергетичний сектор переживає глибоку цифрову трансформацію. Цей перехід зумовлений необхідністю підвищення ефективності, надійності та більш динамічної взаємодії зі споживачами [3]. Фундаментальною характеристикою цифровізації є підвищена зв'язність та повсюдна залежність від цифрових технологій, що прямо та неминуче призводить до значного розширення площі атаки для зловмисників. Сучасні енергетичні системи тепер критично залежать від складних мереж, що включають інтелектуальні лічильники, передові датчики та автоматизовані системи управління. Кожен з цих компонентів, якщо він не захищений належним чином, є потенційною точкою вторгненняя для ворожих суб'єктів [4].

Кібератаки на енергетичну інфраструктуру передбачають використання зловмисниками вразливостей у цифрових мережах з метою порушення операцій, крадіжки даних або отримання геополітичного впливу в енергетичній галузі [5]. Енергетичний сектор є ключовим для забезпечення стабільності та надійності всіх інших критично важливих галузей, що робить його дедалі частішою ціллю для кібератак [7]. Комунальні підприємства керують

системами, які є критично важливими для національної безпеки та громадської безпеки. Енергетичний сектор є однією з найбільш привабливих цілей для кіберзлочинців через свою центральну роль в основі сучасних економік, а також впливу на рівень добробуту населення. Проте варто зазначити, що кібератаки на енргетику є важкими у плануванні та реалізації оскільки вимагають змістовних і вичерпних знань про роботу цієї інфраструктури, принципи побудови мереж і комунікації у системи енергостанцій і power grid вцілому. Виходячи з вищезазначеного цілеспрямовані атаки на енергетичний сектор можуть бути здійснені з кількох причин [3–7].

По-перше, це кіберзлочинці насамперед мотивовані фінансовою вигодою, прагнучи вимагати гроші різними способами. Групи програм-вимагачів, такі як RansomHub/DragonForce та HellCat, особливо активні в націлюванні на енергетичні компанії, прагнучи зупинити виробництво або зашифрувати критичні дані, щоб вимагати вищі викупи. Хактивісти керуються ідеологічними мотивами (наприклад, S16, Noname057(16), групи, пов'язані з Росією, антиізраїльські групи) і часто прагнуть завоювати довіру або привернути увагу до своїх справ, публікуючи передбачувані компрометації мереж операційних технологій. Деякі хактивістські групи також мотивовані екологічними проблемами, націлюючись на енергетичну інфраструктуру, щоб порушити операції, які вони вважають шкідливими [4].

До того ж зачасту атаки на енергетичну інфраструктуру є елементом кібервійни, а угрупування, що здійснюють їх, спонсуються керівництвом держав. Такі дії мають на меті здійснити політичний тиск та провести дестабілізацію соціального та економічного становища у країні-жертві атаки, а загальне значення у сучасному геополітичному ландшафті важко переоцінити. Останнім часом кількість атак на енергетичну інфраструктуру зростає. Це фундаментально підносить кібербезпеку таких від суто технічної проблеми до першочергового імперативу національної безпеки [8].

Рисунок 1.1 – Ступінь ризику зацікавлених сторін у короткостроковій перспективі [9]

На рисунку 1.1 відповідно до звіту [9], cyber insecurity посідає третє місце серед ризиків, що мають місце для урядових організацій та приватного сектору. Більшість компаній критичної інфраструктури в секторі енергозабезпечення належать державі або ж вітчизняним приватним власникам.

1.2 Огляд звітів та досліджень організацій щодо впливу кібератак

Міжнародні організації та профільні дослідницькі центри проводять активний аналіз впливу кібератак на енергетичну інфраструктуру, публікуючи звіти та дослідження, які надають цінну інформацію про масштаби та наслідки цієї загрози. Міжнародне енергетичне агентство у своїх звітах зазначає значне зростання кількості кібератак на комунальні підприємства: у 2022 році їхня кількість подвоїлася порівняно з 2020 роком [10].

IEA також повідомляє, що середня вартість витоку даних в енергетичному секторі у 2022 році досягла 4,72 мільйона доларів США. Аналіз IEA показує, що кібератаки на енергетичні компанії часто призводять до раптового зростання попиту на кваліфікованих фахівців з кібербезпеки. За

оцінками агентства, у 2022 році у світі спостерігався значний дефіцит таких фахівців, який становив близько 3,4 мільйона осіб [11].

Результати досліджень, проведених профільними центрами та експертами у сфері кібербезпеки, також підтверджують зростаючу загрозу для енергетичного сектору. Згідно зі звітом компанії Thales за 2024 рік, 42% компаній, що належать до критичної інфраструктури, включаючи енергетичний сектор, зазнали витоків даних протягом цього року [12]. За даними звіту IBM за 2024 рік, середня вартість відновлення після кібератаки на об'єкти критичної інфраструктури перевищує 5 мільйонів доларів США [13].

1.3 Короткий аналіз конкретних випадків та їхніх наслідків

Протягом останніх років світ став свідком кількох гучних кібератак на енергетичну інфраструктуру в різних країнах, кожна з яких мала значні економічні та соціальні наслідки. У 2010 році комп'ютерний черв'як Stuxnet був використаний для атаки на іранські центрифуги зі збагачення урану в Натанзі, що стало одним з перших відомих прикладів кіберзброї, спрямованої на промислові об'єкти . У 2012 році кібератаки були спрямовані на Saudi Aramco в Саудівській Аравії та RasGas в Катарі з метою зупинки виробництва, що призвело до виведення з ладу десятків тисяч комп'ютерів в Aramco [14].

Особливо тривожними стали кібератаки на енергетичні системи України у 2015 та 2016 роках, коли російські хакери успішно проникли в системи управління електромережами, спричинивши масштабні відключення електроенергії, що торкнулися сотень тисяч споживачів [5]. Ці атаки продемонстрували вразливість критичної інфраструктури до кіберзагроз та можливість використання кібератак як інструменту гібридної війни.

У лютому 2021 року бразильські комунальні компанії Copel та Eletrobras також стали жертвами атак програм-вимагачів, що призвело до порушення їхньої операційної діяльності. У 2023 році повідомлялося про використання програм-вимагачів для проникнення в системи 22 європейських енергетичних компаній, що свідчить про зростаючу загрозу для енергетичного сектору [5].

Згідно з заявою директора з ІТ та зв'язку ПАТ «Черкасиобленерго» Андрія Пилипчука станом на перше півріччя 2023 року 54% кібератак на Україну були спрямовані на енергетичну інфраструктуру [15]. А відповідно до звіту Міністерства енергетики України у 2022 році було заблоковано 1,5 млн спроб атак на енергетичну інфраструктуру [16].

У кінці 2022 року компанія Mandiant розслідувала кібератаку на критичну інфраструктуру України, здійснену пов'язаним із Росією угрупованням Sandworm. Атака мала два етапи: на першому зломисники застосували нову техніку на рівні операційних технологій, використовуючи легітимні інструменти системи, ймовірно, щоб відключити автоматичні вимикачі на підстанції, спричинивши аварійне знеструмлення. Це збіглося з масованими ракетними обстрілами України. Другий етап складав запуск нової версії CADDYWIPER в ІТ-середовищі. Цей інцидент свідчить про зростаючу складність та зрілість кібератак Росії на ОТ-системи. Sandworm продемонстрував здатність швидко розробляти нові інструменти для різних типів промислових систем. За оцінкою Mandiant, ОТ-компонент атаки могли створити менш ніж за два місяці. Спочатку ця активність відстежувалась як окрема, але згодом кластер об'єднали з відомим угрупованням Sandworm — підрозділом ГРУ РФ, який з 2009 року здійснює шпигунство, інформаційні та руйнівні операції, особливо в Україні [17].

Хоча Madiant і не змогли повністю відновити виконання команди ICS, реалізоване двійковим кодом, стало відомо, що атака призвела до позапланового відключення електроенергії. Події 2015 та 2016 років в Україні показали кілька дискретних руйнівних подій проти середовища операційних технологій Крім того, активність Sandworm в мережі операційних технологій виглядає оптимізованою лише для виконання несанкціонованих повідомлень команд ICS, а активність обмежена ІТ-середовищем. Хоча цей зсув, ймовірно, відображає збільшення темпу кібероперацій у воєнний час, він також показує пріоритетні цілі ГРУ в атаках [17, 18].

1.4 Прямі та непрямі економічні наслідки. Соціальні наслідки

1.4.1 Кібератаки на енергетичну інфраструктуру спричиняють значні прямі економічні наслідки.

Серед яких вагому частку становлять витрати на відновлення систем та інфраструктури. Після успішної кібератаки організації змушені інвестувати значні кошти в ідентифікацію завданих збитків, відновлення втрачених даних та приведення до ладу пошкоджених систем. За оцінками, середня вартість відновлення після кібератаки на об'єкти критичної інфраструктури перевищує 5 мільйонів доларів США [13]. У 2022 році середня вартість витоку даних в енергетичному секторі досягла рекордного рівня в 4,72 мільйона доларів США [11]. У 2023 році цей показник становив уже 4,78 мільйона доларів США, а середня вартість руйнівної кібератаки оцінювалася в 5,24 мільйона доларів США [13].

Атака на Colonial Pipeline у 2021 році призвела до значних перебоїв у постачанні палива на східному узбережжі Сполучених Штатів та завдала збитків на мільярди доларів [13]. Кібератака на компанію Halliburton у серпні призвела до втрати або затримки доходів на суму 35 мільйонів доларів США [19].

1.4.2 Непрямі економічні наслідки

Стабільне енергопостачання є критично важливим для функціонування багатьох інших галузей промисловості, включаючи виробництво, транспорт та комунікації. Кібератаки на енергетичні мережі можуть призвести до масштабних відключень електроенергії, що негативно впливає на роботу підприємств, медичних закладів та повсякденне життя громадян. Перебої в енергопостачанні, спричинені кібератаками, можуть порушити функціонування цілих галузей, що призводить до дефіциту товарів та послуг. Енергетичний

сектор є ключовим постачальником продукції для решти економіки, тому кібератаки на нього можуть мати значний вплив на фінансові ринки. Крім того, кібератаки на енергетичну інфраструктуру можуть призвести до потенційного зростання цін на енергоносії.

1.4.3 Соціальні наслідки

Соціальні наслідки кібератак на енергетичну інфраструктуру мають катастрофічний характер, спричиняючи відключення електроенергії, опалення та водопостачання, що безпосередньо впливає на комфорт і безпеку населення. Особливо вразливими є лікарні, де безперебійне електропостачання критично важливе для функціонування медичного обладнання, включаючи апарати штучної вентиляції легенів та діалізні апарати. Перебої в енергопостачанні також ускладнюють доступ до медичних даних та проведення хірургічних операцій. Ефективність роботи екстрених служб (поліції, пожежної служби, швидкої допомоги) залежить від надійності комунікаційних мереж та стабільного електропостачання, а їх порушення затримує час реагування та загрожує життю людей [10,20–21].

Кібератаки становлять особливу загрозу для громадської безпеки та добробуту населення, особливо під час екстремальних погодних умов, коли втрата електроенергії може мати летальні наслідки для вразливих категорій населення. Варто зазначити, що більшість українців на собі відчули руйнівні наслідки дестабілізації енергосистеми. Яскравим прикладом таких наслідків є кібератаки на енергетичні системи України у 2015 та 2016 роках, які призвели до тривалих відключень електроенергії для сотень тисяч людей.

1.5 Атаки спрямовані на верхні рівні енергосистеми та способи закріплення у мережі енергосистеми

Серед основних типів кібератак, спрямованих на енергетичну інфраструктуру, особливе місце займають програми-вимагачі, що є особливо небезпечними для енергетичного сектору, оскільки вони шифрують дані системи та вимагають викуп за їхнє відновлення, що може паралізувати критично важливі операції та заблокувати доступ операторів до систем управління. У першій половині 2021 року спостерігалося значне зростання кількості атак з використанням програм-вимагачів, причому більше половини постраждалих припадало на Сполучені Штати [7].

Фішинг та соціальна інженерія є ще одними поширеними методами кібератак. Вони мають на меті обманним чином завантажити зловмисне програмне забезпечення на ПК співробітників закритої мережі, операторів інфраструктури, аби в подальшому отримати конфіденційну інформацію та несанкціонований доступ до внутрішніх систем. Атаки даного типу не завдають шкоди критичній інфраструктурі напряму, а є лише методом отримання доступу до комп’ютерів у мережі та подальшого розвитку атаки. У 2021 році спостерігався різкий сплеск мобільних фішингових атак, спрямованих на енергетичні компанії, що свідчить про адаптацію зловмисників до використання різних каналів комунікації [22].

Атаки типу "відмова в обслуговуванні" та DDoS мають на меті перевантажити ресурси системи надмірним шахрайським трафіком, що призводить до її уповільнення або повного виходу з ладу. В енергетичному секторі такі атаки можуть спричинити серйозні проблеми, порушуючи роботу систем моніторингу в реальному часі, затримуючи автоматизовані відповіді та ускладнюючи зв'язок між операторами мережі. Тривала DDoS-атака на розумну енергетичну мережу може навіть призвести до каскадних відмов, що вплинуть на цілі регіони. DDoS-атаки є досить поширеним явищем серед кіберзагроз, спрямованих проти організацій критичної національної інфраструктури [5,6].

Гібридні загрози складають з себе комбінацію кібератак з фізичним саботажем, спрямовану на максимізацію завданих збитків. Прикладом такого типу загроз є кібератаки на електроенергетичну мережу України, які відбувалися одночасно з ракетними ударами по енергетичній інфраструктурі [18]. Спостерігається тенденція до зростання кількості вразливих точок в енергомережах Сполучених Штатів, яка становить приблизно 60 нових вразливостей щодня [10].

1.6 Атаки спрямовані на PSS

1.6.1 PSS. Принципи роботи

Power System Stabilizer – це пристрій, який використовується в енергетичних системах для підвищення стабільності електричної мережі. Він призначений для демпфування електромеханічних коливань синхронного генератора.

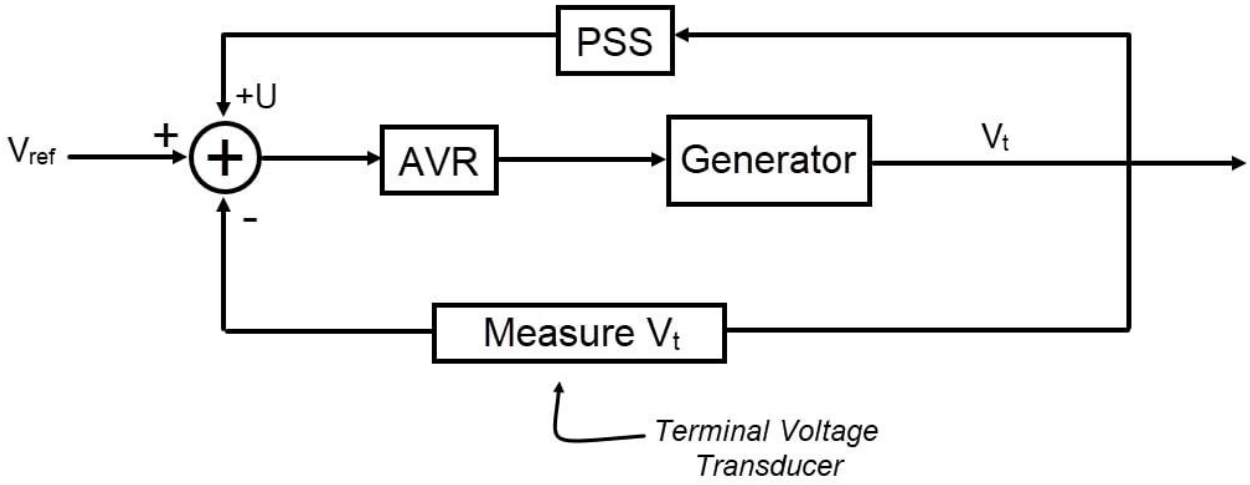

Рисунок 1.2 – Схематичне зображення взаємодії PSS і генератора [23]

За Кундуром, PSS слугує для підвищення динамічної стійкості системи шляхом додавання демпфувального електромагнітного моменту, синхронного з коливаннями ротора, та складається з набору структурних блоків: вхідного

фільтра (washout), фазових коректораів (lead-lag), підсилювача (gain) і лімітерів [24].

PSS виявляє коливання в системі, використовуючи вхідний сигнал, такий як $\Delta\omega$ – відхилення частоти або швидкості ротора, що зазвичай використовується для спрощення реалізації.

Вхідний сигнал пропускається через washout-фільтр — високочастотний фільтр першого порядку із часовою константою T_w, що пропускає тільки коливальні компоненти в діапазоні інтересу та блокує сталі зсуви. Оскільки між зміною напруги збудження та реакцією електричного моменту існує фазове відставання, PSS містить одну або дві секції lead-lag компенсаторів, що забезпечують необхідний фазовий випереджувальний зсув (до ~60° кожен) у смузі 0.2–3 Гц [24].

Параметри часових констант (T_1, T_2, …) підбираються так, щоб пікова фаза компенсаторів відповідала частотам власних коливань системи, забезпечуючи максимальне демпфування без надмірних затримок у сусідніх діапазонах Після фазової компенсації сигнал підсилюється із загальним коефіцієнтом K, що визначає амплітуду демпфувального моменту, і проходить через обмежувач, який запобігає надмірним коливанням вихідної напруги збудження. Отриманий сигнал V_{stab} подається на вхід AVR генератора, коригуючи напругу збудження саме в ті моменти, коли відхилення швидкості ротора спричиняють погасання коливань [24,26].

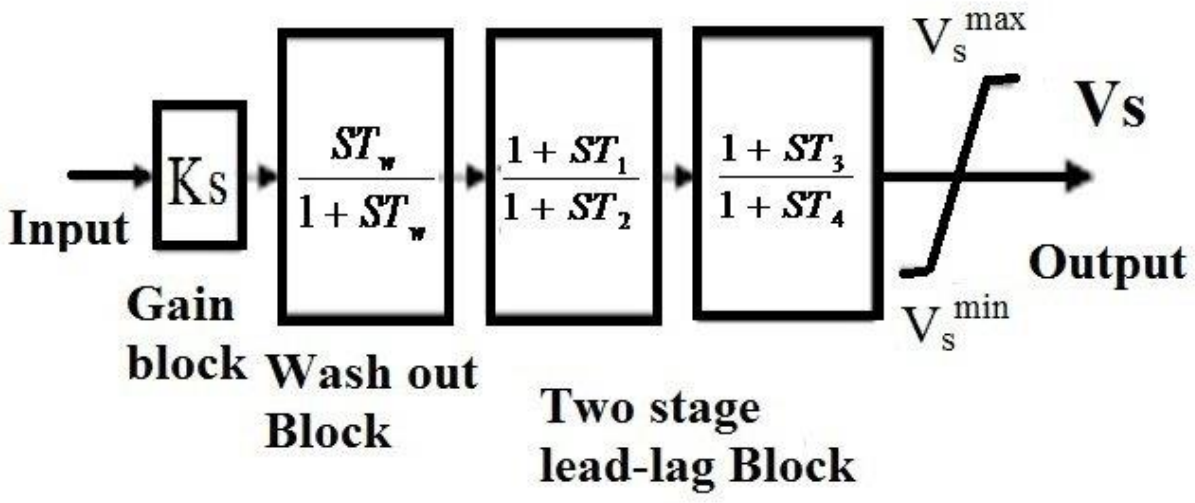

Рисунок 1.3 – Блокове зображення PSS [25]

Якщо вхідний сигнал спотворений або затриманий, PSS може генерувати хибний стабілізуючий сигнал, або вводити сигнал в протифазі, що призводить до неефективного або навіть шкідливого впливу на стабільність системи. Як результат генератор енергосистеми може вийти з ладу або працювати не стабільно, що призведе до зниження ефективності генерації чи ризиків аварійної зупинки усієї електростанції [24, 26].

1.6.2 Приклади атак на PSS

Оскільки атаки на верхні рівні, такі як програми-вимагачі чи злам робочих комп'ютерів операторів інфраструктури зазвичай добре помітні і складають оновну частину зареєстрованих не варто забувати і про атаки, що спрямовані на нижчі рівні енергосистеми. З технічної точки зору, вимкнення PSS може бути досягнуто безпосереднім блокуванням сигналу управління або шляхом ін'єкції спотвореного сигналу, який змушує систему «не сприймати» команду стабілізації. Наприклад, атакуючий може вплинути на мережеву інфраструктуру або протокол передачі даних, щоб переривати сигнал, який має бути направлений до збудника. Наслідки такої атаки не завжди помітні на початкових етапах, проте в умовах збурень (наприклад, після короткочасної лінійної несправності) система не може адекватно реагувати, що загрожує навіть масштабним відключенням.

Перша атака, яку варто розглянути: атака з ін'єкцією зміщення (Bias Injection Attack). Атака з ін'єкцією зміщення полягає у впровадженні атакувальником постійного або синусоїдального збурення до вхідного сигналу PSS. Формально, сигнал, що надходить до стабілізатора, змінюється за формулою:

$$\tilde{u}(t) = u(t) + d(t) \tag{1.1}$$

де $u(t)$ – нормальний сигнал; $d(t)$ – додаткове збурення (зміщення) [27].

Атакувальник може обрати стале зміщення або періодичну функцію, що додається до вихідного сигналу, що в результаті призводить до постійного спотворення оцінки стану системи. Такий тип атаки має серйозний вплив на

динаміку системи: навіть у відсутність додаткових несправностей, ін’єкція зміщення порушує нормальну роботу регулятора, знижуючи демпфуючий ефект PSS. У випадку виникнення додаткового збурення (наприклад, трифазної несправності), система демонструє високі, довготривалі і погано демпфовані осциляції, що може призвести до серйозних порушень стабільності роботи генератора електроенергії.

Наступна атака – це атака із впровадженням неправдивих даних (FDIA). Атаки з ін'єкцією фальшивих даних (False Data Injection Attacks) спрямовані на маніпуляцію вимірюваними даними в енергосистемах з метою спотворення оцінки стану системи без виявлення системами виявлення помилок. Нехай z — вектор реальних вимірювань у системі, який пов'язаний зі станом системи x через рівняння:

$$z = Hx + e, \tag{1.2}$$

де H – матриця спостереження, що описує залежність між станом системи та вимірюваннями; e – вектор похибок вимірювань. Порушник створює вектор фальшивих даних a і додає його до реальних вимірювань, отримуючи змінений вектор вимірюванья z':

$$z' = z + a = Hx + e + a \tag{1.3}$$

Якщо вектор a сконструйований таким чином, що він належить до простору стовпців матриці H. Тобто:

$$a = Hc \tag{1.4}$$

де c – довільний вектор. То спотворення залишиться непоміченим стандартними методами виявлення помилок, оскільки:

$$z' = Hx + e + Hc = H(x + c) + e \tag{1.5}$$

У цьому випадку змінений стан $x' = x + c$ призводить до тих самих залишків при оцінці стану, що й у випадку без атаки, ускладнюючи виявлення втручання [27, 28, 43].

Далі йде атака з відтворенням із затримкою (Delay Replay Attack, DRA). При атаці з відтворенням із затримкою атакувальник спочатку захоплює легітимні дані з сенсорів (наприклад, з PMU), а потім з певною затримкою відтворює їх у системі [44]. Математично це можна описати як:

$$\tilde{u}(t) = u(t_0 + t - T), \tag{1.6}$$

де T – часова затримка, що часто обирається випадковим чином у заданому інтервалі, t_0 – початковий момент часу атаки [44,47,48].

Таким чином, система приймає за актуальними застарілі дані, що порушує синхронізацію між вимірюваним станом і керуючим сигналом. Цей тип атаки, будучи стелс-атакою, може залишатися непоміченим до моменту виникнення несправностей у системі. Затримка в зворотному зв’язку призводить до недемпфованих коливань, оскільки регулятор працює на базі попередніх даних, а не реального стану енергосистеми. Особливо виражений негативний ефект спостерігається під час трифазних несправностей, коли затримка тільки посилює динамічні розбіжності [27,29].

Атака з відтворенням за допомогою внутрішньої моделі (Internal Model Replay Attack). Атака з відтворенням за допомогою внутрішньої моделі є більш складною за механізмом, оскільки атакувальник впроваджує блок внутрішньої моделі, який генерує повторювані сигнали на основі попередніх вимірювань. Основна ідея полягає у використанні блоку, що описується передаточною функцією що генерує повторювані сигнали виходів датчиків. У цьому випадку, цикл зворотного зв'язку нестабільний, тому що відносний градус не дорівнює нулю [27].

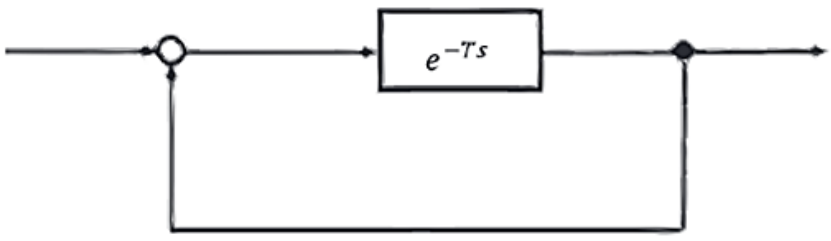

Рисунок 1.4 – Блок-схема атаки за допомогою внутрішньої моделі [27]

У цій роботі основну увагу буде надано темі здійснення та виявлення виду атак, відомого як “Time delay атаки”.

1.7 Часозатримні атаки

Time-delay атаки — це атаки, які штучно створюють затримки в обміні даними між компонентами енергетичної інфраструктури. Цей тип атаки не змінює самі дані — вони залишаються коректними, але їх часова актуальність порушена. Особливо небезпечними вони є для Wide Area Monitoring, Protection and Control Systems та, зокрема, PSS, які залежать від точного й своєчасного надходження даних із віддалених вимірювачів PMU. У контексті енергетичної інфраструктури, особливо кіберфізичних систем, атака із затримкою в часі є специфічним типом кібератаки, яка передбачає зловмисне введення затримок у передачі даних управління в контурах управління системи [30].

У більшості досліджених моделей існує передбачення, що атака здійснюється, коли зловмисник має доступ до входу PSS, як приклад до сигналу частоти, або активної потужності. Це можна реалізувати підключившись до каналу між PMU і контролером або маніпулюючи локальним контролером PSS.

Хоча атаки із затримкою та атаки з відтворенням із затримкою мають спільні елементи реалізації пов'язані з маніпуляцією часовими характеристиками передавання даних, вони мають різні механізми та наслідки. Варто зазначити, що при здійсненні RDA легітимний сигнал, записаний зловмисником може бути надісланий повторно, з певною часовою затримкою, що означатиме надходження до PSS правдивих значень [47,48].

На відміну від атак типу Denial-of-Service і data-injection на інфраструктуру атаки Time-delay є більш важкими для виявлення. Останні можуть завдати більше шкоди, оскільки розкриття може зайняти певний час достатній для виходу з ладу стабільної роботи великої кількості обладнання.

Маніпуляція часом може порушити синхронізовану роботу різних компонентів. Визначення атаки із затримкою в часі в контексті енергетичної інфраструктури є більш нюансованим, ніж загальне визначення в

телекомунікаціях, наголошуючи на цілеспрямованому порушенні операцій системи управління шляхом маніпулювання часом, а не просто на затримці часу відповіді сигналу.

Сучасна енергетична інфраструктура, особливо інтелектуальні мережі, значною мірою залежить від складних та взаємопов'язаних мереж інтелектуальних лічильників, датчиків, автоматизованих систем управління та комунікаційних технологій для забезпечення ефективного моніторингу, контролю та управління виробництвом, передачею та розподілом електроенергії [5]. Атаки із затримкою в часі спеціально націлені на вразливості, притаманні цим комунікаційним мережам, з метою порушення своєчасного потоку критично важливих даних управління між різними компонентами ICS [30].

Зростаюча залежність сучасних енергосистем від обміну даними в реальному часі та автоматизованих механізмів управління робить їх особливо вразливими до атак, які маніпулюють часом цих критично важливих комунікацій. Ефективність та оперативність інтелектуальних мереж залежать від своєчасних даних. Порушення цього часу може мати значні операційні наслідки. Саме тому важливе виявлення таких атак. Математичне формулювання Time-delay атаки виглядає наступним чином:

$$\tilde{u}(t) = u(t - \Delta t), \tag{1.7}$$

де $\tilde{u}(t)$ – спотворений сигнал, який система (PSS) отримує в момент часу t; $u(t - \Delta t)$ – істинний сигнал, який мав місце в минулому, а саме на момент часу $t - \Delta t$; Δt – затримка, введена атакувальником. Це фіксована величина, яка вказує, на скільки часу сигнал відстав. Наприклад, фаза напруги, яка мала бути зареєстрована в 12:00, передається на систему о 12:00:01, при встановленій $\Delta t = 1c$ [27, 48].

Вплив Time Delay на енергосистему:

1) *Зниження ефективності стабілізатора.* Time delay атака порушує зворотний зв'язок між PMU-пристроями та PSS. У наукових матеріалах зазначено, що затримка навіть у кілька сотень мілісекунд може істотно знизити

здатність PSS демпфувати(гасити) коливання у системі. Це збільшує ризик нестабільності, особливо при міжтериторіальних коливаннях потужності [24,27].

2) *Зменшення демпфування низькочастотних коливань*. Затримка даних призводить до неправильних дій стабілізатора, що, замість зменшення коливань, може їх підсилювати. Система в такому випадку працює ніби із запізненням, втрачаючи чутливість до поточних змін [24,27].

3) *Зростання ймовірності каскадних збоїв*. Якщо затримка впливає на декілька вузлів або зон контролю, це може викликати некоректні реакції системи захисту, і як наслідок — каскадні відмови, що можуть призвести до часткового або повного відключення регіону.

Також варто зазначити, що виявлення Time-delay ускладнюється тим, що сама атака має вигляд імітації малого лагу в системі, що може бути звичайною річчю для реальних електромереж [24,27].

Висновки до розділу 1

Спираючись на результати досліджень, описаних у розділі 1, можна зробити низку важливих висновків.

Цифровізація енергетичної інфраструктури значно підвищила ефективність та адаптивність сучасних електромереж. Проте це також розширило площу потенційних кібератак.

Кібератаки на енергетичну інфраструктуру становлять серйозну та зростаючу загрозу для сучасної економіки та суспільства. Прямі та непрямі економічні наслідки включають значні витрати на відновлення систем, мають вплив на інші галузі промисловості. Соціальні наслідки кібератак на енергетичну інфраструктуру є не менш руйнівними.

Висока вартість наслідків кібератак — як економічна, так і соціальна — підтверджується конкретними випадками (Stuxnet, Colonial Pipeline) і статистикою міжнародних агентств. Це зумовлює необхідність інтеграції

кібербезпеки в саму основу розробки, експлуатації та модернізації енергетичних систем.

Особливу загрозу становлять малопомітні атаки на нижчі рівні енергетичних систем, зокрема time-delay атаки та ін’єкції зміщення, які порушують зворотній зв’язок у системі стабілізації та знижують її ефективність. Такі атаки важко виявити на ранньому етапі, але вони мають потенціал призводити до каскадних відмов, масштабних знеструмлень і дестабілізації мереж.

Отже, зростаюча складність атак, їхній технічний рівень і реальні наслідки для енергопостачання, економіки та безпеки населення вимагають перегляду підходів до захисту енергетичної інфраструктури та впровадження ефективних методів виявлення атак, зокрема на рівні PSS.

2 ОГЛЯД МЕТОДІВ ВИЯВЛЕННЯ КІБЕРАТАК НА PSS

2.1 Вибір моделі для дослідження

Для дослідження буде використана двоконтурна система Кундура. Вона була запропонована у відомій монографії Power System Stability and Control і з того часу стала класичною моделлю для тестування алгоритмів контролю стійкості, особливо демпфування низькочастотних осциляцій між регіонами. Система має По два генератори в кожній області, які моделюють великі регіональні генераційні вузли. Міжконтурне з'єднання, оскільки області з'єднані слабкою міжрегіональною лінією, що створює умови для виникнення інтерзональних осциляцій. Навантаження та трансформатори : у кожній області є локальні навантаження та система регулювання напруги через автоматичне регулювання збудження (AVR) і стабілізатори системи (PSS), що є об’єктом дослідження [24].

У системі можливі два основні типи коливань. Перші відомі як локальні коливання, тобто коливання генераторів всередині однієї області (1–2 Гц). Інші – міжконтурні коливання, які означають що генератори в одній області коливаються проти генераторів іншої області з частотою приблизно 0.2–0.8Гц.

За допомогою Simulink, у двоконтурній системі часто вводиться трифазне коротке замикання для ініціювання коливань, які потім вимірюються за допомогою пристроїв синхронного вимірювання фазорів (PMU), встановлених поблизу генераторів. Ці PMU фіксують як локальні (наприклад, коливання між G1 і G2), так і міжзонні коливання, що дозволяє детально аналізувати динамічну поведінку системи [24, 31].

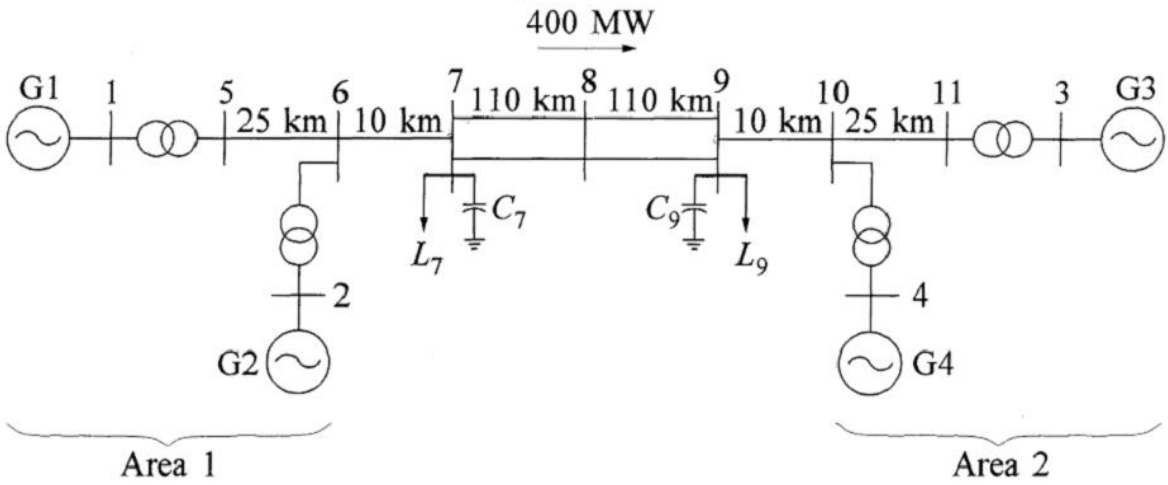

Рисунок 2.1 – Однорядкова діаграма двоконтурної системи [24]

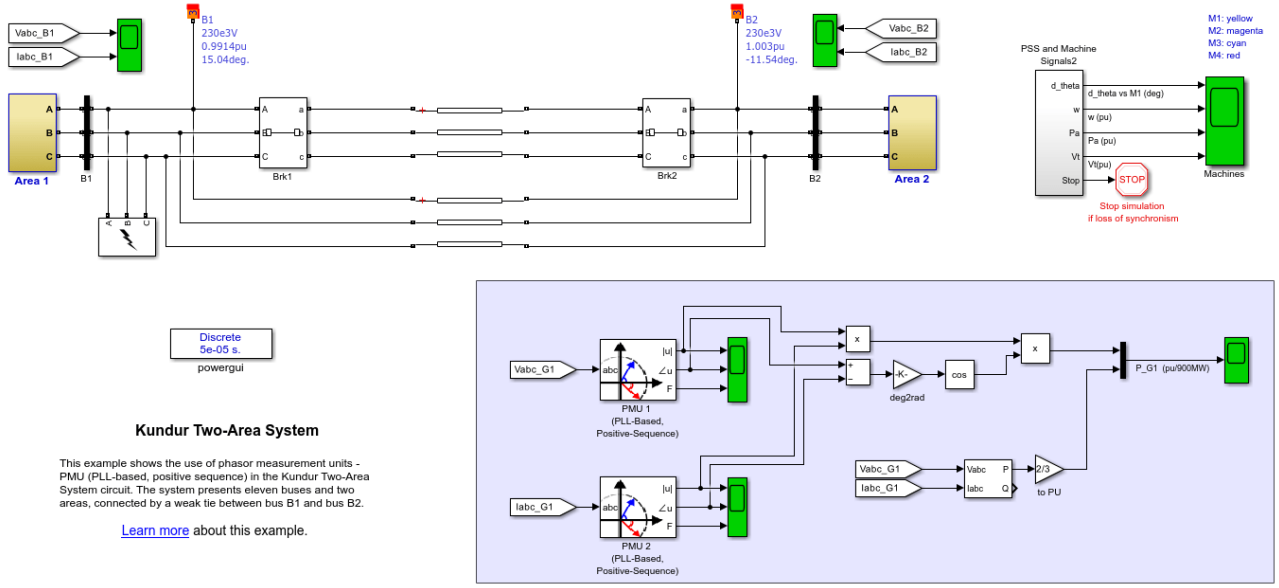

Рисунок 2.2 – Модель Simulink тестової системи Кундура [24,31]

Отже, вибір двоконтурної системи Кундура забезпечує ефективну модель для виявлення та аналізу часозатримних атак на PSS. Такий підхід дозволяє не тільки виявляти наявність атак, але й оцінити їхній вплив на динамічну стійкість енергосистеми, що є вкрай важливим для забезпечення надійності та безпеки електропостачання.

2.2 Важливість PMU у працездатності енергогенераторів

У контексті працездатності PSS пристрої вимірювання фазорів (PMU) відіграють ключову роль. Пристрої вимірювання фазорів є ключовими елементами сучасних систем моніторингу енергосистем. Їхній принцип роботи полягає в оцінці величини та фазового кута електричних фазорних величин, таких як напруга або струм, в електричній мережі. Для цього PMU використовують спільне джерело часу для синхронізації, яким найчастіше є глобальна система позиціонування (GPS) або протокол точного часу IEEE 1588. Синхронізація дозволяє здійснювати вимірювання в реальному часі з багатьох віддалених точок мережі. PMU здатні швидко збирати вибірки з форми сигналу та реконструювати фазорну величину, яка складається з вимірювання кута та величини [32].

PMU насамперед вимірюють сигнали змінного струму з частотою 50/60 Гц, напруги та струми з високою швидкістю, часто до 48 вибірок за цикл, що робить їх ефективними для виявлення коливань напруги або струму протягом одного циклу. Фазорні вимірювання будуються на основі косинусних хвиль, представлених формулою:

$$Acos(\omega t + \theta), \tag{2.1}$$

де A — величина напруги; θ — зсув фазового кута; ω — кутова частота.

У більшості випадків PMU вимірюють величину напруги та фазовий кут, припускаючи сталу кутову частоту. Процес вимірювання включає підгонку даних до синусоїдальної кривої [32].

Аналогові сигнали змінного струму, виявлені PMU, оцифровуються аналого-цифровим перетворювачем для кожної фази. Отримані фазори з часовою міткою можуть передаватися на локальний або віддалений приймач зі швидкістю до 120 вибірок на секунду. Окрім величини та фазового кута, PMU також можуть вимірювати частоту та швидкість зміни частоти в енергосистемі . На основі даних PMU також може бути розрахована активна та реактивна потужність.

Висока частота вибірки PMU, що досягає до 120 вимірювань на секунду, значно перевищує можливості традиційних систем SCADA, які зазвичай надають одне вимірювання кожні 2-4 секунди. Така висока часова роздільна здатність дозволяє інженерам аналізувати динамічні події в мережі, що є неможливим за допомогою повільніших вимірювань SCADA [32,49].

Важливим аспектом роботи PMU є використання GPS для забезпечення спільного часового еталону. Це дозволяє синхронізувати вимірювання, зроблені в різних географічних точках, з точністю до мікросекунди. Однак, якість сигналу GPS може варіюватися, що слід враховувати при зборі даних PMU. Крім того, системи GPS є вразливими до атак на синхронізацію часу, що може бути використано зловмисниками для введення в оману систем моніторингу [32].

У двохконтурній системі Кундура PMU розташовують у ключових вузлах – на генераторах та в точках міжконтурного зв’язку. Це дозволяє моніторити міжконтурні коливання, оскільки PMU дають змогу фіксувати відносні зсуви фаз між регіонами, виявляючи слабку демпфованість.

З’являється можливість аналізувати динаміку коливань, завдяки високій точності та частоті даних можна виконувати онлайн-оцінку режимів, зокрема низькочастотних осциляцій (~0.2–0.8 Гц). До того ж дані з PMU є основою для широкозонних систем моніторингу (WAMS), які допомагають оперативно реагувати на порушення стабільності в енергосистемі [32, 45, 46].

2.3 Методи виявлення часозатримних атак на PSS

2.3.1 Метод нечіткої логіки (Fuzzy Logic)

Даний метод оперує нечіткими множинами та лінгвістичними правилами, що дозволяють працювати з неповними або ж неточними даними. Ідея використання методу полягає у побудові бази з нечітких правил, які будуть описувати «еталонний» і «аномальний» стани системи. Для прикладу можна

використовувати введення словникових змінних як «затримка сигналу велика» чи «затримка сигналу відсутня» з відповідними функціями належності. Під час роботи модель спостерігає фактичні параметри PSS, такі як кути фаз чи керуючі входи і перетворює зазначені у ступені належності до нечітких множин, визначених заздалегідь. [33]

Якщо «затримка сигналу велика» і частота коливань є «нетипова», то спрацювання означає атаку. Дефазифікація нечіткого висновку дає остаточне рішення про ймовірність атаки. Нечіткі системи добре справляються з невизначеністю й «розмитими» ознаками нападів, знижуючи кількість хибних спрацьовувань.

Серед переваг цього методу можна вказати те що він враховує певну невизначеність даних. Також може бути більш гнучким і простішим у інтерпретації. В той час як серед недоліків варто зазначити визначення експертних правил і налаштування функцій перетворення сигналів, в сукупності з необхідністю постійного перетворення сигналу та перевірки на відповідність умовам атаки. Це робить метод ресурсномістким, а також вимагає кваліфікованої оцінки експертної групи для встановлення порогів елементів нечіткої логіки [33].

2.3.2 Метод залишкових сигналів

Цей підхід базується на математичній моделі системи. Припустимо, що для PSS існує модель типу:

$$\begin{cases} \dot{x} = Ax + Bu \\ y = Cx + Du \end{cases} \tag{2.2}$$

x – вектор станів, u – вхід (керуючий сигнал), y – вимірювання PMU. Будують спостерігач, наприклад Льюенберґера, який на кожному кроці оцінює стан $\hat{x}$ і вихід $\hat{y}$ на основі u та попередніх вимірювань [34].

Потім визначають залишковий сигнал

$$r(t) = y(t) - \hat{y}(t) \tag{2.3}$$

Різницю між реальним і прогнозованим виходом. При нормальній роботі оцінка близька до реального значення, тому $r \approx 0$. Якщо ж відбувається атака, то залишок несподівано відхилиться від нуля. Наприклад, для дискретного Luenberger-спостерігача динаміка помилки:

$$e(k) = x(k) - \hat{x}(k) \tag{2.4}$$

задана системою з матрицею $(A - LC)$; при правильно спроектованому спостерігачі ця помилка згасає. Таким чином, стабільна модель забезпечує малий залишок без атаки, а великі залишки свідчать про збої чи втручання [34].

Проте даний варіант дуже чутливий до моделі системи, він не може розрізнити атаку від невизначеності. Для цього методу складно обрати поріг залишкового стану таким чином, щоб невеликі збої, шуми не пов’язані з атакою не давали хибних спрацювань. Також даний метод вразливий до FDIA а обчислювальна складність змушує обирати менш вимогливий метод.

2.3.3 Метод на основі аналізу Фур'є

PSS призначений для демпфувальної дії на низькочастотні коливання генератора. Якщо на ланцюжок керування або вимірювань буде здійснена часозатримна атака, це призводе до додаткової фазової похибки у замкненому контурі. З практичної точки зору, така фаза затримка позначається як додатковий елемент аперіодичного зсуву в частотній характеристиці PSS.

У нормальному стані при частотах коливань в діапазоні $0{,}1-2$ Гц PSS забезпечує необхідну фазу для генерації демпфувального сигналу. Якщо ж у контур введено додаткову затримку $\tau_{ат}$, фазовий запас зменшується приблизно на величину:

$$\Delta\, \phi_{ат}(\omega) \approx -\omega \cdot \tau_{ат}, \tag{2.5}$$

де ω – це кутова частота коливання. На спектральному рівні це проявиться як зміщення пік-фаз та/або поява додаткових бокових частотних компонент, якщо затримка змінна або змінює свою величину у часі [35].

Таким чином, основна ідея виявлення полягає в моніторингу спектральних характеристик вимірюваних сигналів узагальнених PMU-даних і виявленні ненормативних змін фазових зсувів або появи незвичних гармонік. Низькочастотні піки від 0,1 до 0,7 Гц відповідають міжвузловим режимам, а 1–2 Гц – локальні режими. Додаткові піки або зміщення на цих частотах приблизно на

$$\Delta f \approx \frac{1\pi}{2}\frac{\Delta\phi}{\tau} \tag{2.6}$$

можуть вказувати на часозатримну аномалію.

Стосовно помітних переваг аналізу Фур'є варто зазначити високу роздільну здатність за частотою оскільки можна чітко виділити піки міжвузлових та локальних режимів. Також якщо затримка з'являється лише у певні моменти, короткотривале перетворення Фур'є покаже тимчасові «сплески» у спектрі. А сам зсув піку амплітуд можна помітити під час візуалізації спектру [35].

Однак залежність від синхронізованого високочастотного зразка, так коректної оцінки низьких частот потрібна щонайменше кілька герц дискретизації робить цей метод важким у реальному впровадженні. Шум і вмикання чи навпаки вимикання великих навантажень можуть маскувати або псевдо-генерувати сплески у спектрі. Тому необхідна точна фасадна фільтрація та адаптивні пороги [35].

2.3.4 Метод на основі матриці Ганкеля

Метод виявлення часозатримних атак на PSS за допомогою фази розгортання та Ганкелевої матриці. Даний метод у сутності своїй поєднує аналіз розгорнутого фазового кута сигналу з PMU і низькорівневу апроксимацію матриці Ганкеля, побудованої на цих сигналах [36].

У нормі PMU передає фазовий кут $\theta[n]$ у межах $[-\pi, +\pi]$. Коли θ перетинає ці межі при синусоїдальних коливаннях системи, кут «обертається» (з ±180° на ∓180°) — так звана фазова обгортка. Щоб виявити часові аномалії,

спочатку створюють розгорнутий фазовий кут $\phi[n]$, який математично «розгортає» ці стрибки за принципом

$$\phi[0] = \theta[0], \phi[n] = \theta[n] + 2\pi \cdot N[n] \tag{2.7}$$

де $N[n]$ – ціле число «лічильник перекидання», яке збільшується або зменшується на ± 1 щоразу, коли θ переходить через межу $\pm\pi$. В результаті у режимі без втручань $\phi[n]$ - плавна функція часу, що відображає реальний фазовий рух напруги генератора [36].

Під час здійснення time-delay атаки зловмисник зсуває увесь часовий ряд на T секунд:

$$\theta змін[n] = \theta реал[n - k], k = T \cdot fs \tag{2.8}$$

де fs — частота дискретизації PMU. Під час такого зсуву момент переходу через $\pm 180°$ зміщується, а $N[n]$ змінює своє значення у неочікуваний момент. Відтак графік розгорнутого кута $\phi[n]$ спотворюється.

Для виявлення атаки необхідно взяти проміжок з кількох секунд і розгорнутих фазових кутів багатьох каналів PMU, проте можна взяти і лише один PMU або декілька поруч розташованих. Нехай m - кількість каналів, а n - довжина вікна. Далі формується матриця Y розміром $m \times n$, де кожен рядок — вектор $\phi_i = [\phi_i[0], \phi_i[1], \dots, \phi_i[n-1]]$ для -того каналу [36].

На основі Y будують матрицю Ганкеля розміром $(m\,(n/2+1)) \times (n/2+1)$,чи $(n/2+1) \times (n/2+1)$,при $m = 1$. Формально, для одноканального сигналу $\phi[n]$, матриця Ганкеля H будується як:

$$H = \begin{bmatrix} \phi[0] & \phi[1] & \cdots & \phi[(n/2)] \\ \phi[1] & \phi[2] & \cdots & \phi[(n/2)+1] \\ \vdots & \vdots & \ddots & \vdots \\ \phi[(n/2)] & \phi[(n/2)+1] & \cdots & \phi[n-1] \end{bmatrix} \tag{2.9}$$

У випадку $m > 1$, то кожен канал «нарізається» на $n/2+1$ підрядків і укладається у спільну матрицю. [36,37]

Далі беруть сингулярне розкладання матриці $H = U\Sigma V^*$ та залишають лише перший або перші r сингулярні значення. Визначають помилку апроксимації рангу r:

$$e_r = \frac{\|H - U\sum_r V^*\|_F}{\|H\|_F} * 100\% \quad (2.10)$$

де матриця, що містить лише r найбільших сингулярних значень, а $\|\cdot\| F$ - норма Фробеніуса [36].

У нормальному режимі сигнали $\phi_{\text{i}}[n]$ від різних каналів мають високу кореляцію. Тому матриця Ганкеля має низький ранг і відносно невелику помилку апроксимації при $r = 1$. Під час часозатримної атаки, не зважаючи на те, що числові значення мають зсув на T секунд, між каналами порушується фазова синхронність у часі. Даний зсув і призводить до збільшення помилки рангової апроксимації навіть без перестановки стовпці. А після перестановки стовпців e_r зростає ще більше [36,37].

До значущих переваг цього методу належить здатність виявляти ще й FDIA, окрім досліджуваних часозатримних. Метод чутливий навіть до затримок ≥ 1 с. Для негайної перевірки можна комбінувати метод зі згаданими вище методом нечіткої логіки чи методом залишкових сигналів. Щодо недоліків мають місце високі вимоги частоти даних PMU, значні впливи шумів та потреба у значних обчислювальних ресурсах на практиці. Модель також вразлива до часозатримних атак, з рівнем затримки $T \approx 200 - 300$ мс [36,37].

2.3.5 Методи на основі штучного інтелекту

Даний метод буде розглянуто поверхнево, оскільки на разі впровадження штучного інтелекту в системи контролю безпеки енергетичної інфраструктури на практиці є небезпечним кроком.

У цьому підході можна використати різні методи машинного навчання. Серед основних – багатошарові персептрони, згорточні або рекурентні мережі – для аналізу часових рядів. SVM як класичний метод класифікації, який використовує ядра для поділу ознак нормальних й аномальних. Багато досліджень застосовували SVM для виявлення аномалій, іноді в поєднанні з іншими методами.

У деяких дослідженнях штучні нейромережі застосовано для безпосередньої оцінки наявності затримки. Для тестування розробили нейронну мережу для виявлення Time-Delay Switch Attack у двоконтурній системі, продемонструвавши ефективність методу у типових сценаріях [38].

Досліди, зазначені у публікаціях [38-39] показують, що ML-методи можуть досягати високої точності. Так у 2023 спеціалісти навчили Random Forest на даних для виявлення атак та досягли близько 90.6% точності [39]. Дослідники порівнювали традиційні k-means, кластеризацію, автоенкодери та графові нейронні мережі в IEEE 68-шинній системі – результати показали, що методи графових нейронних мереж суттєво перевершують інші за точністю детекції. У простих сценаріях графова нейронна мережа навіть виявилися здатною коректно локалізувати атаковані сенсори. Подібні результати говорить про те, що використання потужних алгоритмів машинного навчання підвищує ймовірність вчасного виявлення кібератак [40].

Проте для побудови ефективної моделі потрібен великий набір даних і не завжди можливо зібрати репрезентативні приклади time-delay атак. Також можливе перенавчання моделі, з характерним перелаштуванням під набір тренувальних даних. І до того ж наразі мережі, здатні виявляти атаки, є ресурсномісткими і часомісткими.

2.4 Метод виявлення заснований на крос-кореляції фаз

2.4.1 Обгрунтування вибору данного методу

Метод виявлення time-delay attacks через аналіз зміни похідної крос-кореляційної функції обрано тому, що він не вимагає диференціювання вхідного сигналу безпосередньо, а отже менш чутливий до шумів. Цей метод використовує «здорові» PMU-дані, які за нормальних умов залишаються незмінними. Під час атаки ці величини розходяться, і це відразу відображається на викривленні кореляції. Дозволяє відстежувати приховані часозатримні

впливи,зокрема time-delay, які до моменту виникнення фактичної нестабільності поводяться у стелс-режимі. Також він працює в реальному часі й може бути реалізований з мінімальними обчислювальними затримками та ресурсними витратами. Таким чином атака буде виявлення, після збурення у системі, оскільки заражений PSS не дасть стабілізувати систему [41,42].

2.4.2 Підготовчий етап

Для виявлення атаки необхідно порівняти еталонний сигнал PMU із тим, що надсилається до PSS. Для фазового кута напруги зі здорового PMU на терміналі генератора надають позначення $y'(t)$, а для фазового кута струму з іншого PMU на тому ж терміналі надають позначення $s(t)$. Діє припущення про те, що вимірювання на PMU і самі PMU не є атакованими. У даному випадку сигнал $s(t)$ відіграє роль «водяного знаку». Далі задається мале згладжувальне значення ε у знаменнику для запобігання діленню на нуль на старті:

$$\psi(0) = 0, t \leftarrow \varepsilon > 0 \tag{2.11}$$

де $\psi(t)$ — поточне значення кореляції, а сама змінна-інтегратор ініціалізується нулем. Параметр часу ε обирається достатньо малим від 10 до 100 мс, щоб не вплинути суттєво на обчислення, але й не допустити стрибка функції в початкових точках [27].

2.4.3 Етап формування функції кросс кореляції

Функція кросс-кореляції має вигляд:

$$\psi(t) = \langle s(\tau)y'(\tau)\rangle(t) = \frac{1}{t}\int_0^t s(\tau)y'(\tau)d\tau\,, t > 0, \tag{2.12}$$

де $\tau \in [0, t]$ – змінна часу, тобто локальна змінна всередині інтегралу, щоє аналогом кроку інтегрування. Значення $\psi(t)$ відповідає середньому добутку поточних фаз струму та напруги за весь час спостереження від 0 до t.

Якщо затримки немає, відношення істинної фази струму та фази напруги залишатиметься стійким, отже $\psi(t)$ змінюватиметься плавно та без зривів. Формула (2.12) усереднює поведінку на проміжку часу та виділяє сталі тренди у взаємозв'язку сигналів. Оскільки у нормальних умовах між фазою струму й напруги на генераторі є стійка фізична залежність — вони змінюються синхронно. Дана крос-кореляція є незалежною від інших чинників, окрім активних замірів PMU. Під час time-delay атаки сигнал $y'(t)$ замінюється затриманим, тому його фазовий зсув більше не збігається з поточним $s(t)$, який не піддається впливу зловмисника, через це добуток $s(\tau) \cdot y'(\tau)$ втрачає стабільну структуру і усереднене значення $\psi(t)$ змінюється неприродно. Інтеграл тут відіграє роль адаптивного монітору, що накопичує інформацію про стан узгодженості сигналів, ігнорує короткочасні випадкові відхилення, в тому числі малі шуми, але чітко вловлює розсинхронізацію, викликану атакою. Сам інтеграл виконує роль фільтра, бо він усереднює коливання сигналу у часі? приглушуючи шум і підкреслюючи сталі зміни у фазовому зв'язку. Замість того щоб реагувати на кожне шумове коливання, інтеграл накопичує значення сигналу і приглушує шумові компоненти [27, 42].

2.4.4 Визачення похідної кросс-кореляції

За умови, що у нормальному стані значення $y'(t)$ і $s(t)$ узгоджені то похідна коливається близько до нуля, стабільна. Якщо атака триває — сигнали залишаються неузгодженими, а отже похідна залишається значною, не повертається до 0. Якщо атака припинилася то і похідна починає згасати назад до нуля [27].

Оскільки безпосереднє диференціювання підсилюватиме шум, пропонується диференціальне рівняння:

$$\frac{d\psi}{dt} = \frac{d}{dt}\left(\frac{1}{t}\int_0^t s(\tau)y'(\tau)d\tau\right). \quad (2.13)$$

За формулою похідної добутку:

$$\frac{d\psi}{dt} = \frac{d}{dt}\left(\frac{1}{t}\right) * \int_0^t s(\tau)y'(\tau)d\tau + \frac{1}{t} * \frac{d}{dt}\left(\int_0^t s(\tau)y'(\tau)d\tau\right). \quad (2.14)$$

Похідна інтеграла від неперервної функції по змінній верхній межі існує і дорівнює значенню підінтегральної функції в точці, що дорівнює верхній межі, тобто:

$$\frac{d}{dt}\left(\int_0^t s(\tau)y'(\tau)d\tau\right) = s(t)y'(t). \quad (2.15)$$

Отримаємо:

$$\frac{d\psi}{dt} = -\frac{1}{t^2}\int_0^t s(\tau)y'(\tau)d\tau + \frac{1}{t}\cdot \mathrm{s(t)y'(t)} \quad (2.16)$$

Шляхом спрощення замість інтегрального виразу можна підставити $t \cdot \psi(t)$, отримаємо кінцеву формулу зміни похідної за часом:

$$\frac{d\psi}{dt} = \frac{\mathrm{s(t)y'(t)} - \psi(t)}{t + \varepsilon}. \quad (2.17)$$

Тут епсілон використовується з метою запобігання ділення на нуль.

2.4.5 Етап реагування. Поріг виявлення

Як вже зазначено, щойно починається осциляція, попередній сигнал починає розходитися з фактичним станом системи. Внаслідок цього у формулі (2.17) величина $s(t)\,y'(t)$ різко змінюється (стосується фазового зсуву). Тому $d\psi/dt$ раптово стрибне вище за нормальний рівень, буде помітно нестандартні коливання. Знаючи це, необхідно встановити поріг реагування threshold перехід якого означав би атаку на інфраструктуру.

Пропонується встановлювати поріг θ на основі попередніх емпіричних вимірювань у «здоровому» режимі роботи системи. Для цього варто оцінити максимальні допустимі значення $|d\psi/dt|$, яке трапляється без зовнішніх втручань. А під час спостереженння $|d\psi/dt| \geq \theta$, необхідно видавати сигнал тривоги. Для точності визначення атаки варто впровадити алгоритм перевірки. А саме на кожному кроці дискретизації обчислювати нове значення $\psi(t)$ і $|d\psi/dt|$, проводити порівняння $|d\psi/dt|$ із θ. Якщо $|d\psi/dt|$ перевищує θ протягом кількох послідовних кроків фіксується здійснення атаки. Необхідність використання кількох послідовних кроків полягає у потребі уникнення спрацювань на одиночний шум [41, 42].

Також пропонується введення критерію ξ, що буде визначений формулою

$$\xi = \frac{1}{\Delta t}\int_{t_1}^{t_2} | s(\tau) - y'(\tau)|d\tau \ , \qquad (2.18)$$

де $t_1 - t_2$ – це короткий часовий проміж після здійснення атаки. А середнє значення модулю різниці швидкостей на цьому проміжку не має перетинати встановлений критерій.

Висновки до розділу 2

У даному розділі було розглянуто модель двоконтурної енергосистеми Кундура, яка використовується для моделювання локальних та міжконтурних коливань, характерних для реальних енергосистем. Було обґрунтовано вибір цієї моделі як тестової платформи для аналізу впливу time-delay атак на роботу Power System Stabilizer.

Було проаналізовано роль пристроїв синхронного вимірювання фазорів (PMU) у виявленні динамічних змін у фазових характеристиках, зокрема тих, які виникають внаслідок зловмисних втручань у сигнали управління.

На основі опрацьованого матеріалу було розглянуто та порівняно кілька методів виявлення time-delay атак на PSS, а саме метод нечіткої логіки, метод залишкових сигналів, аналіз у частотній області (Фур'є), метод на основі

матриці Ганкеля, а також підходи на основі машинного навчання. Було встановлено, що жоден з методів не є універсальним і кожен має свої обмеження, пов’язані з обчислювальними витратами, точністю в умовах шуму або високими ресурсними вимогами до системи реалізації.

З огляду на це, постає важлива задача вибору методу, що міг би ефективно виявляти атаки на PSS у режимі реального часу. На основі проведеного аналізу було зроблено висновок про доцільність розробки практичного модуля для виявлення time-delay атак з використанням підходу, що спирається на дані PMU, фазову кореляцію показників та низькорівневу обробку даних у реальному часі.

3 ВПРОВАДЖЕННЯ МЕТОДУ ВИЯВЛЕННЯ ЧАСОЗАТРИМНИХ АТАК В ТЕСТОВУ МЕРЕЖУ

3.1 Налаштування системи

Як було зазначено у розділі 2 для тестування цього методу буде використана двоконтурна система Кундура.

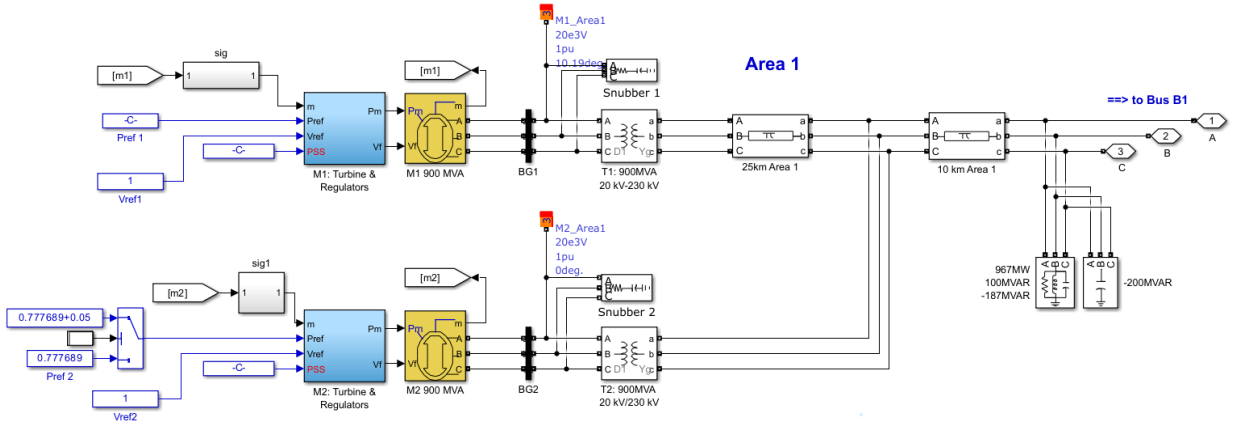

Рисунок 3.1 – Налаштування Зони 1 до проведення тестування

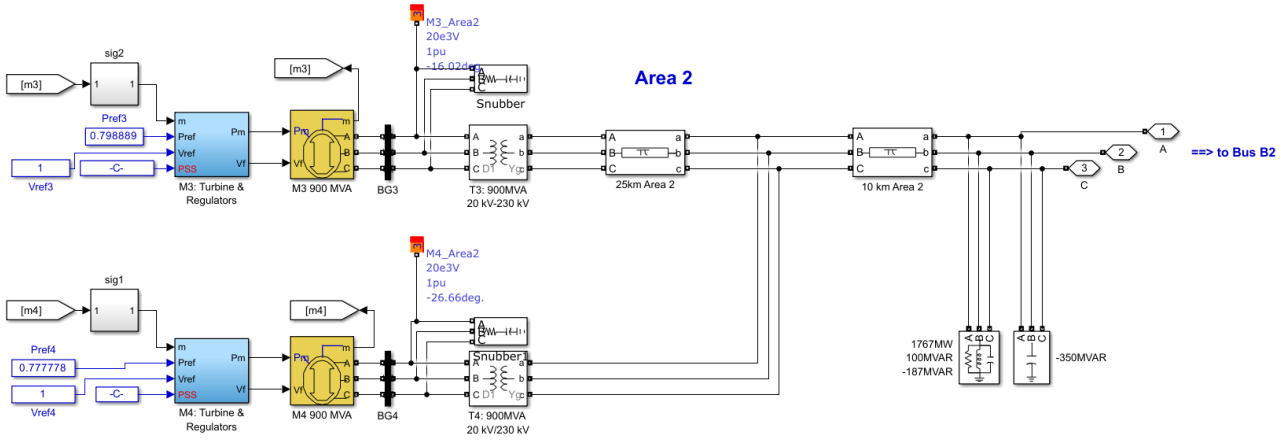

Рисунок 3.2 – Налаштування Зони 2 до проведення тестування

На рисунках 3.1 та 3.2 подані зображення налаштування двох контурів цієї системи. Важливими елементами є Генератор M1(жовтий квадрат), PSS та AVR, що знаходяться у зоні “M1: Turbine and regulators”(синій квадрат) та клеми трифазового вимірювача (чорний прямокутник), що і допомагають вимірювати сигнал на PMU.

3.2 Еталонні показники системи до атаки

Для розуміння того, як активуюче трифазове коротке замикання змінює параметри стабільності системи було продемонстровано відносні кути між роторами генераторів M1,M2,M3,M4; фазовий кут напруги генератора M1 у здоровому стані та амплітуду фази у здоровому стані.

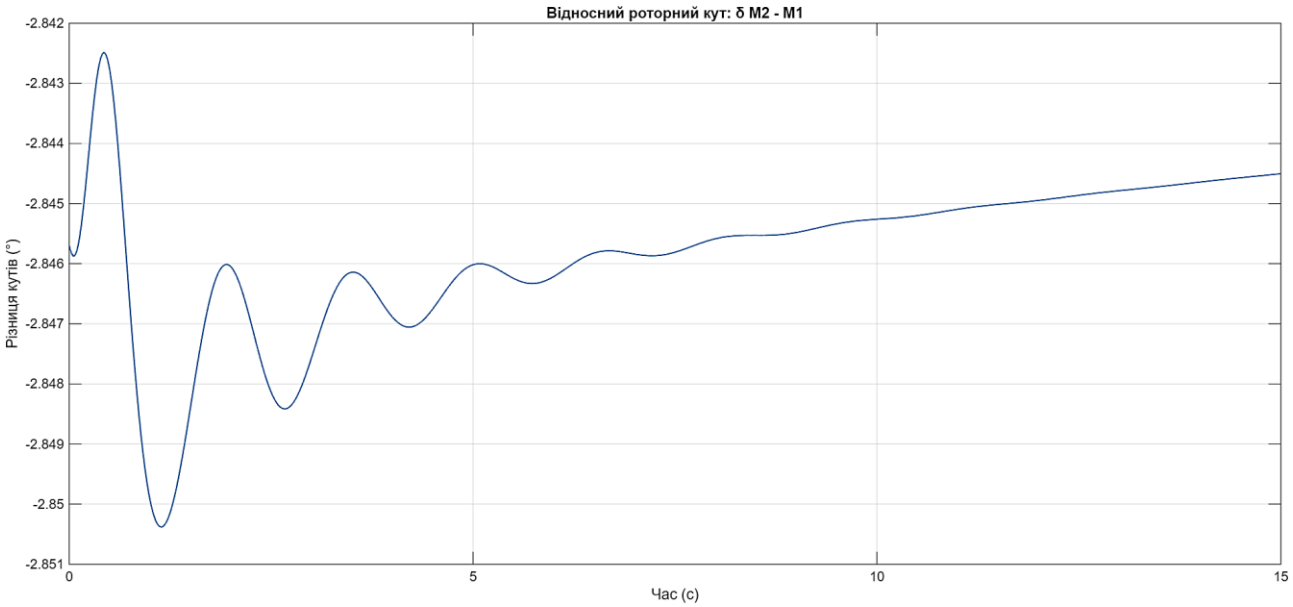

Рисунок 3.3 – Відносний кут між роторами M2 і M1 у здоровій системі

На рисунку 3.3 зображена різниця кутів між роторами генераторів M2 і M1 протягом усієї симуляції здорової активності системи. Те ж саме відношення буде побудоване для кутів між M3 і M1 і між M4 і M1. Зображені коливання на окремих графіках з метою показати наскільки малі коливання (0,0025 між M2 і M1 наприклад) між роторами. Це може значити про стабільну роботу системи.

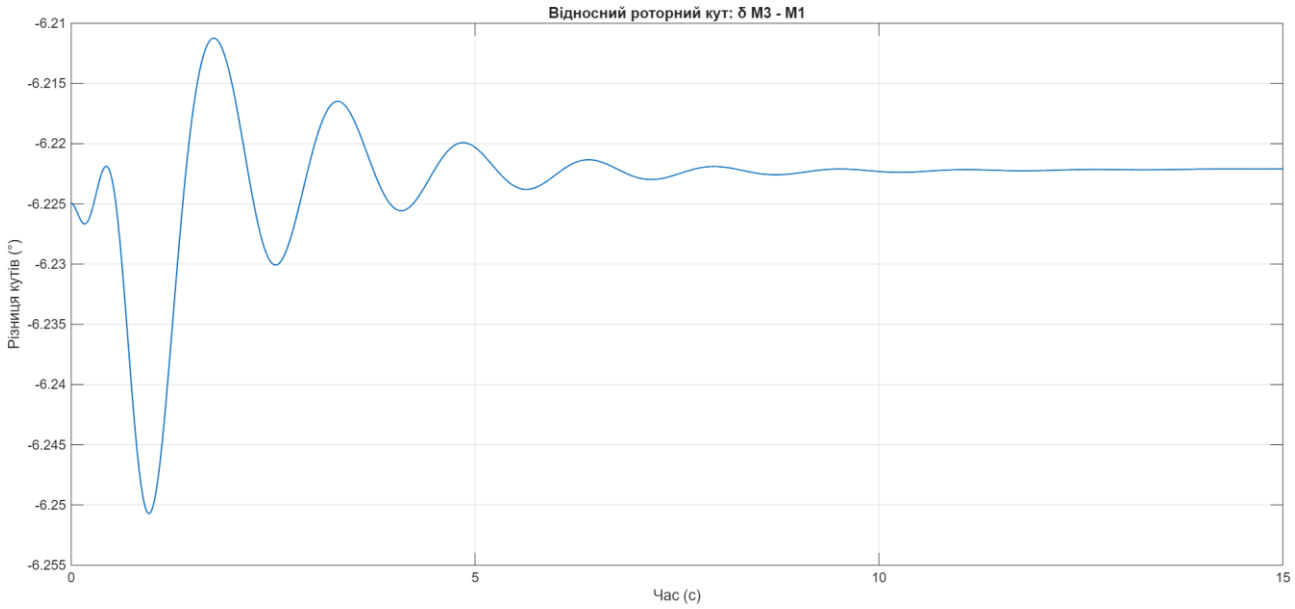

Рисунок 3.4 – Відносний кут між роторами М3 і М1 у здоровій системі

На рисунку 3.4 зображена різниця кутів між генераторами М3 і М1 протягом усієї симуляції здорової активності системи.

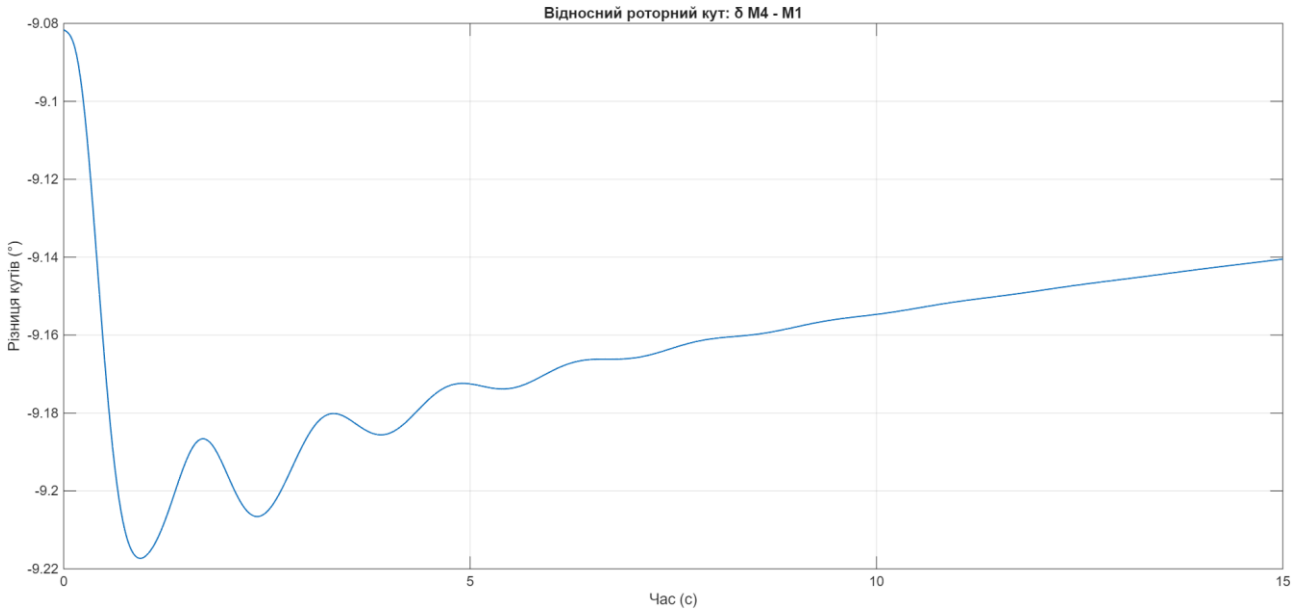

Рисунок 3.5 – Відносний кут між роторами М4 і М1 у здоровій системі

На рисунку 3.5 зображена різниця кутів між генераторами М3 і М1 протягом усієї симуляції здорової активності системи.

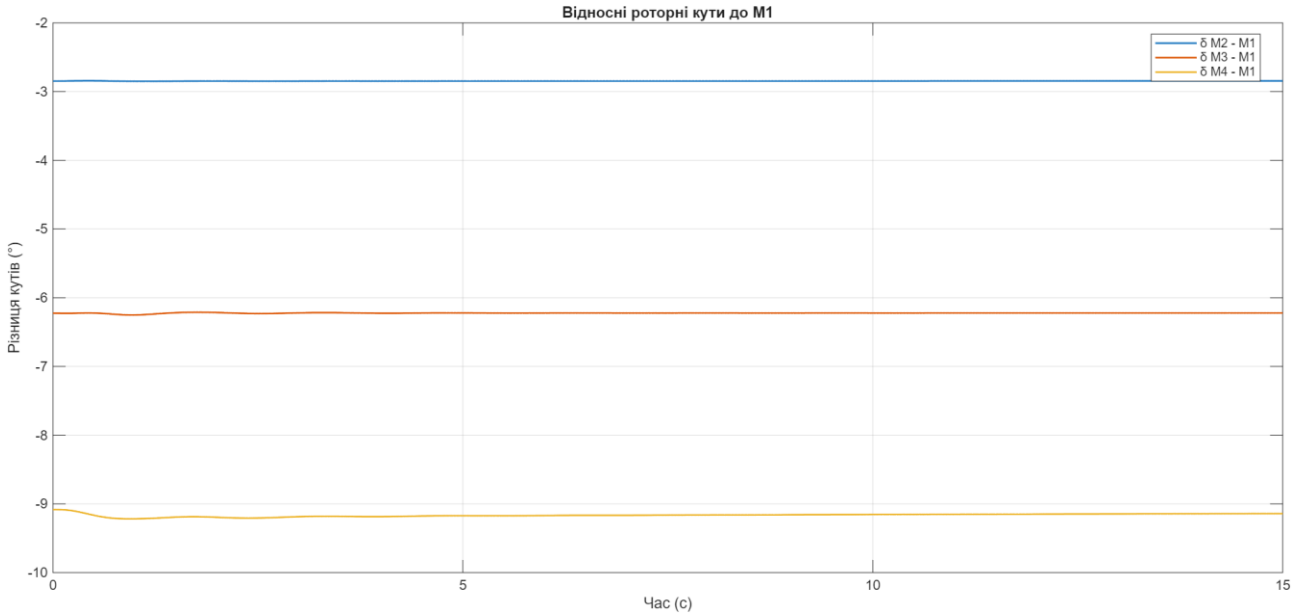

Рисунок 3.6 – Відносний кут між роторами M2,M3,M4 і M1 у здоровій системі

На рисунку 3.6 зображена різниця кутів між генераторами M2-M4 і M1 протягом усієї симуляції здорової активності системи. Всі три відносні кути — δM2−M1, δM3−M1(t), δM4−M1(t) зображені на одному графіку, щоб оцінити міжзонну динаміку та синхронізацію системи в цілому.

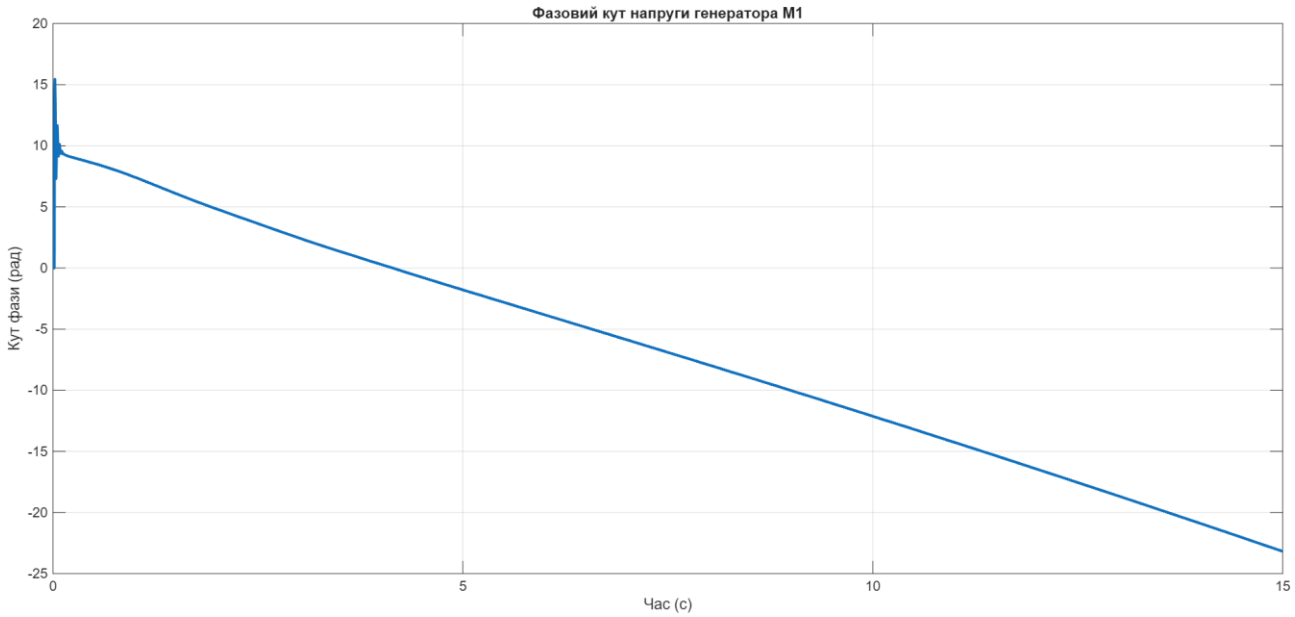

Рисунок 3.7 – Фазовий кут напруги M1 у здоровій системі

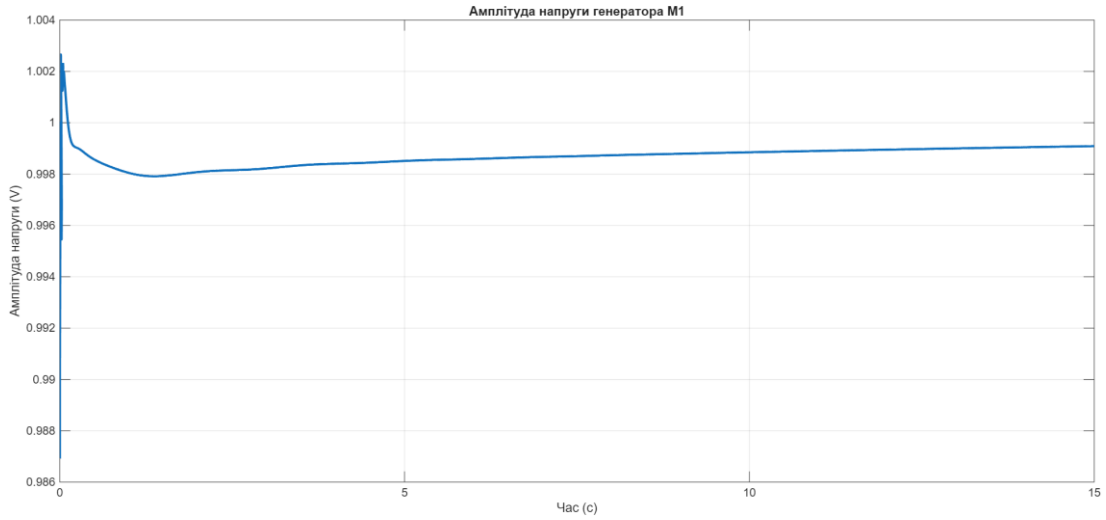

Рисунок 3.8 – Амплітуда напруги M1 у здоровій системі

На рисунках 3.7 і 3.8 зображені фазовий кут напруги генератора M1 у здоровому стані системи, знятий з PMU1 та амплітуда напруги з того ж PMU відповідно. Дані показники було проілюстровано з метою показати еталонний стан системи, а також продемонструвати відсутність впливу сторонніх чинників у спокійному режимі.

3.3 Стан системи після збою

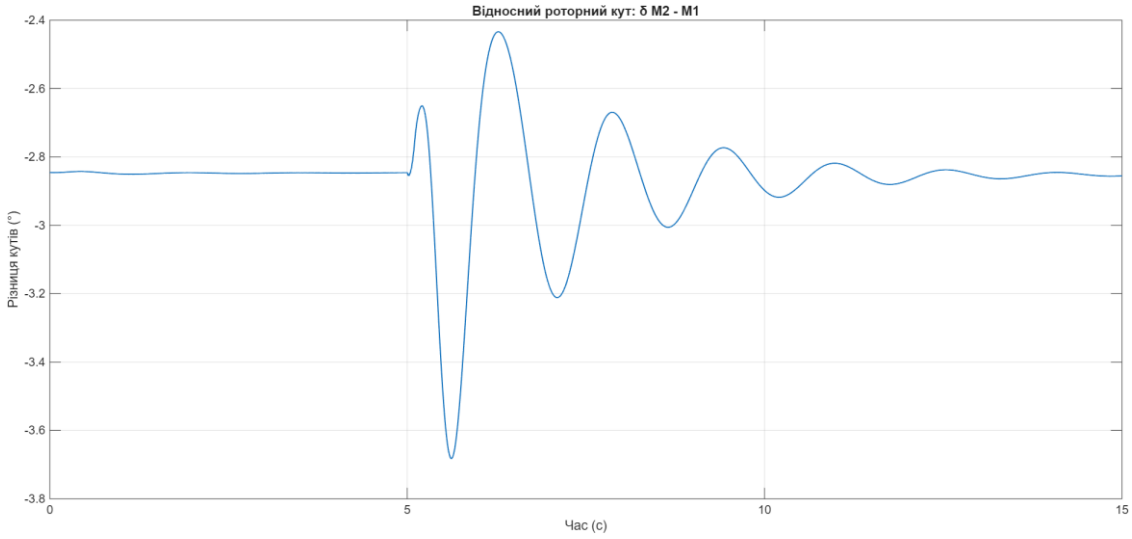

Рисунок 3.9 – Відносний кут між роторами M2 і M1 у здоровій системі після трифазного короткого замикання

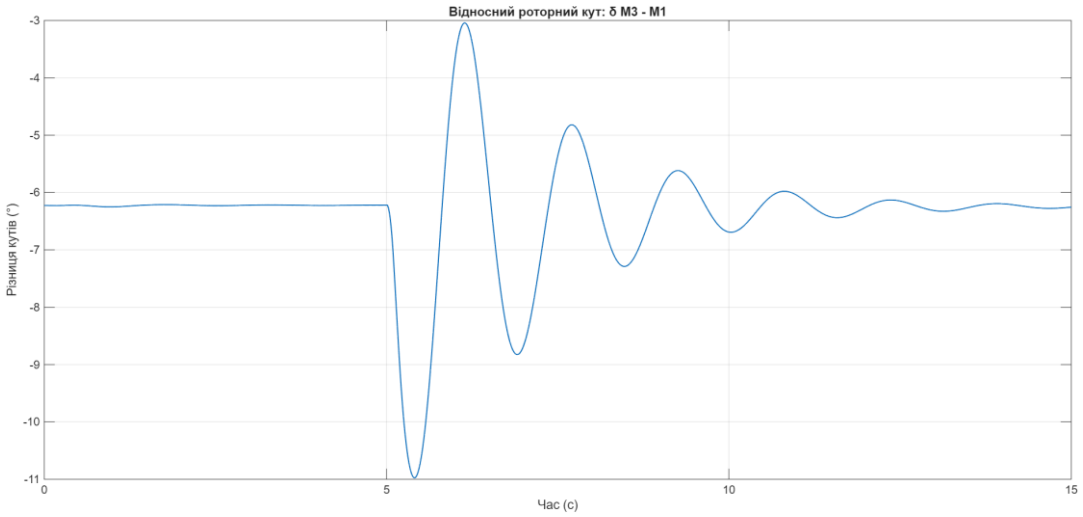

Рисунок 3.10 – Відносний кут між роторами М3 і М1 у здоровій системі після трифазного короткого замикання

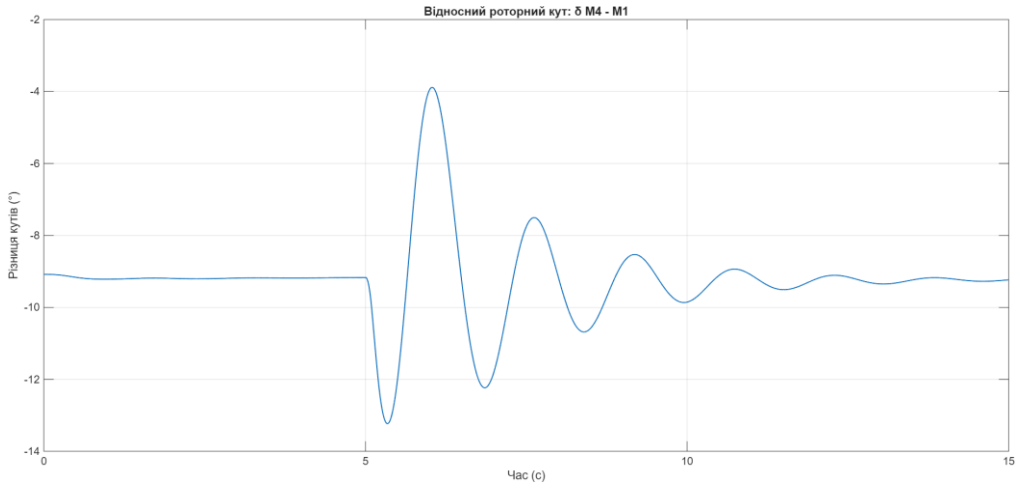

Рисунок 3.11 – Відносний кут між роторами М4 і М1 у здоровій системі після трифазного короткого замикання

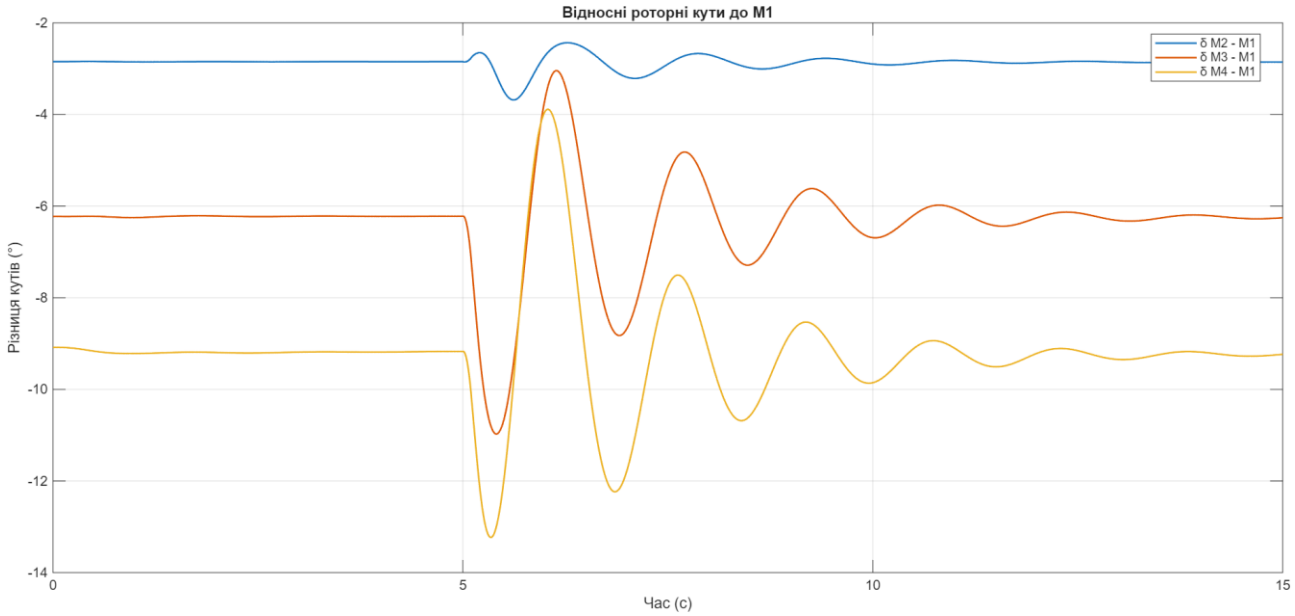

Рисунок 3.12 – Відносний кут між роторами M2,M3,M4 і M1 у здоровій системі після трифазного короткого замикання

На рисунках 3.9–3.12 зображені відносний кут між роторами M2,M3,M4 і M1 у здоровому стані системи після трифазного короткого замикання.

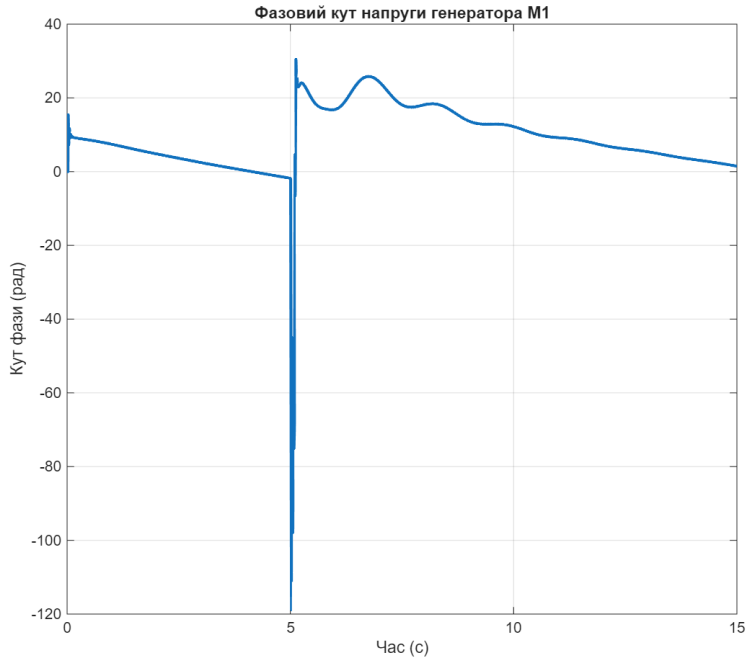

Рисунок 3.13 – Фазовий кут напруги M1 у здоровій системі після трифазного короткого замикання

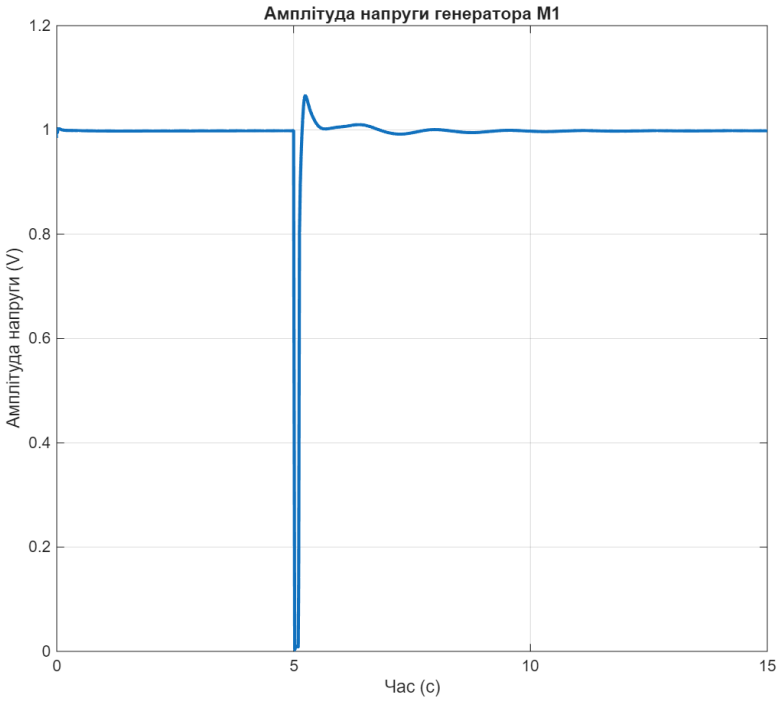

Рисунок 3.14 – Амплітуда напруги M1 у здоровій системі після трифазного короткого замикання

3.4 Блок атаки

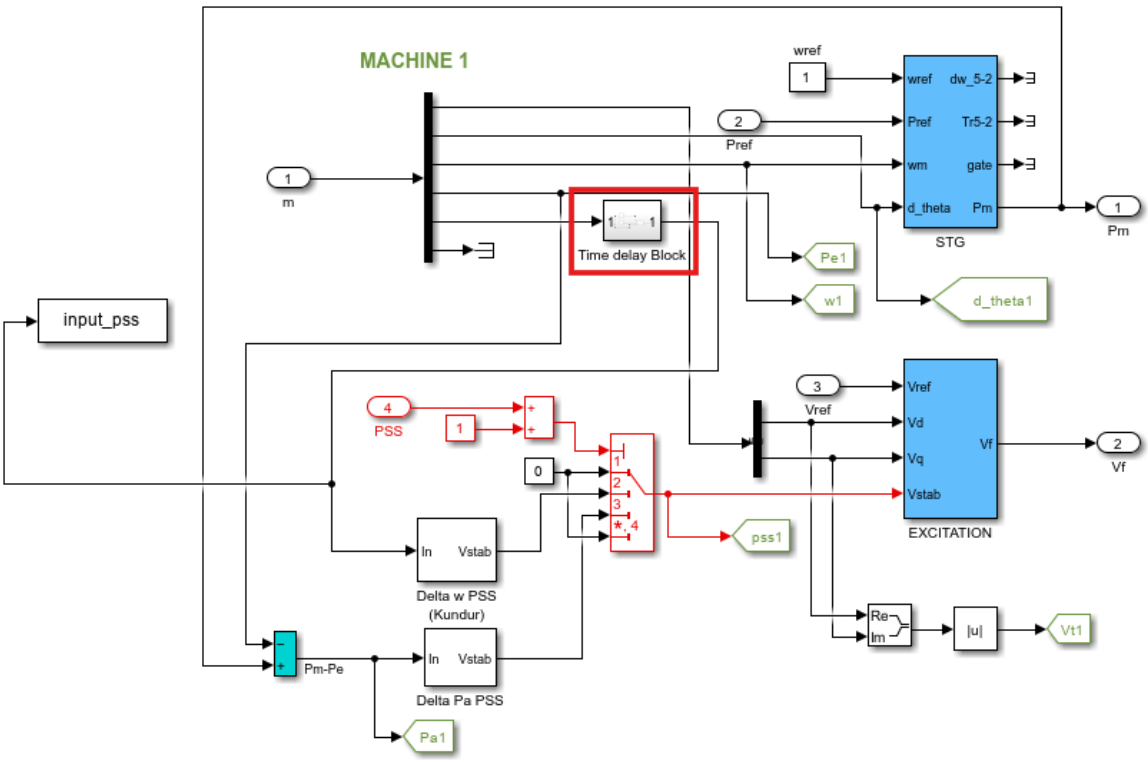

Рисунок 3.15 – Впровадження блок у часозатримної атаки

На рисунку 3.15 зображено блок, який відповідає за впровадження часозатримної атаки, атакований PSS – “Delta w PSS (Kundur)”, що розташований у зоні “M1: Turbine and regulators”. З використанням цього блоку буде імітуватися часозатримна атака на сигнал PSS. Далі буде наведно структуру зображеного блоку зсередини.

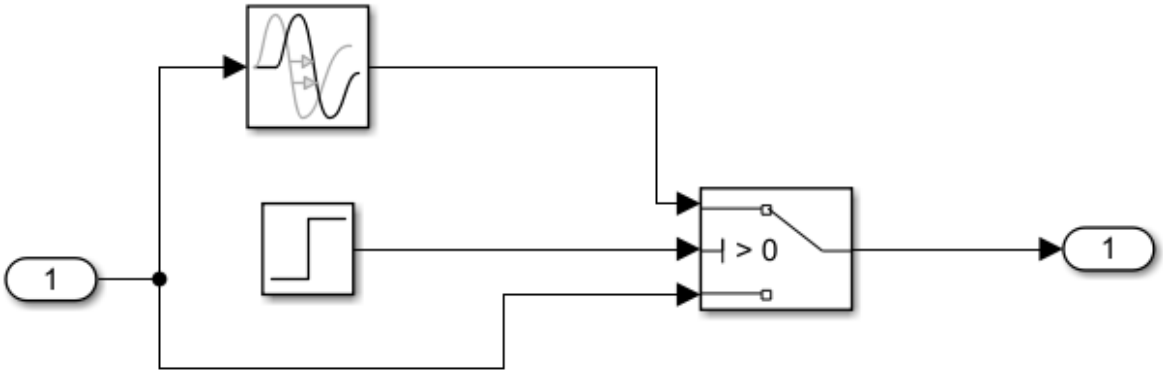

Рисунок 3.16 – Структура блоку часозатримної атаки

Як можна побачити з рисунку 3.16 сам блок отримує на вхід здоровий сигнал відбивання електромеханічних коливань генератора. Сам блок атаки складається з блоку Transport delay, який і затримуватиме сигнал на 2.5 секунди, оскільки саме це число було обране сталою зміщення сигналу, блоку Step, який допоможе розпочати атаку на 2.5 секунді, а до того на PSS надходитимуть актуальні дані, без затримки. Таким чином, спершу сигнал здорової системи буде надходити в реальному часі, а потім із сталою затримкою значення. Перехід від здорового сигналу до затриманого відбувається за допомогою блоку Switch.

3.5 Блок виявлення атаки

Оскільки вже було продемонстровано блок атаки у систему, є необхідним впровадження і блоку виявлення, що опрацьовуватиме значення кореляції та її похідної.

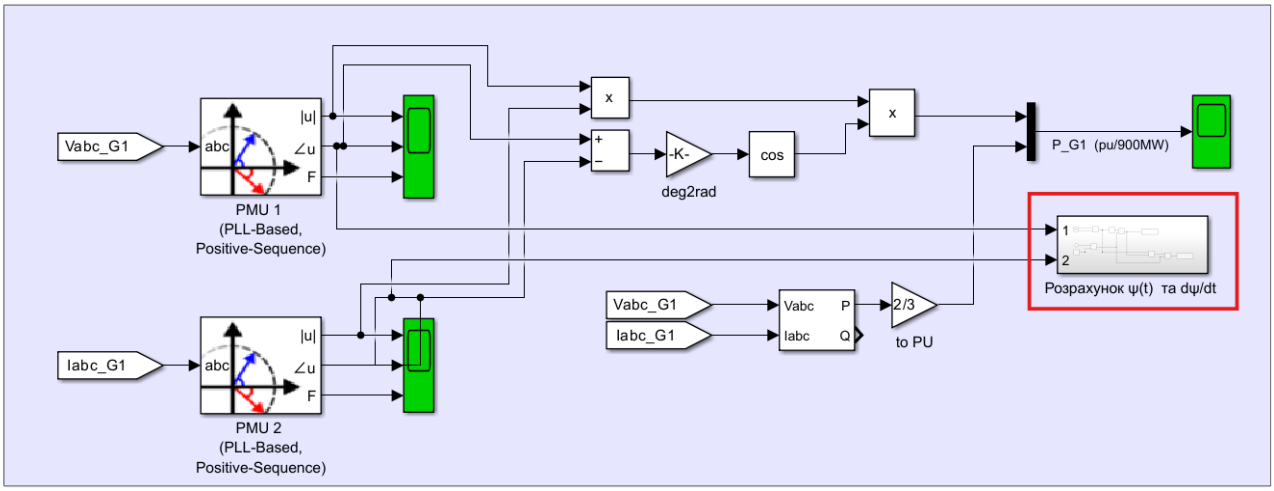

Рисунок 3.17 – Розташування блоку виявлення атаки

На рисунку 3.17 зображена зона впровадження блоку виявлення атаки, також червоним квадратом було обведено блок виявлення атаки, для візуальної зручності.

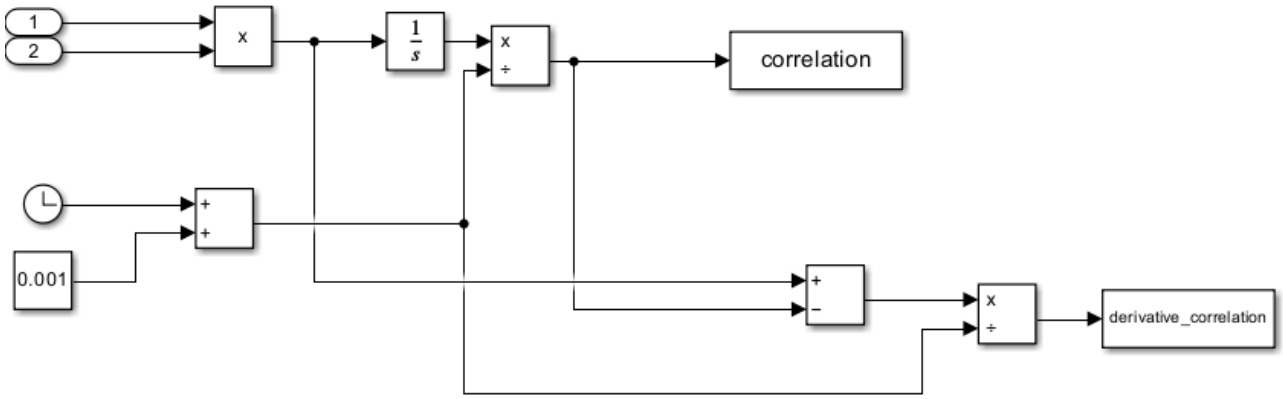

Рисунок 3.18 – Структура блоку виявлення атаки

Всередині блок складається з менших блоків, що рахують формули 2.12 – correlation $\psi(t)$ та 2.17 – derivative_correlation $\frac{d\psi}{dt}$. Сигнали 1 і 2 це сигнали $y'(t)$ та $s(t)$, що надходять з PMU1і PMU2- двох здорових вимірювачів, на генераторі M1. Для ε сталим значенням методом експериментального дослідження було обрано значення 0.001.

3.6 Результати тестування методу в системі

3.6.1 Здоровий стан системи без трифазового короткого замикання

В першу чергу, для аналізу швидкості зміни кореляції показників необхідно ознайомитися з її виглядом до моменту початку атаки.

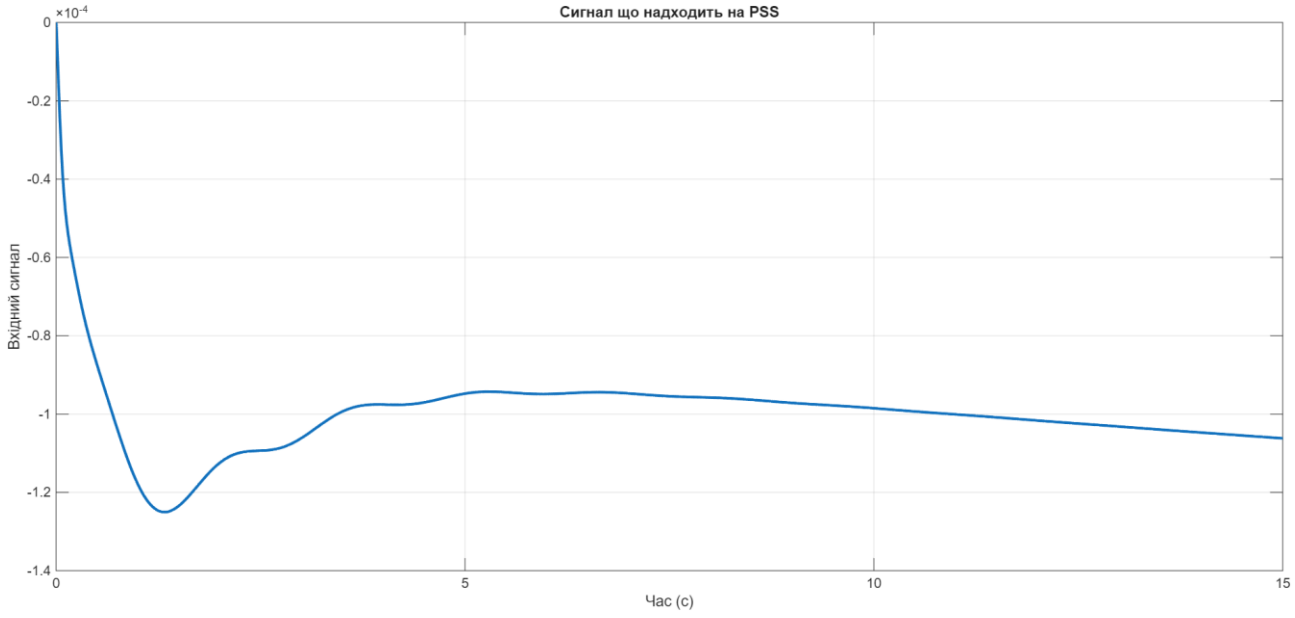

Рисунок 3.19 – Значення вхідного сигналу, що надходить на PSS у здоровому стані

На рисунку 3.19 показано, як змінюється вхідний сигнал на PSS, якщо система функціонує нормально, без збоїв і впровадження атаки. Варто звернути увагу, що проміжок коливань у здоровому стані сягає достатньо малих значень 0 - -$1.2*10^{-4}$.

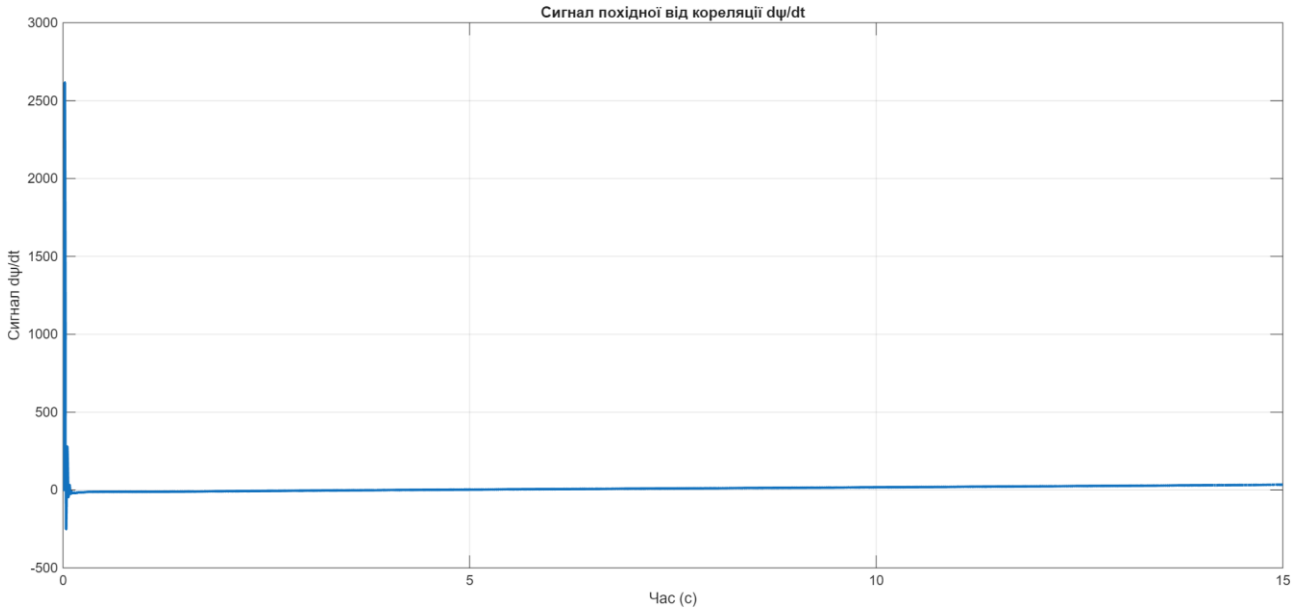

Рисунок 3.20 - Значення зміни сигналу похідної у нормальному стані

$\frac{d\psi}{dt}$ Має стрибок на початку проміжку, що пов'язаний з діленням на дуже мале значення ε, проте після 0,1255 с значення стабілізується і коливається в межах допустимого значення.

3.6.2 Здоровий стан системи з трифазним коротким замиканням

Далі було необхідно визначити, як відхиляється сигнал що надходить на PSS за умови наявності трифазового короткого замикання. Таким чином, були проведені повторні заміри з впровадженням збою на 5ій секунді симуляції роботи системи. Експериментально було перевірено, що здійснення збою саме на часовому проміжку 5-5.1с дає змогу спостерігати за відновленням системи до нормального стану, при умові відсутності атаки.

Аби продемонструвати реакцію генератора М1 на такий збуруючий вплив були заміряні наступні показники.

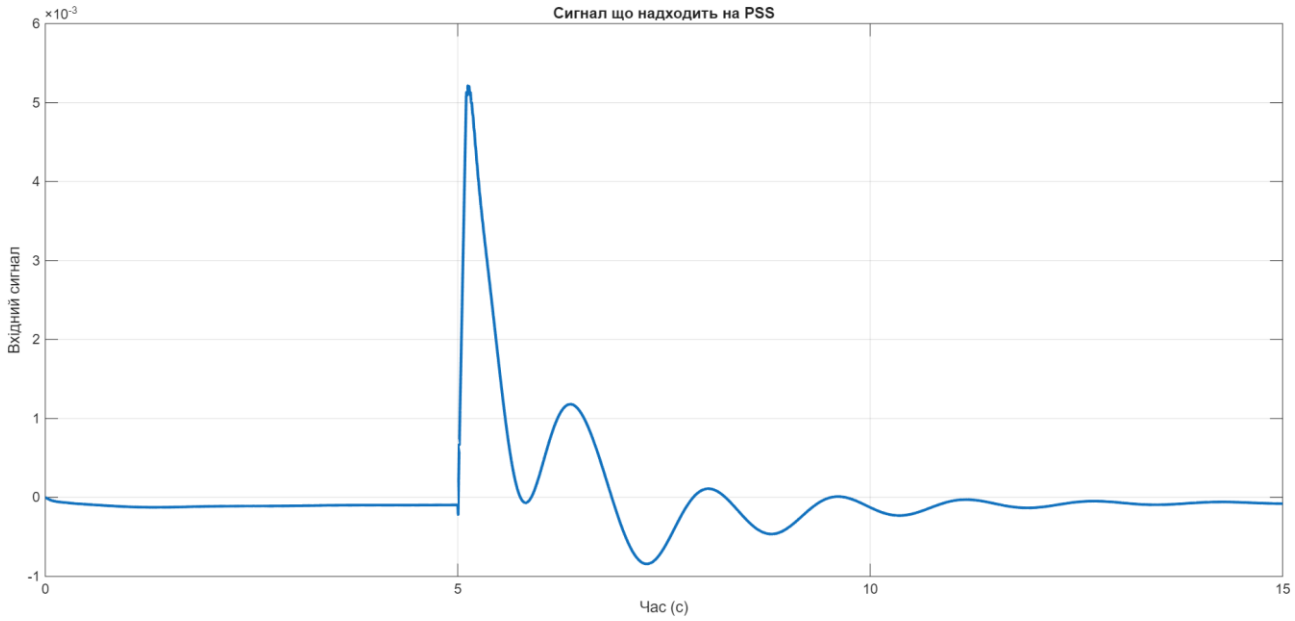

Рисунок 3.21 – Значення вхідного сигналу, що надходить на PSS у здоровому стані при трифазовому короткому замиканні

Як видно з рисунку 3.21 реакція системи на збурення, а також сигналу, що надходить на PSS є миттєвою, та після проходження певного часового проміжку, у випадку зображеному на графіку для повного відновлення стабільності системі знадобилося ~10 секунд.

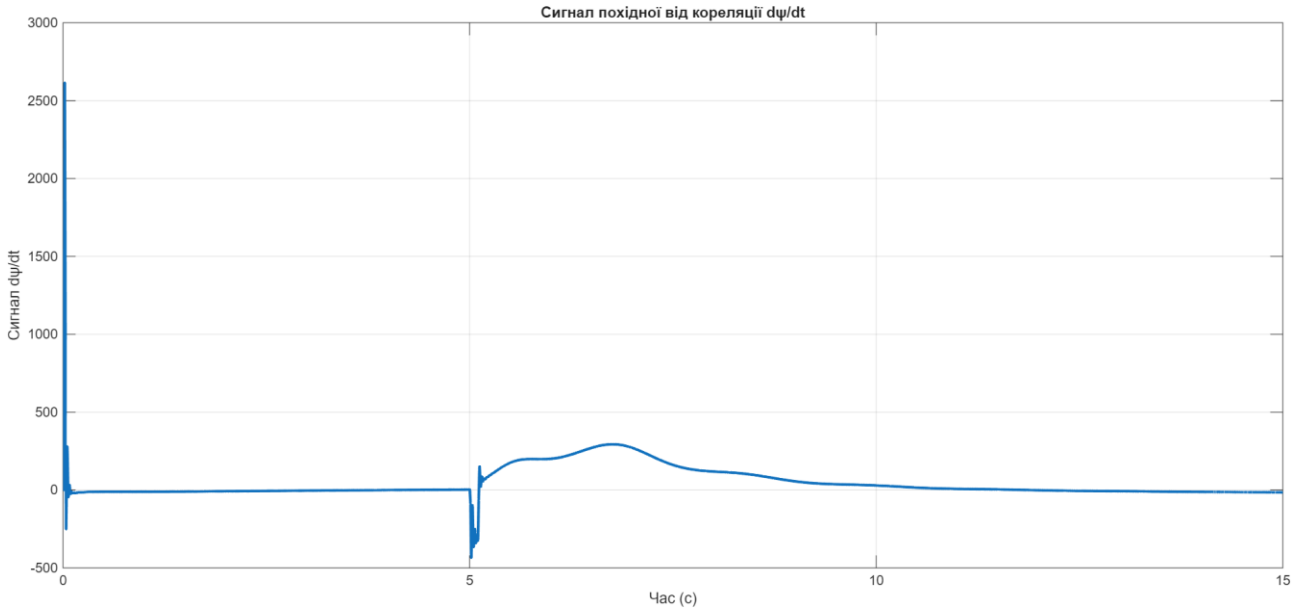

Рисунок 3.22 – Значення зміни сигналу похідної після трифазового збою

На рисунку 3.22 можна чітко побачити, що після збурення швидкість зміни кореляції зростає, та згодом повертається до стану норми, по мірі ліквідації міжзонального коливального впливу, викликаного збоєм.

3.6.3 Вигляд стану системи після впровадження блоку атаки

Оскільки задача полягає у виявленні атаки, що спричиняє деструктивний вплив на стабільність, то варто перевірити, який вплив сама атака може здійснити під час стабільної роботи системи.

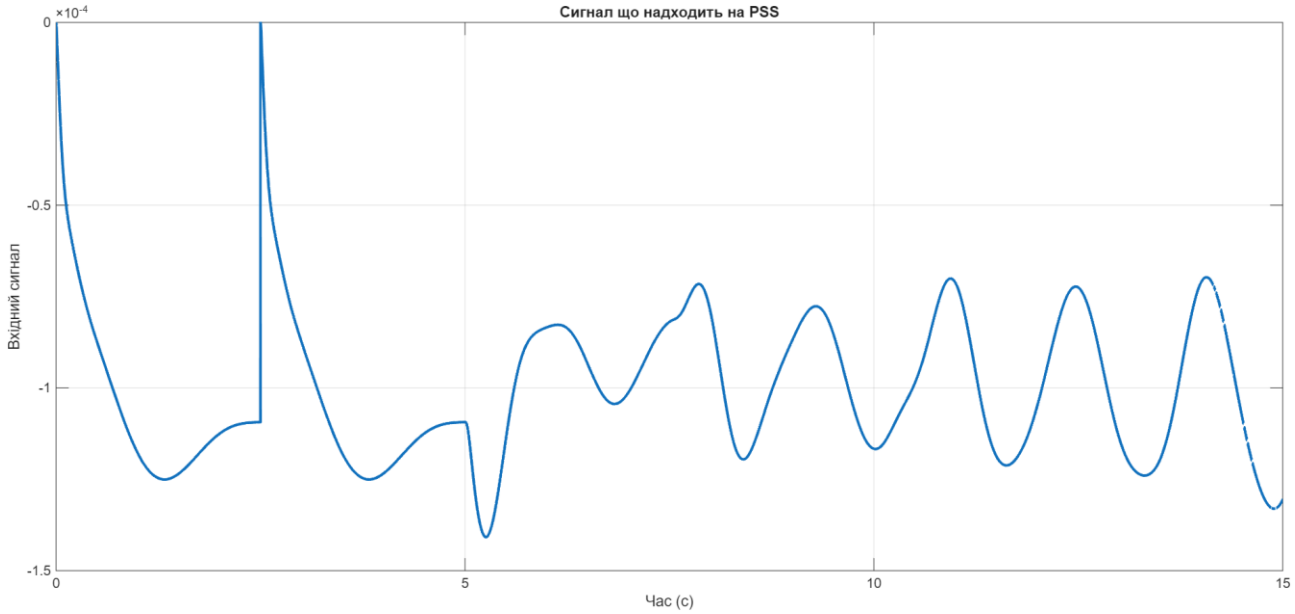

Рисунок 3.23 – Сигнал що надходить на уражений PSS

Як можемо побачити із візуалізації отриманих результатів, сигнал отриманий на 2.5 с відповідає сигналу на початку відрізку, саме тому час впровадження був підібраний 2.5 секунди від початку. Далі починаються незатухаючі збурення, через те, що на PSS завжди надходить сигнал із затримкою, проте самі коливання відбуваються на дуже малому рівні і не несуть значної шкоди системі, оскільки відхилення під час синхронної роботи є недостатніми для виведення системи з ладу.

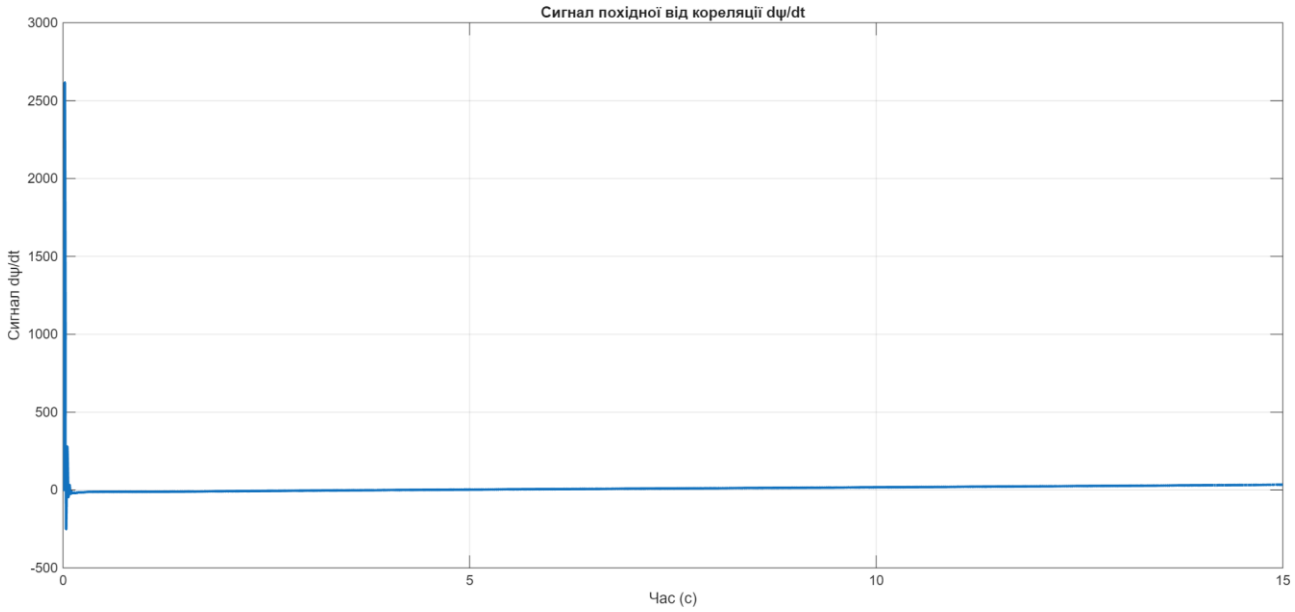

Рисунок 3.24 – Значення зміни сигналу похідної у «зараженому» стані

Проте, як видно з рисунку 3.24 такі малі коливання не впливають на зміну самої кореляції, її швидкість зміни коливається у допустимих значеннях. Для перевірки впливу атаки саме на PSS і здатність повернення до стабільного значення системи було знову введено трифазове коротке замикання на проміжку 5-5.1с

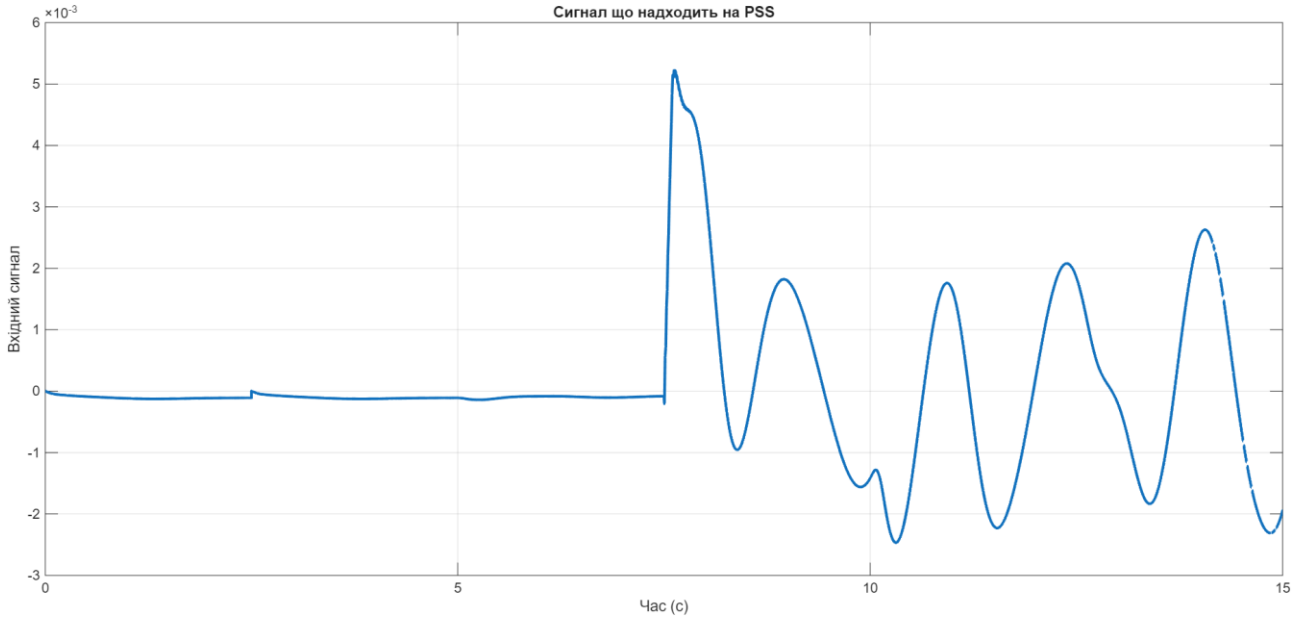

Рисунок 3.25 – Сигнал, що надходить на заражений PSS після збою

Можна спостерігати, що на точці 2.5 секунди від початку симуляції, маємо невеличкий стрибок, який краще видно на рисунку 3.23, та на рисунку

2.25 через зміну масштабів це коливання не здається таким відчутним, на відміну від тих, які спричинені трифазовим коротким замиканням і є нестабільними, через які PSS може дестабілізувати систему всупереч своєму призначенню.

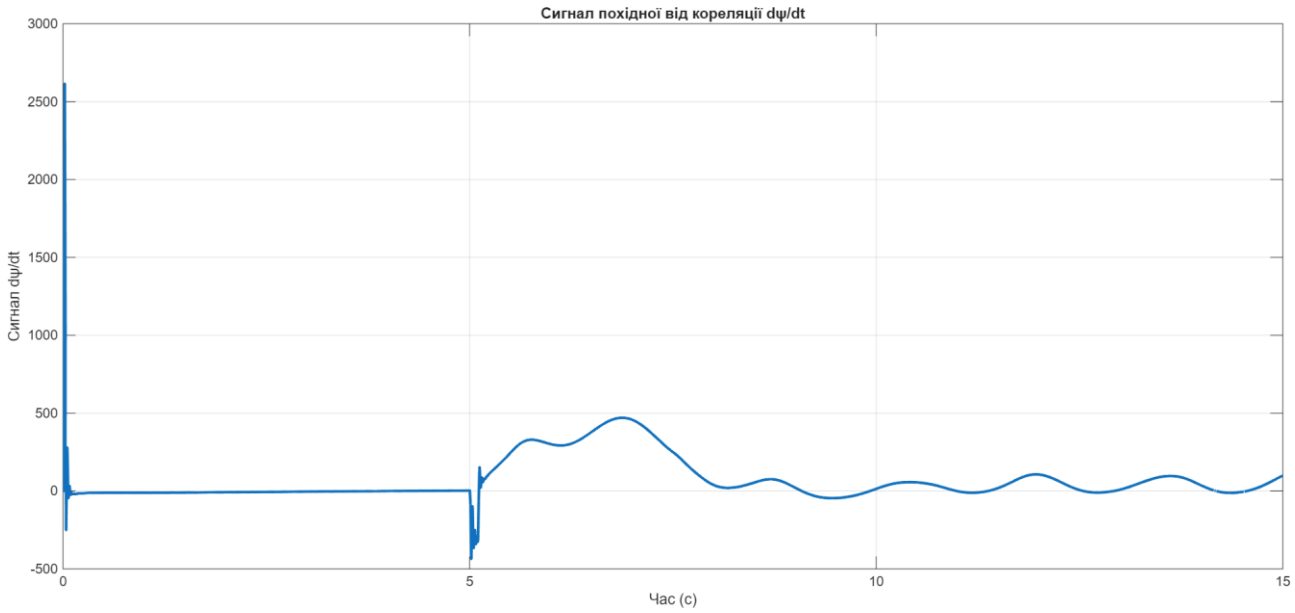

Рисунок 3.26 – Значення зміни сигналу похідної у «зараженому» стані після збурення

Хоча зростання максимальної швидкості зміни кореляції візуально помітне, це може бути не так добре зрозуміло у реальному стані системи, також варто зазначити, що на рисунку 3.26 помітно відсутність повернення швидкості зміни кореляції до еталонного стану.

Для цього і буде введено поріг, який визначатиме, що на систему здійснюється атака. Мірою визначення трешхолда стане максимальне допустиме значення для зміни швидкості кореляції після збою у здоровій системі. Для цього було знайдено пікову точку швидкості зміни кореляції на проміжку 3 секунди від початку атаки, оскільки саме швидкі виміри допоможуть зрозуміти, що була здійснена атака і її вплив не дає повернутися в нормальне положення після збою.

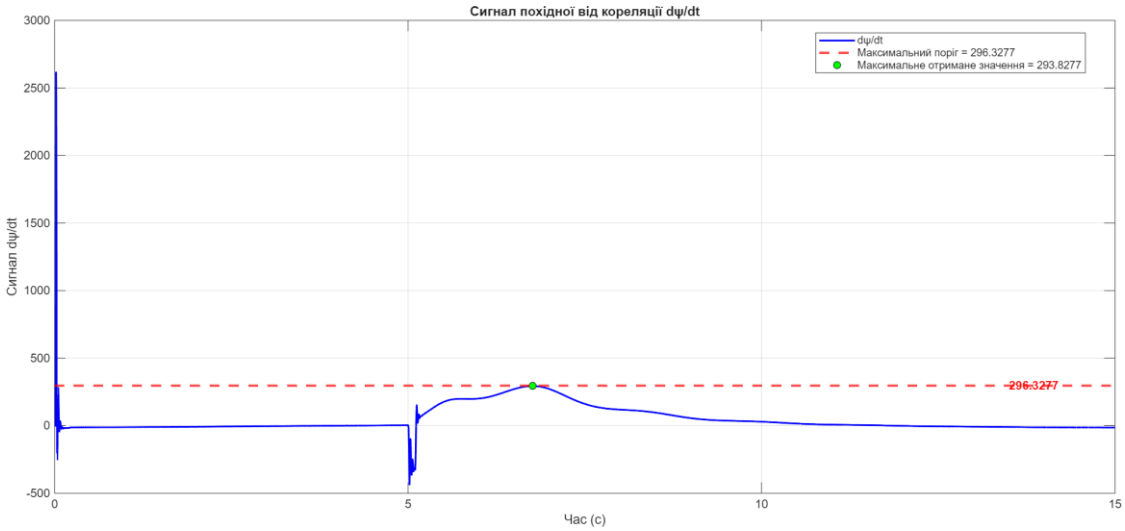

Рисунок 3.27 – Визначення порогового значення

Експериментальним методом значення threshold було визначене як максимум від швидкості зміни кореляції +2.5 од./с. Додатковий проміжок був доданий з метою врахування невеликих флуктуації, викликаних шумом, перехідними процесами або незначними збуреннями не пов'язаними з атакою, допустимим вважається відхилення в межах до +2.5 від цього максимуму. Інакше система має повідомляти про атаку. Найвище значення похідної сягнуло 293.8277 в $t = 6.7607$ с, в той час як максимальне допустиме значення 296.3277. Для підтвердження було повторно запущено систему уражену часозатримної атакою і побудовано графік швидкості зміни кореляції в часі.

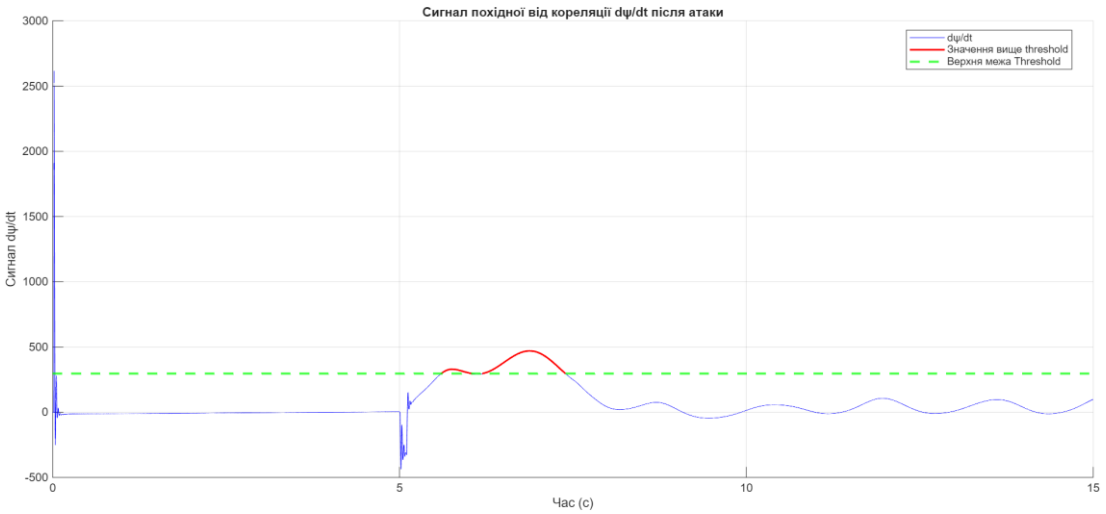

Рисунок 3.28 – Спрацювання виявлення атаки

На рисунку 3.28 червоним кольором виділено ті ділянки, де швидкість значно перевищила threshold на декількох послідовних кроках ітерування. А отже в системі дійсно є вплив часозатримної атаки.

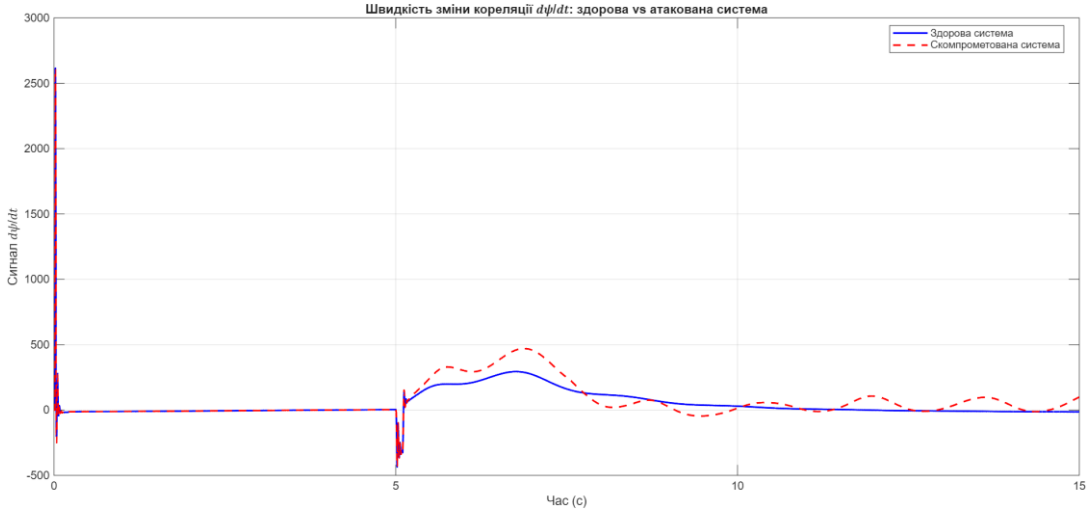

Рисунок 3.29 – Різниця швидкостей зміни кореляції у нормальній і скомпрометованій системі

Як результат експериментального дослідження було виявлено, що на проміжку часу 5.1-8.1с. $\xi\,(5.1-8.1\ \text{с}) = 49.001011$, а середня різниця у швидкості змін похідної (5.1–8.1с): 85.0403. Отже вирахувано, що у скомпрометованій системі, швидкість зміни похідної після збурення значно вища, що пов’язано із впливом часозатримної атаки.

Висновки до розділу 3

У даному розділі було здійснено практичне впровадження та тестування методу виявлення часозатримних атак в тестову мережу на базі двоконтурної системи Кундура. Проведено комплексне дослідження поведінки системи в трьох основних режимах: нормальна робота, робота при трифазному короткому замиканні та робота під впливом часозатримної атаки.

Аби забезпечити надійне виявлення кібератак було розроблено спеціальний блок детекції, що базується на аналізі кореляції між сигналами

PMU та швидкості її зміни. Встановлено оптимальні параметри системи виявлення, зокрема порогове значення.

Було показано, що часозатримна атака спричиняє значну деградацію стабільності енергосистеми. Якщо в нормальному стані коливання системи мають стабільний вигляд, то під час атаки система втрачає здатність до швидкого відновлення після збурень. Особливо критичним є вплив атаки на PSS, що призводить до впровадження нестабільних коливань замість виконання стабілізуючої функції.

Експериментально підтверджено ефективність методу виявлення: система надійно ідентифікує моменти, коли швидкість зміни кореляції перевищує встановлений поріг, що свідчить про наявність часозатримної атаки. Це дозволяє своєчасно виявляти атаки та вживати відповідних заходів протидії.

ВИСНОВКИ

У даній дипломній роботі було проведено аналіз енергетичних систем із фокусом на принципи роботи пристроїв стабілізації потужності PSS та вимірювальних пристроїв PMU. У результаті проведеного аналізу було виявлено критичні вразливості цих систем до часозатримних атак, які можуть призвести до порушення синхронізації та втрати стабільності енергосистеми. Встановлено, що більшість методів захисту недостатньо ефективні для протидії сучасним кібератакам, спрямованим на критичну інфраструктуру.

Сформовано математичні моделі атак із часовою затримкою, які дозволяють кількісно оцінити вплив кібератак на функціонування PSS. Ці моделі враховують специфіку роботи PSS та особливості передачі даних у системах.

Запропоновано інноваційний метод виявлення часозатримних атак на основі аналізу крос-кореляційної залежності між сигналами PMU. Цей метод дозволяє в режимі реального часу ідентифікувати аномальні затримки у передачі даних під час активного збурення системи та своєчасно активувати захисні механізми. Розроблений алгоритм характеризується високою чутливістю до атак, а threshold встановлений за результатами практичного дослідження.

Результати комп'ютерного моделювання підтвердили критичний вплив часозатримних кібератак на стабільність енергосистеми та продемонстрували ефективність запропонованого методу виявлення. Показано, що при перетині встановленого експериментальними вимірами порогу впродовж кількох ітерацій, реагування система виявляє часозатримну атаку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Cyber Attack[Електронний ресурс] // NIST.gov – Режим доступу до ресурсу: https://csrc.nist.gov/glossary/term/cyber_attack
2. What is a cyberattack? [Електронний ресурс] // IBM.com – 2021 – Режим доступу до ресурсу: https://www.ibm.com/think/topics/cyber-attack
3. Cybersecurity Challenges for Smart Grids: Protecting Critical Infrastructure [Електронний ресурс] // cyient.com – 2025 – Режим доступу до ресурсу: https://www.cyient.com/blog/cybersecurity-challenges-for-smart-grids-protecting-critical-infrastructure
4. Resecurity warns of increased cyber threats to energy and nuclear facilities from hacktivists and nation-states [Електронний ресурс] // industrialcyber.co – 2025 – Режим доступу до ресурсу: https://industrialcyber.co/utilities-energy-power-water-waste/resecurity-warns-of-increased-cyber-threats-to-energy-and-nuclear-facilities-from-hacktivists-and-nation-states/
5. Cybersecurity in the power sector [Електронний ресурс] // eurelectric.org – 2025 – Режим доступу до ресурсу: https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/
6. Cybersecurity for Energy and Utilities [Електронний ресурс] // darktrace.com – Режим доступу до ресурсу: https://www.darktrace.com/cyber-ai-glossary/cybersecurity-for-energy-and-utilities
7. Cyberattacks: preparing a defense for energy infrastructure [Електронний ресурс] // gevernova.com - Режим доступу до ресурсу: https://www.gevernova.com/gas-power/resources/articles/2021/energy-cyber-attack
8. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури: Постанова від 19 червня 2019р. // КАБІНЕТ МІНІСТРІВ УКРАЇНИ.
9. The Global Risks Report 2024. 19th ed. In partnership with Marsh McLennan and Zurich Insurance Group. Geneva: World Economic // World Economic Forum – 2024.

10. Critical infrastructure faces 30 percent surge in cyber attacks, KnowBe4 report highlights [Електронний ресурс] // industrialcyber.co – 28.08.2024 – Режим доступу до ресурсу: https://industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/
11. Cybersecurity – is the power system lagging behind? [Електронний ресурс] // iea.org – 01.08.2023 – Режим доступу до ресурсу: https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind
12. United States: Cyber attacks on energy infrastructure on the rise [Електронний ресурс] // energynews.pro – 12.09.2024 – Режим доступу до ресурсу: https://energynews.pro/en/united-states-cyber-attacks-on-energy-infrastructure-on-the-rise/
13. Understanding the Impact of Cyber Attacks on Non-Stop Production Industries [Електронний ресурс] // salvador-tech.com – 28.12.2024 – Режим доступу до ресурсу: https://www.salvador-tech.com/post/the-impact-of-cyber-attacks-on-non-stop-production-industries
14. The Energy Sector: A Prime Target for Cyber Attacks [Електронний ресурс] // fpa.org by Patricia Schouker – Режим доступу до ресурсу: https://fpa.org/energy-sector-prime-target-cyber-attacks/
15. Статистика кібератак на енергетику України [Електронний ресурс] // expro.com.ua – 30.10.2023 – Режим доступу до ресурсу: https://expro.com.ua/novini/54-vsh-kberatak-na-ukranu-pripadayut-na-energetiku
16. Кіберзахист енергосектору: у 2022 році заблоковано понад 1,5 млн спроб атакувати галузь // Міністерство енергетики України – 30.06.2023 – Режим доступу до ресурсу: https://www.mev.gov.ua/novyna/kiberzakhyst-enerhosektoru-u-2022-rotsi-zablokovano-ponad-15-mln-sprob-atakuvaty-haluz
17. Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology [Електронний ресурс] // Mandiant – 09.11.2023 – Режим доступу до ресурсу: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

18. Sandworm Hackers Caused Another Blackout in Ukraine —During a Missile Strike Energy Giant Halliburton Reveals $35m Ransomware Loss [Електронний ресурс] // Wired by Andy Greenberg – 09.11.2023 – Режим доступу до ресурсу: https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/
19. Energy Giant Halliburton Reveals $35m Ransomware Loss // infosecurity-magazine.com by Phil Muncaster – 12.11.2024 – Режим доступу до ресурсу: https://www.infosecurity-magazine.com/news/energy-giant-halliburton-35m/
20. Cyberattacks and Their Impact on Utilities and Energy [Електронний ресурс] // ironwoodcyber.com – 10.10.2024 – Режим доступу до ресурсу: https://www.ironwoodcyber.com/news/the-impact-of-cyberattacks-on-critical-infastructure
21. Critical Infrastructure Protection in Modern Society [Електронний ресурс] // industrialcyber.co – 21.05.2024 – Режим доступу до ресурсу: https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society/
22. Cybersecurity Threats to Critical Energy Infrastructure: Business Continuity in a Changing Geopolitical Environment // – 10.10.2023 https://insights.issgovernance.com/posts/cybersecurity-threats-to-critical-energy-infrastructure-business-continuity-in-a-changing-geopolitical-environment/
23. Power System Stabilizer [Електронний ресурс] // crystalinstruments.com — 18.07.2018 – Режим доступу до ресурсу: https://www.crystalinstruments.com/blog/2018/7/29/power-system-stabilizer
24. Kundur P., Balu N., Lauby M. Power System Stability and Control. — McGraw-Hill Education, 1994. — 1176 с. — (EPRI power system engineering series). — ISBN 9780070359581.;
25. Doradla, P. H. K., Emandi, R., Bhuvanagiri, N. V., & Gandrakota, G. S. S. (2011). Design Of Power System Stabilizer To Improve Small Signal Stability By Using Modified Heffron-Phillip's Model. International Journal of Engineering Science and Technology (IJEST), 3.

26. IEEE Recommended Practice for Excitation System Models for Power System Stability Studies // IEEE Std 421.5-2016 (Revision of IEEE Std 421.5-2005). — 2016. — С. 1—207. — DOI: 10.1109/IEEESTD.2016.7553421.]
27. Said A., Matsuo T. Assessment of Cyber Attacks against Power System Stabilizer and Their Detection Using Phasor Measurement Units // Journal of the Institute of Industrial Applications Engineers Vol. — 2024. — Т. 12, No 3. — С. 48—57. — DOI: 10.12792/JIIAE.12.48.
28. Y. Liu, P. Ning, and M. K. Reiter, “False Data Injection Attacks against State Estimation in Electric Power Grids ”, ACM Transactions on Information and System Security, Vol. 14, No. 1, Article No.13, pp.1-33, 2011.
29. A. Said, Y. Gotoh, T. Matsuo, Assessment of Replay Attacks against Power System Stabilizer, in: Proceedings of the 10th IIAE International Conference on Intelligent Systems and Image Processing 2023, The Institute of Industrial Applications Engineers, Japan, 2023.
30. X. Lou, C. Tran Huu, R. Tan, D. K. Y. Yau, and Z. T. Kalbarczyk, “Assessing and Mitigating Impact of Time Delay Attack against Cyber-Physical Systems,” 2016. URL: http://publish.illinois.edu/cps-security/files/2018/05/delay.pdf
31. Mathworks // https://ch.mathworks.com/help/sps/ug/pmu-pll-based-positive-sequence-kundur-s-two-area-system.html
32. Yilu Liu; Lamine Mili; Jaime De La Ree; Reynaldo Francisco Nuqui; Reynaldo Francisco Nuqui (2001-07-12). "State Estimation and Voltage Security Monitoring Using Synchronized Phasor Measurement". Research Paper from Work Sponsored by American Electric Power, ABB Power T&D Company, and Tennessee Valley Authority. Virginia Polytechnic Institute and State University. CiteSeerX 10.1.1.2.795933.
33. M.S. Iantorno and K. Beladda, “Fuzzy Logic for Cybersecurity: Intrusion Detection and Privacy Preservation with Synthetic Data,” 2023.
34. Intriago, A., Liberati, F., Hatziargyriou, N. D., & Konstantinou, C. (2023). Residual-Based Detection of Attacks in Cyber-Physical Inverter-Based Microgrids. ArXiv Preprint ArXiv:2306.07082. https://arxiv.org/abs/2306.07082

35. M. Kravchik and A. Shabtai, “Efficient Cyber Attack Detection in Industrial Control Systems Using Lightweight Neural Networks and PCA,” IEEE Transactions on Dependable and Secure Computing, 2021, doi: 10.1109/TDSC.2021.3050101.
36. I. Khan and V. Centeno, “Detecting GPS-spoofing Attack on PMU Data with Phase Angle Unwrapping Technique and Low-Rank Approximation of Hankel Matrix”, Proc. of 2022, IEEE Power & Energy Society General Meeting (PESGM), pp.17-21, 2022.
37. P. Gao, M. Wang, J. H. Chow, S. G. Ghiocel et al., “Identification of successive ‘Unobservable’ cyber data attacks in power systems through matrix decomposition,” IEEE Transactions on Signal Processing, vol. 64, pp. 5557–5570, 2016.
38. Sargolzaei, A., Yen, K. K., Abdelghani, M. N., Mehbodniya, A., & Sargolzaei, S. (2015). A novel technique for detection of time delay switch attack on load frequency control. Intelligent Control and Automation, 6(04), 205.
39. Tuyizere, D., & Ihabwikuzo, R. (2023). Machine Learning to detect cyber-attacks and discriminating the types of power system disturbances. arXiv preprint arXiv:2307.03323.
40. Yin, T., Naqvi, S. A. R., Nandanoori, S. P., & Kundu, S. (2024, December). Advancing Cyber-Attack Detection in Power Systems: A Comparative Study of Machine Learning and Graph Neural Network Approaches. In 2024 Resilience Week (RWS) (pp. 1-9). IEEE.
41. Косарик Д. А., Гальчинський Л. Ю. Пом’якшення наслідків атаки на нижньому рівні управління, як елемент резильєнтності об’єктів критичної інфраструктури. // XXII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених теоретичні і прикладні проблеми фізики, математики та інформатики. — 2024. — Т. 22. — С. 265—268.
42. Слєпий Р.Ю., Гальчинський Л. Ю. Використання PMU для виявлення атаки на енергетичну інфраструктуру // XXIII всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених теоретичні і прикладні проблеми фізики, математики та інформатики. — 2025. — Т. 23 с. 267-269.

43. D. B. Rawat and C. Bajracharya, “Detection of false data injection attacks in smart grid communication systems”, IEEE Signal Processing Letters, Vol. 22, pp.1652-1656, 2015.
44. X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D.Dominnguez-Garcia, “Spoofing GPS receiver clock offset of phasor measurement units ”, IEEE Transactions on Power Systems, Vol.28, No.3, pp.3253-3262, 2013.
45. S. Barreto, M. Pignati, G. Dan, J. Y. Le Boudec, and M. Paolone, “Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation ”, IEEE Transactions on Smart Grid, Vol. 9, pp. 3530-3542, 2018.
46. S. B. Andrade, J.-Y. Le Boudec, E. Shereen, G. Dan, M.Pignati, and M. Paolone, “A continuum of undetectable timing-attacks on PMU-based linear state-estimation ”, Proc. of 2017 IEEE International Conference on Smart secure framework for resource-limited adversaries ”, Automatica, Vol.51, pp.135–148, 2015.
47. K. Murakami, H. Suemitsu, and T. Matsuo, “Classification of Repeated Replay Attacks and Its Detection Monitor ”, Proc.of 2017 IEEE 6th Global Conference on Consumer Electronics, pp.320–321, 2017.
48. A. Said, Y. Gotoh, and T. Matsuo, “Assessment of Replay Attacks against Power System Stabilizer ”, Proc. of the 10th IIAE International Conference on Intelligent Systems and Image Processing 2023 (ICISIP 2023), pp.4-10, 2023.
49. A. Xue, H. Kong, Y. Yongzhao, F. Xu, L. Wang, G. Wei, B. Shi, S. Leng, T. Bi, “Method of amplitude data recovery in PMU measurements that considers synchronisation errors”, IET Gener. Transm. Distrib., Vol. 14, Iss. 24, pp. 5746-5755, 2020.