

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)

«_____» _____ 2026 р.

Дипломна робота

на здобуття ступеня бакалавра

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

спеціальності 125 «Кібербезпека»

на тему: «Порівняльна оцінка кіберрезильєнтності мікромережі при переході від
традиційного керування до системи на основі федеративного навчання»

Виконав (-ла): здобувач вищої освіти IV курсу, групи ФБ-21

Тютюннікова Віолета

Керівник Гальчинський Леонід Юрійович

доцент кафедри інформаційної безпеки, к.т.н., доцент,

(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент _____

_____ (посада, науковий ступінь, вчене звання, науковий ступінь,
прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без відповідних
посилань.

Здобувач вищої освіти _____ (підпис)

Київ – 2026 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)

«17» червня 2026 р.

**ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти**

Тютюннікова Віолета Євгенівна
(прізвище, ім'я, по батькові)

1. Тема роботи «Порівняльна оцінка кіберрезильєнтності мікромережі при переході від традиційного керування до системи на основі федеративного навчання»
Керівник роботи Гальчинський Леонід Юрійович к.т.н., доцент, доцент кафедри інформаційної безпеки,

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «29»_травня 2026 р. № 2001-с

2. Термін подання роботи здобувачем вищої освіти «09» червня 2026 р.

3. Вихідні дані до роботи

Літературні джерела, існуючі підходи до оцінки кіберрезильєнтності об'єктів критичної інфраструктури, архітектурні специфікації традиційних та Smart Grid енергосистем, еталонна тестова система IEEE 33-Bus, реальні CVE-ідентифікатори, математична модель теорії складних мереж, бібліотеки Python (pandapower, networkx, PyTorch), алгоритм федеративного навчання FedAvg, існуючі підходи до виявлення аномалій у профілях напруги розподільчих мереж.

4. Зміст (дипломної роботи) пояснювальної записки (перелік завдань, які потрібно розробити)

Огляд літературних джерел з аналізу концепції кіберрезильєнтності та архітектурних особливостей традиційних і Smart Grid енергосистем, порівняння поверхонь кіберзагроз обох архітектур, обґрунтування методу оцінки та розробка математичного апарату комплексного показника резильєнтності на базі теорії складних мереж, побудова графових моделей на тестовій системі IEEE 33-Bus, реалізація програмного інструменту симуляції кібератак з прив'язкою до реальних CVE-ідентифікаторів, реалізація модуля федеративного навчання для раннього виявлення аномалій та оцінка його впливу на інтегральну резильєнтність.

5. Перелік графічного (ілюстративного) матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо) презентація.

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Визначення напрямку ДР	17.02.2026 – 03.03.2026	Виконано
2	Визначення теми ДР	04.03.2026 – 07.03.2026	Виконано
3	Огляд наукової літератури за темою	08.03.2026 – 18.03.2026	Виконано
4	Аналіз кіберрезильєнтності та архітектур енергосистем	19.03.2026 – 28.03.2026	Виконано
5	Аналіз вразливостей вузлів мережі та системи CVSS	29.03.2026 – 03.04.2026	Виконано
6	Написання першого розділу	04.04.2026 – 14.04.2026	Виконано
7	Розробка показника резильєнтності R, динамічної моделі інциденту та системи федеративного навчання	15.04.2026 – 30.04.2026	Виконано
8	Написання другого розділу	01.05.2026 – 10.05.2026	Виконано
9	Програмна реалізація інструменту (Python, pandapower, LSTM, FedAvg)	11.05.2026 – 22.05.2026	Виконано
10	Проведення експериментів та аналіз результатів	23.05.2026 – 28.05.2026	Виконано
11	Написання третього розділу	29.05.2026 – 02.06.2026	Виконано
12	Оформлення ДР	03.06.2026 – 05.06.2026	Виконано
13	Створення презентації для передзахисту	06.06.2026 – 07.06.2026	Виконано
14	Передзахист	09.06.2026	
15	Захист	17.06.2026	

Здобувач вищої освіти

(підпис)

Керівник роботи

(підпис)

Віолета ТЮТЮННІКОВА
(Власне ім'я, ПРІЗВИЩЕ)

Леонід ГАЛЬЧИНСЬКИЙ
(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг роботи 77 сторінок, 16 ілюстрацій, 3 таблиці, 49 джерел літератури.

Об'єкт дослідження: кіберрезильєнтність розподільчих енергетичних систем.

Предмет дослідження: порівняння кіберрезильєнтності традиційної мережі та інтелектуальної Smart Grid із застосуванням федеративного навчання.

Мета дослідження: порівняльна оцінка кіберрезильєнтності енергосистеми при переході від традиційного централізованого керування до системи на основі федеративного навчання.

Методи дослідження: теорія складних мереж і теорія графів, система CVSS, федеративне навчання (FedAvg) та LSTM, інтегральна оцінка кривої $R(t)$; моделювання на еталонній мережі IEEE 33-Bus засобами Python.

Отримані результати: розроблено програмний інструмент порівняльної оцінки кіберрезильєнтності двох архітектур (традиційної та Smart Grid із федеративним навчанням) на мережі IEEE 33-Bus із прив'язкою до реальних CVE. Показано, що за координованої атаки традиційна мережа втрачає 57 % резильєнтності, а Smart Grid із федеративним навчанням - 7 %; федеративне навчання скоротило час виявлення атаки до 8.8–11.5 с і підвищило F1-міру детектора до 0.85–0.94 при збереженні конфіденційності даних.

Результати роботи були представлені на XXIV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених "Теоретичні і прикладні проблеми фізики, математики та інформатики".

Ключові слова: кіберрезильєнтність, Smart Grid, федеративне навчання, FedAvg, електроенергетика.

ABSTRACT

The thesis comprises 77 pages, 16 figures, 3 tables, and 49 references.

Research object: cyber resilience of distributed power systems.

Research subject: comparison of the cyber resilience of a traditional grid and an intelligent Smart Grid using federated learning.

Research objective: comparative assessment of the cyber resilience of a power system during the transition from traditional centralized control to a system based on federated learning.

Research methods: complex network theory and graph theory, the CVSS system, federated learning (FedAvg) and LSTM, integral evaluation of the $R(t)$ curve; modeling on the IEEE 33-Bus reference network using Python.

Results: A software tool was developed for the comparative assessment of the cyber resilience of two architectures (traditional and Smart Grid with federated learning) on the IEEE 33-Bus network, linked to real CVEs. It is shown that under a coordinated attack, the traditional network loses 57% of its resilience, while the Smart Grid with federated learning loses 7%; federated learning reduced attack detection time to 8.8–11.5 s and increased the detector's F1 score to 0.85–0.94 while preserving data privacy.

The results of the work were presented at the 24th All-Ukrainian Scientific and Practical Conference of Students, Graduate Students, and Young Scientists “Theoretical and Applied Problems of Physics, Mathematics, and Computer Science.”

Keywords: cyber resilience, Smart Grid, federated learning, FedAvg, electric power engineering.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	9
ВСТУП.....	12
1 КІБЕРРЕЗИЛЬЄНТНІСТЬ ЕНЕРГЕТИЧНИХ МЕРЕЖ.....	15
1.1 Кіберрезильєнтність як властивість критичної інфраструктури	15
1.2 Архітектура традиційних централізованих енергосистем.....	16
1.3 Інтелектуальні енергосистеми на основі мікрокластерної архітектури.....	20
1.4 Порівняльний аналіз поверхні кіберзагроз та механізмів локалізації відмов	23
1.5 Вразливості вузлів мережі як вектор реалізації кібератак.....	24
1.6 Аналіз існуючих методів оцінки та підвищення кіберрезильєнтності, обґрунтування методологічного підходу	25
Висновки до розділу 1	28
2 МЕТОДИКА ПОРІВНЯЛЬНОЇ ОЦІНКИ КІБЕРРЕЗИЛЬЄНТНОСТІ ЕНЕРГЕТИЧНИХ МЕРЕЖ.....	31
2.1 Обґрунтування вибору методу оцінки.....	31
2.2 Система оцінки вразливостей вузлів мережі	32
2.3 Параметри топології мережі як кількісні показники резильєнтності..	34
2.3.1 Алгебраїчна зв'язність.....	35
2.3.2 Середня найкоротша відстань	36
2.3.3 Середня центральність за посередництвом.....	36
2.3.4 Діаметр графа.....	37
2.3.5 Критичне навантаження.....	38
2.3.6 Комплексний показник резильєнтності R	38
2.4 Перемикання резервних ліній як механізм відновлення системи	40
2.5 Динамічна модель інциденту та інтегральна резильєнтність.....	41
2.6 Федеративне навчання як механізм раннього виявлення аномалій	43

2.7 Методика комплексної порівняльної оцінки двох архітектур енергомереж	47
Висновки до розділу 2	48
3 РЕАЛІЗАЦІЯ ІНСТРУМЕНТУ ПОРІВНЯЛЬНОЇ ОЦІНКИ КІБЕРРЕЗИЛЬЄНТНОСТІ.....	50
3.1 Моделювання топологій та тестове середовище	50
3.2 Реалізація комплексного показника резильєнтності та динамічної моделі інциденту	56
3.3 Реалізація системи федеративного навчання як механізму раннього виявлення атак	59
3.4 Реалізація багаторівневої логіки детекції та прийняття рішень	62
3.5 Результати експерименту та аналіз.....	62
Висновки до розділу 3	69
ВИСНОВКИ	71
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SCADA (Supervisory Control and Data Acquisition) - система диспетчерського управління та збору даних.

RTU (Remote Terminal Unit) - віддалений термінал збору даних.

PLC (Programmable Logic Controller) - програмований логічний контролер.

HMI (Human-Machine Interface) - людино-машинний інтерфейс.

DER (Distributed Energy Resources) - розподілені джерела енергії.

IoT (Internet of Things) - Інтернет речі.

AMI (Advanced Metering Infrastructure) - інфраструктура інтелектуального обліку (інтелектуальні лічильники).

ICS (Industrial Control Systems) - промислові системи управління.

IDS (Intrusion Detection System) - система виявлення вторгнень.

VPN (Virtual Private Network) - віртуальна приватна мережа.

FDI (False Data Injection) - атака впровадження хибних даних.

DoS (Denial of Service) - атака на відмову в обслуговуванні.

CVE (Common Vulnerabilities and Exposures) - міжнародна система ідентифікаторів публічно відомих вразливостей інформаційної безпеки.

CVSS (Common Vulnerability Scoring System) - відкрита система кількісної оцінки тяжкості вразливостей.

CWSS (Common Weakness Scoring System) - система оцінки класів архітектурних слабкостей програмного забезпечення.

EPSS (Exploit Prediction Scoring System) - система прогнозування ймовірності експлуатації вразливості.

NVD (National Vulnerability Database) - Національна база даних вразливостей США.

FL (Federated Learning) - федеративне навчання.

FedAvg (Federated Averaging) - алгоритм зваженого усереднення ваг моделей у федеративному навчанні.

LSTM (Long Short-Term Memory) - рекурентна нейронна мережа з довгою короткочасною пам'яттю.

BFS (Breadth-First Search) - алгоритм пошуку в ширину.

PMU (Phasor Measurement Unit) - пристрій синхронізованих векторних вимірювань.

Smart Grid - інтелектуальна енергетична мережа з двостороннім потоком електроенергії та інформації.

NIST (National Institute of Standards and Technology) - Національний інститут стандартів і технологій США.

NIAC (National Infrastructure Advisory Council) - Консультативна рада з питань критичної інфраструктури США.

NERC CIP (North American Electric Reliability Corporation - Critical Infrastructure Protection) - стандарт захисту критичної інфраструктури електроенергетики.

IEC (International Electrotechnical Commission) - Міжнародна електротехнічна комісія.

IEEE (Institute of Electrical and Electronics Engineers) - Інститут інженерів електротехніки та електроніки.

CISA (Cybersecurity and Infrastructure Security Agency) - Агентство з кібербезпеки та безпеки інфраструктури США.

E-ISAC (Electricity Information Sharing and Analysis Center) - центр обміну та аналізу інформації в електроенергетиці.

IEEE 33-Bus - еталонна 33-вузлова тестова розподільча електрична мережа.

λ_2 - алгебраїчна зв'язність (друге за величиною власне значення матриці Лапласа, значення Фідлера).

L - середня найкоротша відстань між вузлами графа.

$d(u,v)$ - мінімальна кількість ребер на шляху між вершинами u та v .

$C_B(v)$ - центральність за посередництвом вершини v .

C_{AB} - середня центральність за посередництвом графа.

σ_{st} - загальна кількість найкоротших шляхів між вершинами s та t .

$\sigma_{st}(v)$ - кількість найкоротших шляхів між s та t , що проходять через вершину v .

D - діаметр графа.

E_{CL} - частка обслугованого критичного навантаження.

R - комплексний показник резильєнтності.

$R(t)$ - часова крива показника резильєнтності.

ΔR - приріст показника резильєнтності після замикання резервних ліній.

$F1$ – гармонічне середнє точності та повноти (метрика якості детектора аномалій).

МВт – мегават (одиниця активної потужності).

МВА – мегавольт-ампер (одиниця повної потужності).

кА – кілоампер (одиниця сили струму).

Ом/км – питомий опір лінії електропередачі.

Кіберрезильєнтність – здатність системи передбачати загрози, поглинати вплив кібератаки, витримувати її та швидко відновлювати власну функціональність.

Мікрокластер (мікромережа) – локально обмежена електрична система з власними джерелами генерації, накопичувачами та контролером, здатна функціонувати у підключеному та острівному режимах.

Острівний режим – автономний режим роботи мікрокластера, за якого він живить локальних споживачів від власних DER без зв'язку із зовнішньою мережею.

Каскадна деградація – послідовне поширення відмов мережею після компрометації вузла або лінії електропередачі.

Резервна лінія (tie-line) – нормально розімкнена міжсегментна з'єднувальна лінія, замикання якої відновлює зв'язність мережі після інциденту.

Інтегральна резильєнтність – нормована площа під кривою $R(t)$, що одночасно враховує глибину провалу, тривалість деградованого стану та динаміку відновлення.

ВСТУП

Актуальність роботи:

Енергетична інфраструктура є одним із ключових елементів критичної інфраструктури держави, від стабільного функціонування якої залежить робота систем охорони здоров'я, водопостачання, транспорту та зв'язку. Стрімка цифровізація енергосистем відкриває принципово нові вектори кіберзагроз, атаки на об'єкти критичної енергетичної інфраструктури перейшли з категорії гіпотетичних сценаріїв до задокументованих реальних інцидентів. Атака BlackEnergy 3 та систематичні кібероперації під час повномасштабного вторгнення підтверджують, що захист енергомереж від кіберзагроз є стратегічним пріоритетом національної безпеки. Традиційна парадигма кіберзахисту, орієнтована на запобігання атакам, виявляється недостатньою в сучасних умовах. Альтернативою є концепція кіберрезильєнтності - здатності системи передбачати загрози, витримувати атаки та відновлювати власну функціональність. Водночас систематичне кількісне порівняння кіберрезильєнтності традиційних централізованих мереж та інтелектуальних систем за умов ідентичних кіберзагроз залишається відкритим науковим завданням. Це особливо актуалізується у контексті застосування федеративного навчання, яке забезпечує конфіденційність даних та підвищує ефективність виявлення аномалій у розподілених енергетичних системах, що й обґрунтовує необхідність подальших досліджень у цій сфері.

Метою дослідження: є порівняльна оцінка кіберрезильєнтності енергосистеми при переході від традиційного централізованого керування до інтелектуальної системи на основі федеративного навчання.

Завдання дослідження:

1. Проаналізувати концепцію кіберрезильєнтності, архітектурні особливості та порівняти поверхні кіберзагроз традиційних і Smart Grid енергосистем.

2. Обґрунтувати вибір методу оцінки, розробити математичну модель комплексного показника резильєнтності, формалізувати алгоритм її обчислення та побудувати графові моделі на тестовій системі IEEE 33-Bus.

3. Реалізувати програмний інструмент симуляції кібератак та провести порівняльний аналіз чотирьох сценаріїв з реальними CVE-ідентифікаторами.

4. Реалізувати модуль федеративного навчання на основі LSTM та FedAvg для раннього виявлення аномалій та оцінити його вплив на інтегральну резильєнтність через динамічну модель інциденту.

Об'єкт дослідження: кіберрезильєнтність розподільчих енергетичних систем в умовах кіберфізичних атак на основі вразливостей вузлів мережі.

Предмет дослідження: методи кількісної оцінки та порівняльного аналізу кіберрезильєнтності традиційних та Smart Grid розподільчих енергосистем із застосуванням федеративного навчання.

Методи дослідження: теорія складних мереж і теорія графів для моделювання топологічних властивостей мереж; система CVSS для класифікації кіберзагроз; алгоритм BFS та метод власних значень матриці Лапласа для обчислення параметрів резильєнтності; федеративне навчання (зважений алгоритм FedAvg) для децентралізованого виявлення аномалій у профілях напруги; нейронна мережа на основі LSTM для виявлення аномальних і нормальних режимів роботи енергетичної системи; інтегральна оцінка резильєнтності на основі числового інтегрування кривої $R(t)$; моделювання на тестовій системі IEEE 33-bus із бібліотекою pandapower для верифікації результатів.

Новизна одержаних результатів: Удосконалено методику оцінки кіберрезильєнтності розподільчих енергомереж завдяки комплексній метриці, яка інтегрує топологічні параметри графа, електричний показник критичного навантаження та реальні CVSS-оцінки технічних вразливостей. Запропоновано модель порівняння двох архітектурних конфігурацій на єдиній шкалі з чотирифазною часовою динамікою інциденту, що враховує підтримку критичних навантажень в автономному острівному режимі та ранню детекцію атак засобами

федеративного навчання. Адаптовано та оптимізовано децентралізоване федеративне навчання на базі LSTM-мереж та алгоритму FedAvg через механізм локального донавчання, який дозволяє виявляти кібератаки на ранніх стадіях без ризику розкриття операційних даних.

Практичне значення одержаних результатів: Розроблений програмний інструмент дозволяє операторам розподільчих мереж кількісно обґрунтовувати перехід від традиційної архітектури до Smart Grid та є відтворюваним на еталонній системі IEEE 33-Bus із можливістю адаптації до реальних топологій. Методику розрахунку показника резильєнтності та динамічної моделі інциденту можна застосовувати на етапі проектування й реконструкції об'єктів критичної інфраструктури для оцінки ефективності резервних ліній і оптимального розміщення розподілених джерел генерації. Архітектура FL-модуля з персоналізованим донавчанням може слугувати прототипом систем децентралізованого виявлення аномалій для підприємств енергосектору з підвищеними вимогами до конфіденційності.

Апробація результатів роботи: XXIV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених "Теоретичні і прикладні проблеми фізики, математики та інформатики"

1 КІБЕРРЕЗИЛЬЄНТНІСТЬ ЕНЕРГЕТИЧНИХ МЕРЕЖ

1.1 Кіберрезильєнтність як властивість критичної інфраструктури

Сучасна критична інфраструктура функціонує в умовах постійної невизначеності та зростаючої кількості кібератак, та векторів їх реалізації. В таких умовах традиційна парадигма захисту інформаційних систем, побудована на принципах недопущення атаки, виявляється принципово недостатньою. З огляду на це в академічному та практичному середовищі відбувається перехід до результат-орієнтовної моделі, центральною складовою якої є поняття кіберрезильєнтності - властивості системи продовжувати функціонувати та відновлюватися навіть під впливом атаки.

Поняття резильєнтності є міждисциплінарним за своїм походженням: воно прийшло в інженерію з психології та екології, де описує здатність живих систем зберігати ключові функції та відновлюватись після зовнішніх збурень. У контексті критичної інфраструктури Національний інститут стандартів і технологій США (NIST) у публікації SP 800-160 визначає кіберрезильєнтність як здатність готуватися до мінливих умов та пристосовуватися до них, а також витримувати збій у роботі та швидко відновлюватися після нього; включає здатність витримувати цілеспрямовані атаки, аварії або природні загрози чи інциденти, а також відновлюватися після них [1]. Консультативна рада з питань критичної інфраструктури США (NIAC) визначає кіберрезильєнтність в контексті критичної інфраструктури як здатність зменшувати масштаби та/або тривалість подій, що спричиняють збитки. Ефективність стійкої інфраструктури або підприємства залежить від їхньої здатності передбачати, пом'якшувати наслідки, адаптуватися та/або швидко відновлюватися після потенційно збиткової події [2].

Фреймворк Cybersecurity Compass розглядає кіберрезильєнтність як критичну фазу безперервного циклу кібербезпеки поряд з управлінням ризиками та виявленням і реагуванням. Вихідна теза фреймворку полягає в тому, що жодна

організація не може повністю унеможливити кіберінциденти, тому здатність поглинати удар, відновлюватись і навчатись є настільки ж важливою, як і превентивний захист. Цикл кіберрезильєнтності охоплює три послідовні фази:

- Поглинання інциденту - в момент атаки резильєнтна система продовжує виконувати критичні функції, мінімізуючи глибину деградації.
- Відновлення - оперативне повернення до нормального рівня функціональності з мінімальним операційним простоем і відхиленням від стратегічних цілей.
- Навчання та адаптація - постінцидентний аналіз перетворює кожен удар на джерело вдосконалення захисних механізмів, підвищуючи стійкість до майбутніх загроз.

Загальна мета всіх трьох фаз це скорочення одночасно глибини деградації при атаці та часу відновлення після неї. Організація, що послідовно проходить цей цикл, з кожним інцидентом стає менш вразливою та швидше відновлює функціональність [3].

1.2 Архітектура традиційних централізованих енергосистем

Сучасна енергосистема України є прямою спадщиною радянської електроенергетичної моделі, побудованої за централізованим ієрархічним принципом. Великі потужності генерують електроенергію, що передається через систему підстанцій різних класів напруги до кінцевих споживачів. Переважно енергосистема має радіальну структуру - вузли послідовно з'єднані від живильних підстанцій до споживачів без резервних шляхів передачі електроенергії. Через це пошкодження однієї магістральної лінії може спричинити каскадні наслідки для всіх споживачів, підключених до цієї лінії. Така структурна вразливість радіальної топології підтверджується системним аналізом мережі на основі теорії складних мереж [4]. Приклад такої радіальної топології з вузлами критичного навантаження наведено на рисунку 1.1.



Рисунок 1.1 – Топологія традиційної радіальної розподільчої мережі

Управління такою мережею реалізує окрема система - централізована й зосереджена в єдиному диспетчерському центрі, де оператори здійснюють моніторинг та управління через систему SCADA (Supervisory Control and Data Acquisition). SCADA-система інтегрує дані від розподілених по мережі віддалених терміналів (Remote Terminal Unit, RTU), програмованих логічних контролерів (Programmable Logic Controller, PLC) та людино-машинних інтерфейсів (Human-Machine Interface, HMI), що відображають стан тисяч точок мережі в режимі реального часу [5]. Таку трирівневу ієрархію управління - від диспетчерського центру через RTU/PLC до польових пристроїв - наведено на рисунку 1.2.

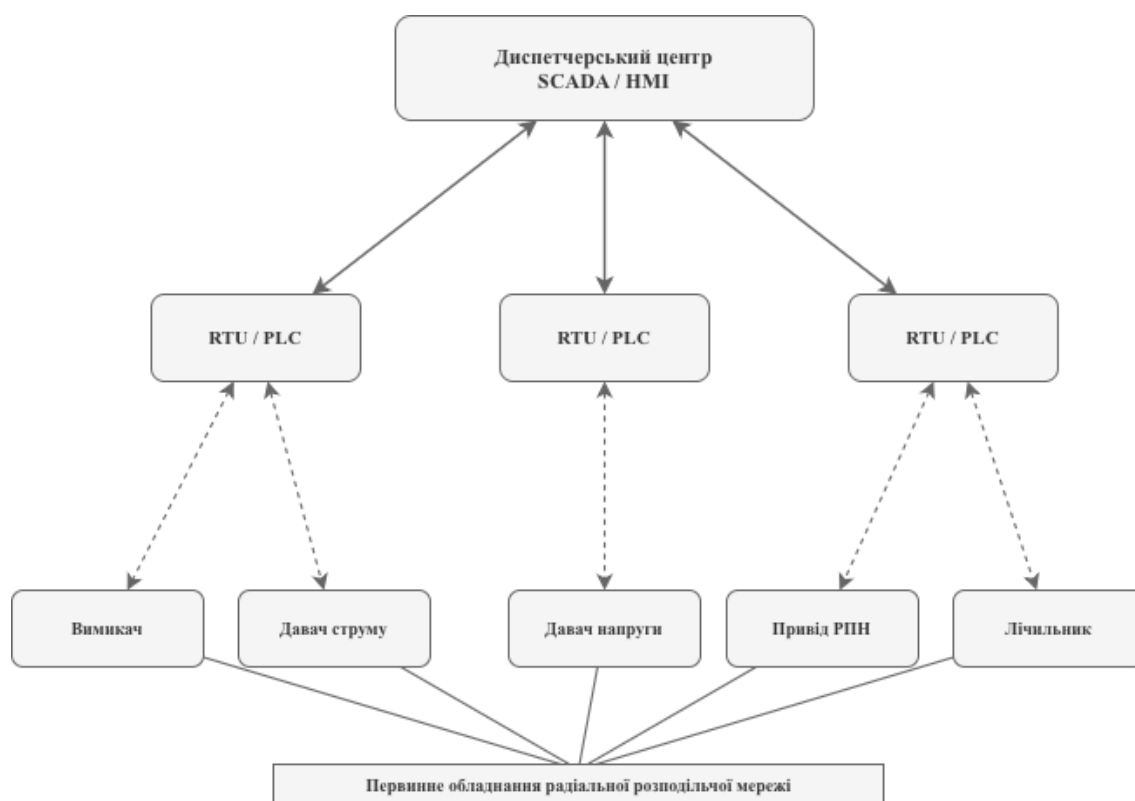


Рисунок 1.2 – Трирівнева архітектура системи управління традиційним енергооб'єктом

Принципово важливим аспектом є те, що системи SCADA традиційних енергомереж проектувалися із пріоритетом доступності і надійності над безпекою, оскільки на той момент кіберзагрози не розглядалися як реалістичний ризик. У термінах теорії графів розподільча мережа середньої напруги має радіальну структуру без циклів, тобто є деревом, на відміну від високовольтних передавальних мереж, які мають петлеву топологію з надлишковими шляхами [6]. Це означає, що видалення будь-якого ребра або вузла гарантовано розділяє граф, і кожна успішна атака на транзитний вузол автоматично перетворюється на каскадне послідовне відключення без жодних механізмів локалізації.

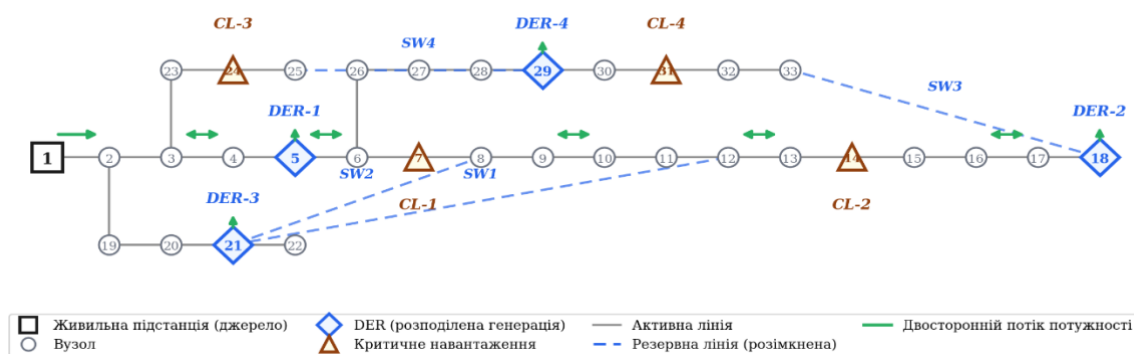
Практичним підтвердженням цієї теоретичної вразливості стала атака BlackEnergy 3 на українських операторів енергосистеми у грудні 2015 року. Згідно з офіційним звітом CISA, зловмисники отримали легітимні облікові дані та використали їх для дистанційного доступу до системи управління через VPN-

з'єднання. Опинившись усередині мережі, вони здійснювали пряме дистанційне керування вимикачами підстанцій через програмне забезпечення промислових систем управління, фактично використовуючи SCADA так само, як і легітимний диспетчер. Атака була скоординована і відбулась на трьох обленерго синхронно. По завершенні оперативної фази зловмисники запустили шкідливе програмне забезпечення KillDisk на серверах SCADA, яке знищило файли та пошкодило завантажувальні записи систем, унеможлививши дистанційне відновлення. Внаслідок атаки без електроенергії залишилися близько 225 000 споживачів [7]. Аналіз цієї кібератаки, проведений спільною командою E-ISAC та SANS ICS, дозволив сформулювати ключові висновки щодо природи сучасних кіберзагроз для SCADA-систем. Встановлено, що ні BlackEnergy 3, ні KillDisk самі по собі не спричинили відключення електроенергії, фактичною причиною стало пряме дистанційне керування зловмисниками системою SCADA через HMI для відкриття вимикачів підстанцій. Всі інші інструменти слугували або для отримання доступу, або для затримки відновлення. Було зафіксовано якісно новий характер атаки, вперше у світовій практиці зловмисники не лише використали ICS проти його власних операторів, але й цілеспрямовано знищили засоби відновлення - пошкодили прошивку польових пристроїв та видалили системне програмне забезпечення, знищивши шляхи для автоматичного відновлення [8].

Таким чином, архітектура традиційної централізованої енергосистеми характеризується специфічним профілем кіберрезильєнтності, що визначається двома взаємопов'язаними особливостями. З одного боку, відносно невелика кількість цифрових компонентів обумовлює вузьку поверхню атаки, а отже зловмисник має обмежену кількість точок мережевого входу. З іншого боку, радіальна топологія та повна залежність від централізованого ручного відновлення забезпечують вкрай низьку структурну резильєнтність, тому будь-яка успішна атака на ключовий вузол автоматично трансформується в каскадне відключення, а відновлення займає критично тривалий час. Така система є відносно важкою для проникнення, але катастрофічно вразливою після успішної компрометації.

1.3 Інтелектуальні енергосистеми на основі мікрокластерної архітектури

Концепція Smart Grid являє собою автоматизовану широкорозгалужену мережу енергопостачання, що характеризується двостороннім потоком електроенергії та інформації і може контролювати все: від електростанцій до уподобань споживачів та окремих побутових приладів. Топологію інтелектуальної мережі з розподіленими джерелами, критичними навантаженнями та резервними лініями, де потік потужності є двостороннім, наведено на рисунку 1.3.



реалізованим рішенням для підтримки мережі в екстремальних умовах і збереження живлення критичних навантажень [11]. Острівний режим є визначальним для кіберрезильєнтності: при виявленні атаки або порушенні зв'язку із зовнішньою мережею мікрокластер продовжує жити локальних споживачів від власних DER без участі оператора. Дослідження підтверджують, що при атаках типу FDI та DoS на ізольовану мікромережу правильно спроектований розподілений регулятор забезпечує відновлення частоти та балансу потужності завдяки острівному режиму DER [12]. Принципово важливим є інституційний вимір цієї властивості: децентралізована система з тисячами автономних вузлів усуває ризик єдиної точки відмови, оскільки локальна самодостатність кожного сегмента обмежує наслідки атаки масштабом окремого кластера - на відміну від централізованої архітектури, де компрометація диспетчерського центру призводить до повного відключення сегмента без механізму автономного відновлення [13]. Концептуальну архітектуру такої децентралізованої системи та ієрархію її управління наведено на рисунку 1.4.

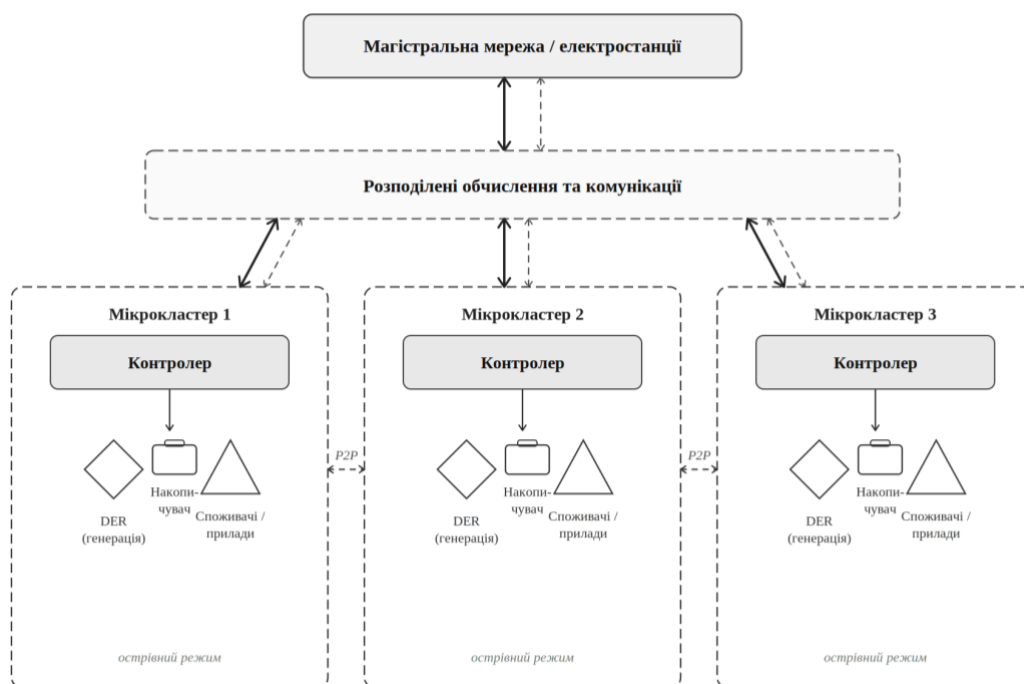


Рисунок 1.4 – Архітектура розподіленої системи управління інтелектуальною мікромережею

Ефективне функціонування мікрокластерної архітектури забезпечується взаємодією трьох взаємозалежних рівнів, спільне проектування яких є ключовим принципом побудови кіберрезильєнтної мікромережі. Фізичний рівень охоплює генеруючі установки, системи накопичення енергії та навантаження кластера. Комунікаційний рівень відповідає за обмін даними та управляючими сигналами між компонентами. Кіберрівень реалізує функції виявлення аномалій, автоматичного реагування та координації між компонентами системи. Саме узгоджене проектування всіх трьох рівнів, а не ізольований захист кожного окремо визначає здатність мікромережі зберігати функціональність під час кібератаки [14].

На відміну від традиційних систем, Smart Grid спирається на стандартизовані протоколи з вбудованим захистом, де IEC 61850 стандартизує обмін між компонентами підстанційного рівня та забезпечує сумісність пристроїв різних виробників, тоді як IEC 62351 визначає вимоги до автентифікації та шифрування трафіку [15]. Завдяки цьому компрометація мережевого доступу в Smart Grid не надає зловмиснику автоматичного контролю над обладнанням, на відміну від традиційної системи, де відсутність верифікації команд перетворює будь-який несанкціонований доступ до мережі на пряму загрозу підстанціям. Практичним механізмом відновлення зв'язності при кібератаці є автоматичне замикання перемикачів міжсегментних з'єднувальних ліній (tie-line). У нормальному стані ці перемикачі розімкнені, зберігаючи радіальну топологію для спрощення управління потоками потужності. При виявленні ізоляції сегмента контролер автоматично замикає відповідний перемикач, відновлюючи зв'язність мережі. Ключовою перевагою є швидкість, автоматичне відновлення займає секунди, тоді як ручне відновлення традиційної системи вимірюється годинами [16].

Таким чином, Smart Grid не скасовує кіберризики, а якісно перерозподіляє їх, замість критично важливих цілей з'являється велика кількість менш критичних з обмеженим локальним впливом при компрометації. Мікрокластерна сегментація означає, що успішна атака на окремий вузол не поширюється на решту системи - суміжні сегменти продовжують функціонувати незалежно, а скомпрометований

кластер переходить до острівного режиму живлення від власних DER. Острівна робота є не аварійним відступом, а спроектованою нормою поведінки системи в умовах загрози.

1.4 Порівняльний аналіз поверхні кіберзагроз та механізмів локалізації відмов

Порівняння кіберрезильєнтності двох архітектур потребує розмежування між кількістю потенційних точок проникнення та системними наслідками їх компрометації. Традиційна централізована система та інтелектуальна мережа Smart Grid характеризуються діаметрально протилежними профілями кіберризиків, що визначаються їх топологічними та функціональними особливостями. Традиційна централізована енергосистема характеризується відносно вузькою поверхнею атаки, обумовленою обмеженою кількістю цифрових компонентів. Основними потенційними точками проникнення є SCADA-сервери, RTU/PLC та мережеві канали між ними. У систематичних аналізах кібербезпеки енергомереж зазначають, що в традиційних системах кількість цифрових точок входу залишалась обмеженою, тоді як зростання використання цифрових та децентралізованих технологій суттєво розширює поверхню атаки [17]. Водночас саме ця концентрація управління в єдиному диспетчерському центрі є критичним недоліком, бо успішне проникнення до SCADA надає зловмиснику контроль над усією мережею. Інтелектуальна енергомережа містить значно ширшу поверхню атаки внаслідок інтеграції великої кількості IoT-пристроїв, інтелектуальних лічильників (AMI), комунікаційних шлюзів, розподілених джерел енергії (DER) та контролерів мікромереж. Підкреслюється, що кожен компонент комунікаційної мережі є потенційною ціллю для кібератак, при цьому інтеграція протоколів зв'язку з різних рівнів створює додаткові вектори проникнення [18].

Ключова різниця між двома архітектурами полягає не у ширині поверхні атаки, а у топологічних наслідках успішної компрометації та здатності системи

локалізувати відмову. У радіальній централізованій системі мережа має деревоподібну структуру без циклів, тому відмова транзитного вузла негайно ізолює весь підключений підграф. Систематичний огляд каскадних відмов кіберфізичних енергосистем підкреслює, що каскадні відмови є прямим наслідком централізованої операційної парадигми та взаємозалежності компонентів, а децентралізація операцій через розподілені енергоресурси дозволяє досягти локальної самодостатності, суттєво знижуючи ризик каскадного поширення збоїв [13]. Таким чином, дві архітектури демонструють діаметрально протилежні профілі кіберрезильєнтності. Традиційна система має вузьку поверхню атаки, що ускладнює проникнення, однак кожна успішна атака на ключовий вузол автоматично трансформується в каскадне відключення без механізмів автоматичного стримування, а відновлення вимірюється годинами або навіть днями. Smart Grid містить значно ширшу поверхню атаки з більшою кількістю потенційних точок входу, однак компрометація окремого вузла залишається інцидентом локального масштабу. Скомпрометований кластер переходить до острівного режиму від власних DER, суміжні сегменти продовжують функціонувати незалежно, а автоматичне перемикання резервних ліній відновлює зв'язність мережі протягом відносно короткого проміжку часу. Ця асиметрія формулюється як фундаментальна дилема сучасних енергосистем: збільшення кількості цифрових компонентів розширює поверхню атаки, але водночас створює інфраструктуру для реалізації механізмів виявлення, локалізації та автоматичного відновлення [17].

1.5 Вразливості вузлів мережі як вектор реалізації кібератак

Кібератаки на енергосистеми реалізуються через цілеспрямовану технічну експлуатацію задокументованих вразливостей програмного та апаратного забезпечення конкретних мережевих вузлів. Стандартизованим інструментом

ідентифікації таких вразливостей є міжнародна система Common Vulnerabilities and Exposures (CVE). Вона забезпечує єдину систему ідентифікаторів для публічно відомих вразливостей інформаційної безпеки: кожній зареєстрованій вразливості присвоюється унікальний ідентифікатор, що дозволяє однозначно посилатися на неї в технічній документації, координувати зусилля з усунення між різними організаціями та забезпечувати сумісність між різними інструментами безпеки [19]. Для кількісної оцінки тяжкості кожної вразливості використовується Common Vulnerability Scoring System (CVSS) - відкритий фреймворк, який присвоює кожній вразливості числовий показник тяжкості в діапазоні від 0 до 10 на основі трьох груп метрик. На основі метрик обчислюється числова оцінка, яка транслюється у якісну шкалу тяжкості: None (0), Low (0.1–3.9), Medium (4.0–6.9), High (7.0–8.9) та Critical (9.0–10.0) [20]. Для ілюстрації різноманітності вразливостей, релевантних для енергетичних систем, розглянемо три CVE-ідентифікатори, що використовуються у сценаріях кібератак на розподільчу мережу [21]:

- CVE-2020-10937 (CVSS 7.5, High) - вразливість підміни таблиць маршрутизації, що дозволяє ізолювати цільовий вузол від решти мережі [22].
- CVE-2021-40825 (CVSS 8.6, High) - використання незмінюваного криптографічного ключа, що дозволяє зловмиснику з мережевим доступом віддалено надсилати команди контролеру [23].
- CVE-2017-7921 (CVSS 9.8, Critical) - неправильна автентифікація з підвищенням привілеїв, що дозволяє маніпулювати командами до автоматичних вимикачів через SCADA [24].

1.6 Аналіз існуючих методів оцінки та підвищення кіберрезильєнтності, обґрунтування методологічного підходу

Аналіз наукової літератури виявляє кілька методологічних підходів до кількісної оцінки кіберрезильєнтності енергосистем. Попри різноманітність запропонованих рішень, кожне з них характеризується власним балансом переваг і

обмежень, що у сукупності обумовлює необхідність адаптації методології, придатної для порівняльного аналізу двох архітектурних конфігурацій за єдиним критерієм. Інтегральний підхід на основі міри деградації системи зі шкалою від 0 до 1 охоплює три компоненти резильєнтності: здатність поглинати вплив атаки, відновлюватись після неї та уникати повного колапсу [25]. Принциповою перевагою є те, що метод відображає динаміку системи протягом усього інциденту, а не лише кінцевий стан після відновлення, це дозволяє кількісно охарактеризувати, наскільки глибокою була деградація і наскільки швидко система повернулась до нормального рівня.

Підхід на основі “трапеції резильєнтності” систематизує метрики оцінки через трапецію деградації, площа якої відображає сукупні втрати функціональності від початку інциденту до повного відновлення [26]. Концепція є інтуїтивно зрозумілою і придатною для порівняння сценаріїв, оскільки система з меншою площею фігури є резильєнтнішою.

Функціональний підхід оцінює резильєнтність через показники обслуговування споживачів. У систематичному огляді метрик резильєнтності енергосистем виділяють групу показників, що базуються на кількості знеструмлених споживачів, обсязі необслугованого навантаження та тривалості відключення [26]. Цей підхід формалізується через відношення обслугованого критичного навантаження до загального критичного навантаження системи, що приймає значення від 0 до 1 [21]. Показник є практично значущим, безпосередньо вимірюваним і зрозумілим регуляторам та операторам. Однак він фіксує лише поточний стан системи в момент атаки і принципово не враховує структурні параметри мережі, що визначають поведінку цього показника. Принципово важливим є те, що два різних топологічних рішення можуть давати однакове значення показника при одній атаці, але принципово різні значення при інших сценаріях.

Найбільш інтегрованим є топологічний підхід на основі теорії складних мереж [21]. Метод поєднує CVSS-оцінки вразливостей вузлів із параметрами зв'язності графа (алгебраїчна зв'язність, середня найкоротша відстань, середня

центральність за посередництвом, діаметр) та електричним параметром обслуговування критичних навантажень. Атака моделюється як виведення з ладу вузлів або ліній, після чого оцінюється структурна деградація мережі. Механізм перемикання резервних ліній дозволяє врахувати адаптивну реакцію Smart Grid і кількісно відобразити різницю між фазами атаки та відновлення. Принципово важливим є те, що метод не обмежується окремими ізольованими показниками, а реалізує комплексний підхід до порівняння двох архітектур. При цьому слід розмежовувати поняття «метрика» та «міра»: міра є кількісним або якісним засобом запису атрибута конкретної системи, тоді як метрика є засобом для порівняння якості двох або більше систем шляхом застосування міри [27]. Обраний топологічний підхід побудований саме за цим принципом: п'ять окремих мір (алгебраїчна зв'язність, середня найкоротша відстань, середня центральність за посередництвом, діаметр графа та частка обслугованого критичного навантаження) інтегруються в єдину метрику - комплексний показник R , який знаходиться у діапазоні від 0 до 1, що дозволяє порівняти резильєнтність двох архітектурних конфігурацій за єдиною шкалою [21].

Водночас сучасні дослідження виявляють, що ключовим фактором підвищення резильєнтності є не лише структурна надмірність мережі, а й швидкість виявлення аномалії, яка безпосередньо визначає глибину каскадної деградації. Систематичний огляд підходів до підвищення кіберрезильєнтності мікромереж дозволяє виділити кілька основних напрямків.

Перший напрямок пов'язаний із реконфігурацією топології мережі, тобто автоматичним перемиканням резервних ліній та острівним режимом мікрокластерів. Цей підхід забезпечує структурне відновлення зв'язності мережі після виявлення інциденту, проте його ефективність критично залежить від часу виявлення атаки: що пізніше виявлено аномалію, тим глибшою є каскадна деградація на момент початку відновлення [28].

Інший напрямок охоплює централізовані системи виявлення вторгнень (IDS) на основі SCADA, які аналізують потоки телеметрії для ідентифікації аномальних патернів поведінки. Типова затримка виявлення у таких системах складає від

десять секунд до хвилин, що в контексті каскадної деградації енергосистеми може бути критичним. Крім того, централізований підхід до виявлення аномалій успадковує фундаментальну проблему традиційних систем - єдину точку відмови, де компрометація центрального сервера IDS залишає всю мережу без захисту [29].

Найбільш перспективний напрямок передбачає застосування методів машинного навчання для децентралізованого виявлення аномалій безпосередньо на вузлах розподіленої генерації (DER). У цьому контексті федеративне навчання (Federated Learning, FL) виділяється як підхід, що найбільш органічно узгоджується з архітектурою мікрокластерної Smart Grid системи. Федеративне навчання було запропоновано у фундаментальній роботі McMahan та співавторів як децентралізована парадигма машинного навчання, де кілька клієнтів спільно навчають глобальну модель без передачі необроблених даних на центральний сервер [30]. Кожен клієнт обчислює локальні оновлення моделі на основі власних даних і надсилає лише отримані ваги до центрального агрегатора, який обчислює нову глобальну модель за допомогою зваженого усереднення (FedAvg) і розподіляє її назад між клієнтами для наступного раунду навчання. Федеративне навчання є перспективною альтернативою централізованим підходам, що дозволяє вузлам опрацьовувати дані локально та передавати між собою лише параметри моделі. Ключовою перевагою такої парадигми є захист приватності, оскільки вихідні дані залишаються на вузлах, істотно зменшується вірогідність їх несанкціонованого розкриття, перехоплення чи зловживання, і це особливо актуально для інтелектуальних енергетичних мереж, де характер споживання електроенергії може опосередковано відображати чутливу інформацію про поведінку користувачів та режими роботи обладнання. На противагу класичним рішенням із централізованим збором даних, федеративний підхід виключає безпосередній обмін вимірюваннями між учасниками та природно враховує відмінності в умовах роботи окремих вузлів, надаючи кожному з них можливість підлаштовуватися під власне оточення та водночас збагачувати спільну глобальну модель. На практиці кожен вузол самостійно навчає LSTM-модель на локальних часових рядах, а на центральний сервер агрегації надсилаються виключно вагові коефіцієнти, тобто

жодні необроблені телеметричні вимірювання за межі вузла не виходять [31]. Поєднання мікрокластерної архітектури з федеративним навчанням формує модель енергетичної інфраструктури, стійку одночасно до фізичних і кіберзагроз [32].

Висновки до розділу 1

У першому розділі проведено комплексний аналіз концепції кіберрезильєнтності енергетичних мереж та обґрунтовано теоретичну базу для порівняльної оцінки архітектурних конфігурацій. Встановлено, що кіберрезильєнтність є фундаментальною властивістю критичної інфраструктури, яка доповнює традиційну парадигму превентивного захисту здатністю системи поглинати вплив атаки, відновлювати функціональність та адаптуватися до нових загроз.

Аналіз архітектурних особливостей двох типів енергосистем виявив принципово різні профілі кіберрезильєнтності. Традиційна централізована система характеризується вузькою поверхнею атаки, що ускладнює проникнення, проте радіальна деревоподібна топологія та залежність від єдиного диспетчерського центру обумовлюють катастрофічні наслідки успішної компрометації: каскадне відключення без механізмів автоматичної локалізації та відновлення, що вимірюється годинами. Інтелектуальна система Smart Grid на основі мікрокластерної архітектури містить значно ширшу поверхню атаки внаслідок інтеграції IoT-пристроїв, AMI, DER-контролерів та комунікаційних шлюзів. Водночас зазначені інтегровані компоненти забезпечують принципово кращу здатність до локалізації наслідків атаки та автоматичного відновлення зв'язності, скорочуючи час відновлення з годин до секунд.

Систематизовано вразливості вузлів енергосистем за рівнями функціональної ієрархії та описано три CVE-ідентифікатори (CVE-2020-10937, CVE-2021-40825, CVE-2017-7921), що використовуються як основа для моделювання сценаріїв кібератак у подальших розділах роботи.

Проведено порівняльний аналіз методологічних підходів до кількісної оцінки кіберрезильєнтності та її підвищення, обґрунтовано вибір топологічного підходу на основі теорії складних мереж як найбільш відповідного для порівняльного аналізу різних архітектур. Визначено, що федеративне навчання є одним із найбільш перспективних шляхів підвищення кіберрезильєнтності мікромереж, оскільки воно одночасно забезпечує раннє децентралізоване виявлення аномалій, збереження конфіденційності операційних даних та усунення єдиної точки відмови централізованих систем виявлення вторгнень. Обґрунтовано доцільність інтеграції FL-модуля з механізмом перемикання резервних ліній для кількісної оцінки впливу раннього виявлення на інтегральну резильєнтність системи.

2 МЕТОДИКА ПОРІВНЯЛЬНОЇ ОЦІНКИ КІБЕРРЕЗИЛЬЄНТНОСТІ ЕНЕРГЕТИЧНИХ МЕРЕЖ

2.1 Обґрунтування вибору методу оцінки

На основі розглянутих методологічних підходів до кількісної оцінки кіберрезильєнтності енергосистем було зроблено попередній висновок на користь топологічного підходу. Загалом порівняльна оцінка кіберрезильєнтності традиційної та інтелектуальної енергосистем висуває п'ять специфічних вимог до обраного методу:

- Метод має забезпечувати єдиний числовий показник, однаково придатний для обох архітектур - радіальної мережі без резервування та мікрокластерної системи з DER та перемикачами резервних ліній.
- Метод має явно враховувати механізм відновлення зв'язності, оскільки саме ця здатність є визначальною архітектурною перевагою інтелектуальної мережі.
- Необхідна прив'язка до реально задокументованих вразливостей, а не до абстрактних сценаріїв.
- Метод має дозволяти оцінку на етапі моделювання за відсутності реальних даних про атаки. Цю вимогу підкреслює методологія кіберрезильєнтного проєктування мікромереж, що формулює принцип кількісної оцінки резильєнтності саме на етапі проєктування [14].
- Метод має інтегрувати кілька метрик у комплексний показник, оскільки жодна окрема метрика не здатна повноцінно охарактеризувати кіберстійкість складної системи.

Інтегральний підхід на основі міри деградації [25] забезпечує єдиний показник і частково реалізує комплексну оцінку через три компоненти резильєнтності (поглинання, відновлення, уникнення колапсу), однак він не містить явного механізму моделювання перемикання резервних шляхів як

дискретної операції відновлення та не передбачає прив'язки до конкретних CVE-ідентифікаторів. У межах даної роботи інтегральна оцінка реалізується як чисельно-симуляційна функція, що базується на динамічній еволюції показника резильєнтності. Значення показника формується на основі результатів розрахунків поточкорозподілу в електричній мережі, змін топології мережі та сценарно-заданих кібератак, після чого агрегується в інтегральний показник шляхом чисельного інтегрування по часовій осі. Підхід на основі “трапеції резильєнтності” [26] є інтуїтивно зрозумілим і придатним для візуального порівняння сценаріїв, проте залишається теоретичним і не пропонує обчислювального алгоритму для реальних топологій із заданими параметрами вузлів та ліній. Функціональний підхід через показники обслуговування споживачів фіксує лише поточний стан системи в момент атаки і принципово не враховує структурні та динамічні властивості мережі. Виділяються також два принципових класи підходів: модельно-орієнтовані, що базуються на точному моделюванні динаміки мікромережі та дата-орієнтовані, що використовують машинне навчання для виявлення аномалій та адаптивного управління [33]. Обраний топологічний підхід належить до модельно-орієнтованого класу і має перевагу інтерпретованості, бо кожен компонент показника резильєнтності має чіткий фізичний зміст, що дозволяє не лише констатувати різницю в резильєнтності, але й пояснити, які саме структурні фактори її обумовлюють. Водночас дата-орієнтований підхід залучається як доповнення, оскільки LSTM-мережа у складі федеративного навчання аналізує вектори напруги по всіх шинах і виявляє аномалії до того, як деградація досягає критичної глибини. Така комбінація дозволяє поєднати прозорість модельного розрахунку резильєнтності з адаптивністю машинного навчання, а отже модельна складова пояснює що відбувається зі структурою мережі, а дата-орієнтована - коли саме почалося відхилення від норми.

2.2 Система оцінки вразливостей вузлів мережі

Кіберскладова обраної методики базується на системі CVSS [20], основні принципи та структуру якої вже було описано. Вибір саме CVSS не є єдиним можливим рішенням, серед альтернатив слід виділити CWSS (Common Weakness Scoring System), що оцінює не конкретні вразливості, а класи архітектурних слабкостей програмного забезпечення, та EPSS (Exploit Prediction Scoring System), що прогнозує ймовірність реальної експлуатації вразливості протягом наступних 30 днів на основі статистичних моделей. Кожна з цих систем має свої переваги: CWSS дозволяє оцінити вразливість на етапі проектування, коли конкретні CVE ще не відомі, а EPSS враховує реальну активність зловмисників та наявність публічних експлойтів. Проте для цілей моделювання енергосистеми CVSS має принципову перевагу, бо кожна оцінка прив'язана до конкретного CVE-ідентифікатора з описом вразливого обладнання, що дозволяє доцільно присвоїти оцінку конкретному типу вузла мережі. CWSS оперує на рівні абстрактних класів слабкостей без такої прив'язки, а EPSS потребує актуальних даних про активність зловмисників, які швидко застарівають і не забезпечують відтворюваність результатів через кілька місяців після публікації. Крім того, CVSS є де-факто галузевим стандартом, бо саме ця система використовується більшістю виробників промислового обладнання для публікації інформації про вразливості, що забезпечує найширшу базу даних для моделювання.

Базова оцінка CVSSBase обчислюється як результат поєднання двох підоцінок - експлуатації (Exploitability) та впливу (Impact). Для енергосистем найбільш критичною є метрика доступності, оскільки основною метою кібератаки на енергетичну інфраструктуру є саме порушення безперервного електропостачання, а не крадіжка даних чи маніпуляція інформацією.

У контексті моделювання системи кожному вузлу мережі присвоюється CVSS-оцінка відповідно до вразливості обладнання, встановленого на цьому вузлі. Оцінки отримуються з бази CVE через Національну базу вразливостей NVD [19]. Це принципово відрізняє обраний підхід від абстрактного моделювання, де рівні

вразливості задаються довільно або генеруються випадковим чином. Використання реальних CVE-ідентифікаторів забезпечує верифікованість кожного вхідного параметра моделі та його відповідність реальному обладнанню енергосистем. Для порівняльного аналізу буде використовуватися три вразливості із різними оцінками, що дозволить дослідити чутливість показника резильєнтності до різних рівнів тяжкості атаки. Якщо різниця між архітектурами зберігається при всіх трьох рівнях CVSS, це підвищує надійність висновку про архітектурну перевагу певної системи. CVSS оцінює тяжкість вразливості як ізольовану технічну характеристику, тоді як її реальні наслідки для функціонування мережі визначаються ще й топологічним значенням ураженого вузла. Ця асиметрія між технічною оцінкою вразливості та її системним впливом є фундаментальною проблемою, яку не вирішує жодна система оцінки вразливостей окремо. Саме тому обрана методика комбінує CVSS-оцінки з параметрами теорії складних мереж, де перші визначають, які вузли будуть скомпрометовані, другі - які структурні наслідки це спричинить для мережі в цілому [21].

2.3 Параметри топології мережі як кількісні показники резильєнтності

Теорія складних мереж забезпечує математичний апарат для кількісної оцінки структурних властивостей мережі та їх деградації при виведенні з ладу окремих компонентів. Розподільча енергосистема моделюється як неорієнтований граф $G = (N, E)$, де N - множина вузлів (шини, підстанції, точки навантаження), E - множина ребер (лінії електропередачі), а кожне ребро з'єднує вузли i та j ($i, j = 1, 2, \dots, N$). Вибір неорієнтованого графа обумовлений тим, що лінії електропередачі розподільчої мережі забезпечують двосторонню передачу потужності, особливо в умовах наявності DER, коли потоки можуть змінювати напрямок залежно від балансу генерації та споживання. На цьому графі обчислюються чотири топологічні параметри та один електричний, що в сукупності характеризують різні аспекти структурної резильєнтності [21]. Кожен з п'яти параметрів відображає

окрему складову здатності мережі протистояти кібератаці та відновлюватись після неї. Алгебраїчна зв'язність характеризує стійкість до фрагментації, середня найкоротша відстань визначає ефективність передачі, середня центральність за посередництвом - наявність вузьких місць, діаметр - розтягнутість мережі, а критичне навантаження у свою чергу визначає функціональну здатність забезпечувати споживачів.

2.3.1 Алгебраїчна зв'язність

Алгебраїчна зв'язність (λ_2) є мірою глобальної структурної стійкості мережі до фрагментації. Цей параметр визначається як друге за величиною власне значення матриці Лапласа графа $L = D - A$, де D - діагональна матриця ступенів вершин, A - матриця суміжності [34]. Друге власне значення λ_2 є мірою глобальної зв'язності, де для від'єданого графа, що складається з двох або більше ізольованих компонент, $\lambda_2 = 0$, для зв'язного графа $0 < \lambda_2 \leq N$ [20, 33]. Тобто чим вище значення λ_2 , тим стійкішою є мережа до розділення на ізольовані сегменти при видаленні вузлів або ребер. Критичний огляд відмовостійкості енергомереж з позицій теорії складних мереж підтверджує, що алгебраїчна зв'язність є одним з найбільш інформативних параметрів для оцінки структурної резильєнтності, оскільки вона відображає мінімальний бар'єр, який необхідно подолати для фрагментації мережі [35]. Радіальна розподільча мережа за структурою є деревом, що топологічно ближче до шляху, ніж до повного графа, тоді як для дерева значення для λ_2 є мінімальним серед усіх зв'язних графів тієї самої розмірності [35].

Принципово важливою є властивість монотонного зростання λ_2 при додаванні ребер до графа [34], кожна додаткова лінія, зокрема резервні магістральні шляхи, гарантовано підвищує алгебраїчну зв'язність. Це математично обґрунтовує перевагу Smart Grid з перемикачами резервних ліній перед радіальною мережею без резервування, тому що додавання навіть одного резервного ребра перетворює дерево на граф із циклом, що стрибкоподібно підвищує λ_2 . Це пояснює,

чому навіть невелика кількість резервних ліній може суттєво підвищити структурну резильєнтність.

2.3.2 Середня найкоротша відстань

Середня найкоротша відстань (L) характеризує ефективність передачі електроенергії та управляючих сигналів у мережі. Параметр обчислюється як середнє значення мінімальних шляхів між усіма парами вершин графа [36] за формулою:

$$L = \frac{2}{N(N-1)} \sum_{u \neq v} d(u, v)$$

де $d(u, v)$ - мінімальна кількість ребер на шляху між вершинами u та v . Для обчислення найкоротших шляхів використовується алгоритм пошуку в ширину, що є стандартним алгоритмом обходу графа для знаходження найкоротших шляхів у незважених графах [34]. При видаленні вузлів внаслідок кібератаки показник різко зростає, оскільки шляхи подовжуються через відсутність прямих з'єднань, або стає невизначеною при розпаді графа на ізольовані компоненти, у цьому випадку деякі пари вершин стають взаємно недоступними [21].

2.3.3 Середня центральність за посередництвом

Середня центральність за посередництвом кількісно характеризує наявність вузьких місць, інакше кажучи критичних транзитних вузлів, через які проходить непропорційно велика частка потоків у мережі. Показник окремої вершини визначається як частка найкоротших шляхів між усіма парами вершин, що проходять через обрану [35] та обраховується за формулою:

$$C_B(v) = \sum_{s,t \neq v} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

де σ_{st} - загальна кількість найкоротших шляхів між вершинами s та t , а $\sigma_{st}(v)$ - кількість тих шляхів, що проходять через вершину v . У свою чергу високе значення параметра вказує на те, що вершина є критичним транзитним вузлом [36]. Середня центральність обчислюється як середнє арифметичне середніх центральностей для всіх вершин графа [37, 38]:

$$C_{AB} = \frac{1}{n} \sum_{v \in V} C_B(v)$$

Для енергосистеми величина характеризує структурну рівномірність розподілу транзитних потоків. Високе значення означає наявність вузлів, видалення яких спричинить непропорційно велику деградацію зв'язності. У радіальній мережі практично кожен нелистовий вузол має високу центральність за посередництвом, через те що він є єдиним транзитним шляхом для всіх нижчих вузлів, оскільки іншого маршруту просто не існує. Додавання резервних магістралей створює альтернативні шляхи, перерозподіляючи транзитне навантаження між кількома вузлами та знижуючи середню центральність за посередництвом [21].

2.3.4 Діаметр графа

Діаметр графа визначається як максимальна найкоротша відстань між будь-якою парою вершин [39] та обчислюється за формулою:

$$D = \max_{u,v} d(u, v)$$

Якщо середня найкоротша відстань характеризує типову ефективність передачі в мережі, то діаметр характеризує найгірший випадок, а саме максимальну топологічну відстань між найбільш віддаленими вузлами. Для енергосистеми більший діаметр означає, що крайні споживачі знаходяться на значній топологічній відстані від джерел живлення та управляючих центрів, що збільшує час передачі сигналів управління та підвищує вразливість периферійних сегментів. При кібератаці видалення транзитних вузлів збільшує показник, оскільки найкоротші шляхи між деякими парами вершин подовжуються через необхідність обходу скомпрометованого вузла. У свою чергу у граничному випадку при розпаді графа на ізольовані компоненти діаметр стає невизначеним, що відповідає повній втраті зв'язності між деякими частинами мережі [21].

2.3.5 Критичне навантаження

На відміну від чотирьох попередніх параметрів, що є суто топологічними характеристиками графа, критичне навантаження є електричним параметром, що безпосередньо відображає функціональну здатність системи виконувати своє основне призначення - забезпечувати електроенергією критичних споживачів. Параметр визначається як відношення забезпеченого критичного навантаження до загального [40]:

$$E_{CL} = \frac{\text{Забезпечене критичне навантаження}}{\text{Загальне критичне навантаження}}$$

Якщо показник набуває значення, що дорівнює одиниці, це означає повну функціональність системи, коли всі критичні споживачі, зокрема лікарні, дата-центри та системи водопостачання, забезпечені електроенергією, тоді як нуль відповідає повному колапсу. Показник змінюється безперервно в цьому діапазоні та є інтуїтивно зрозумілим для операторів і регуляторів, оскільки безпосередньо відображає частку критичних споживачів, які продовжують отримувати

електропостачання під час інциденту [40]. У такому випадку показник відображає зв'язок між топологічними властивостями мережі та фактичним енергетичним результатом [21].

2.3.6 Комплексний показник резильєнтності R

П'ять попередньо описаних параметрів інтегруються в єдиний комплексний показник, який і є показником резильєнтності системи. Для приведення метрик до єдиної шкали виконується узгодження напрямку їх інтерпретації, де збільшення алгебраїчної зв'язності та критичного навантаження відповідають зростанню резильєнтності, а зростання середньої найкоротшої відстані, середнього арифметичного середніх центральностей для всіх вершин графа та діаметру графа - її зниженню. У зв'язку з цим для останніх показників застосовується інверсивне перетворення, і підсумкове значення обчислюється згідно з формулою [21]:

$$R = \frac{1}{5} (\widehat{\lambda}_2 + \widehat{L}^{-1} + \widehat{C}_{AB}^{-1} + \widehat{D}^{-1} + \widehat{E}_{CL}) \quad (2.1)$$

де $\widehat{\lambda}_2$ – нормалізована алгебраїчна зв'язність графа мережі; $\widehat{L}^{-1}$ - інверсне нормалізоване значення середньої найкоротшої відстані між вузлами; $\widehat{C}_{AB}^{-1}$ - інверсне нормалізоване значення середнього арифметичного центральностей усіх вершин графа; $\widehat{D}^{-1}$ - інверсне нормалізоване значення діаметру графа; $\widehat{E}_{CL}$ - нормалізоване значення частки обслугованого критичного навантаження. Вихідні абсолютні значення цих компонентів не є статичними константами, а обчислюються динамічно на кожному кроці симуляції шляхом прямого перетворення розрахункової електричної моделі середовища pandapower у неорієнтований граф засобами бібліотеки networkx. Найбільш комплексним є обчислення електричного параметра частки обслугованого критичного навантаження, що спирається на результати ітераційного розрахунку

потокорозподілу методом Ньютона-Рафсона із точністю збіжності 10^{-5} МВА. Сама ж нормалізація здійснюється шляхом ділення поточних обчислених абсолютних значень на значення відповідного параметра у стандартному режимі роботи системи, тобто без кібератак, і коли усі перемикачі резервних ліній розімкнені. Таким чином, $R = 1.0$ відповідає нормальному стану системи, а зниження R кількісно відображає деградацію резильєнтності під впливом кібератаки [21]. Формула використовує рівні ваги для всіх п'яти компонентів, тоді як у реальній системі їхня відносна важливість може відрізнятися. Однак для цілей порівняльного аналізу рівні ваги є обґрунтованим вибором, оскільки вони забезпечують нейтральність оцінки відносно конкретних пріоритетів оператора і дозволяють виявити фундаментальні структурні відмінності між архітектурами.

2.4 Перемикання резервних ліній як механізм відновлення системи

Перемикання резервних ліній є ключовим механізмом, що дозволяє кількісно відобразити принципову архітектурну різницю між традиційною та інтелектуальною енергосистемами. Наявність або відсутність цього механізму визначає здатність системи до автоматичного відновлення зв'язності після кібератаки, тобто саме ту властивість, яку дослідження виділяють як один з ключових елементів кіберрезильєнтної операції [35]. Водночас слід враховувати, що перемикання ліній безпосередньо відновлює лише одну з трьох базових функцій енергосистеми - передачу електроенергії, тоді як генерація та розподіл забезпечуються іншими засобами; саме тому його ефект є більшим для Smart Grid, яка завдяки розподіленій генерації переходить в острівний режим, і меншим для традиційної радіальної мережі, позбавленої такого резерву.

У стандартному режимі роботи розподільча мережа функціонує в радіальній конфігурації, тобто перемикачі резервних ліній знаходяться у розімкненому стані, зберігаючи деревоподібну топологію для спрощення управління потоками

потужності та координації релейного захисту [21]. Резервні магістральні шляхи з'єднують різні гілки радіальної мережі, створюючи потенційні альтернативні траєкторії передачі електроенергії, така організація забезпечує можливість живлення критичних навантажень через суміжні мікромережі при відмові основного шляху [9]. В нормальному стані перемикачі не впливають на топологію графа - енергосистема функціонує як дерево, але при виникненні інциденту вони перетворюються з пасивних елементів на активний інструмент відновлення. Наслідки цієї операції для кожного з п'яти параметрів є прогнозованими - алгебраїчна зв'язність підвищується внаслідок монотонності при додаванні ребер [34]; середня найкоротша відстань зменшується, оскільки з'являються альтернативні шляхи між деякими парами вершин; середня центральність знижується за рахунок перерозподілу транзитних потоків між більшою кількістю шляхів; діаметр може суттєво зменшитись, якщо резервний шлях з'єднує дві найвіддаленіші частини мережі; критичне навантаження підвищується, якщо замикання перемикача відновлює живлення ізольованих критичних споживачів через DER суміжного кластера [21].

2.5 Динамічна модель інциденту та інтегральна резильєнтність

Комплексний показник R фіксує стан мережі у конкретний момент часу, проте не описує динаміку переходу між станами протягом інциденту. Для порівняння двох архітектур - традиційної мережі та Smart Grid із федеративним навчанням - необхідна динамічна модель, що відображає еволюцію показника на всьому життєвому циклі інциденту. Концептуальною основою такої моделі є багатофазний фреймворк, який відображає послідовність фаз деградації, перебування у деградованому стані, відновлення та постінцидентної адаптації [41]. Систематичний огляд метрик резильєнтності підтверджує, що інтегральні показники на основі площі під кривою продуктивності є одними з найбільш інформативних для порівняльного аналізу [25, 26]. Адаптація фреймворку до

контексту кібератак на розподільчу мережу реалізується з урахуванням трьох ключових параметрів: моменту початку атаки, тривалістю фізичної деградації та часу детекції, що залежить від архітектури системи. Фаза деградації починається з моменту атаки і завершується протягом кількох секунд, у цей час показник резильєнтності лінійно знижується від нормального стану до мінімуму, що відповідає миттєвому структурному показнику атакованої мережі. У свою чергу лінійна модель деградації є стандартним спрощенням у дослідженнях резильєнтності енергосистем [26, 42].

Після виявлення аномалії ініціюється відновлення, тобто замикання перемикачів резервних ліній, що провокує зростання показника резильєнтності від значення на момент детекції до рівня відновлення. Для традиційної системи механізм автоматичного відновлення відсутній, тому показник залишається на рівні деградації до кінця горизонту. Тривалість перебування системи у деградованому стані вважається одним із найбільш критичних факторів, що визначають ступінь впливу інциденту [42]. Для інтелектуальної системи із федеративним навчанням детекція відбувається суттєво раніше завдяки LSTM-моделям на вузлах розподіленої генерації, що розпізнають аномальні патерни напруги без очікування централізованого опитування [43, 45]. Рання детекція має подвійний ефект: менша глибина провалу показника, оскільки деградація ще не досягла мінімуму, та коротша тривалість деградованого стану.

В аналітичному вимірі коефіцієнт сукупної стійкості на часовому горизонті визначається як інтегральний показник резильєнтності (I), який відповідає нормованій площі під часовою кривою $R(t)$ і чисельно обчислюється методом трапецій дискретно з кроком $\Delta t = 0.1$ с на загальному вікні моніторингу $T = 90$ с за пронумерованою математичною залежністю:

$$I = \frac{1}{T} \int_0^T R(t) dt \approx \frac{\Delta t}{T} \sum_{k=0}^{N-1} \frac{R(t_k) + R(t_{k+1})}{2} \quad (2.2)$$

де $R(t_k)$ - значення комплексного показника резильєнтності у k -й дискретний момент часу; $k = 0, 1, \dots, N$;

Нормування на загальний час T дає значення інтегральної резильєнтності в діапазоні $I \in [0, 1]$, де $I=1$ відповідає ідеальній системі без деградації, а наближення до нуля свідчить про глибоку втрату функціональності. Геометричний зміст цього показника та послідовність фаз інциденту візуалізовано на рисунку 2.1, де заштрихована площа під ідеалізованою кривою відображає розрахований інтеграл.

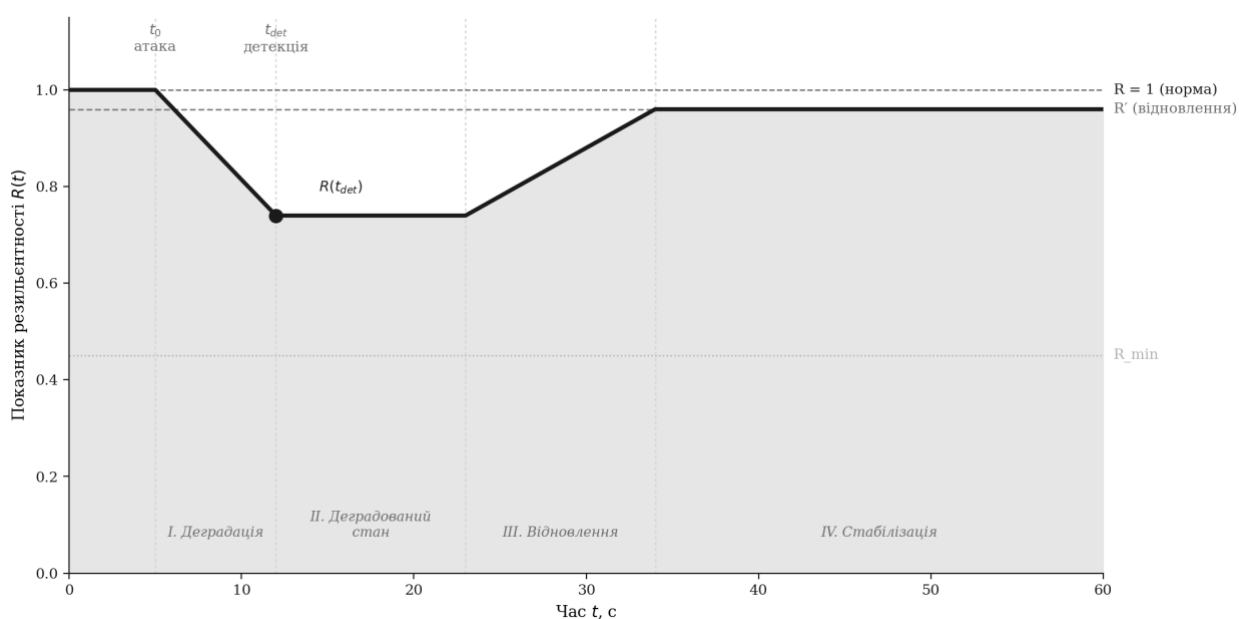


Рисунок 2.1 – Ідеалізована динамічна модель інциденту $R(t)$

Комплексний характер такого підходу дозволяє одночасно враховувати глибину падіння продуктивності, тривалість перебування у деградованому стані та динаміку відновлення, що робить інтегральну резильєнтність високорелевантним інструментом для порівняльного аналізу різних системних архітектур [26, 41]. Окрім статичної переваги, зумовленої острівним ефектом, інтелектуальна мережа здобуває додаткову перевагу в динаміці завдяки федеративному навчанню, яке виконує раннє виявлення аномалій безпосередньо на вузлах розподіленої генерації. Раннє виявлення скорочує тривалість перебування у деградованому стані та зменшує глибину провалу, оскільки перемикання резервних ліній ініціюється до завершення інциденту. Тому раннє виявлення засобами федеративного навчання

слід розглядати як додаткове покращення інтегральної резильєнтності Smart Grid, що накладається на її базову статичну перевагу.

2.6 Федеративне навчання як механізм раннього виявлення аномалій

Система федеративного навчання інтегрується у Smart Grid як децентралізований модуль виявлення аномалій, що доповнює механізм перемикання резервних ліній ранньою детекцією кібератак. Система організована за топологією «зірка» з чотирма клієнтами на вузлах розподіленої генерації та центральним агрегатором. У цій архітектурі кожен клієнт виконує подвійну функцію - генерацію електричної потужності та моніторинг профілів напруги суміжних шин. Доведено, що такий федеративний підхід забезпечує точність детекції на рівні централізованих систем, одночасно гарантуючи конфіденційність даних [43]. Як детектор аномалій використовується двошарова рекурентна мережа на основі архітектури LSTM із класифікаційним шаром. Вибір цієї архітектури обумовлений її доведеною ефективністю для виявлення аномалій у часових рядах енергосистем [44]. Методологія агрегації базується на зваженому алгоритмі FedAvg [30]. У кожному раунді зв'язку t центральний агрегатор обчислює нові глобальні ваги моделі w_{t+1} як зважену суму локальних ваг $w_{k,t}$ отриманих від K клієнтів:

$$w_{t+1} = \sum_{k=1}^K \frac{n_k}{n} \times w_{k,t} \quad (2.3)$$

де n_k - кількість навчальних зразків k -го клієнта, а n - загальна кількість зразків у системі. Це природно враховує різну розмірність вхідних даних через різну кількість шин у зоні спостереження кожного контролера. Архітектуру глобальної агрегації за топологією «зірка» наведено на рисунку 2.2.

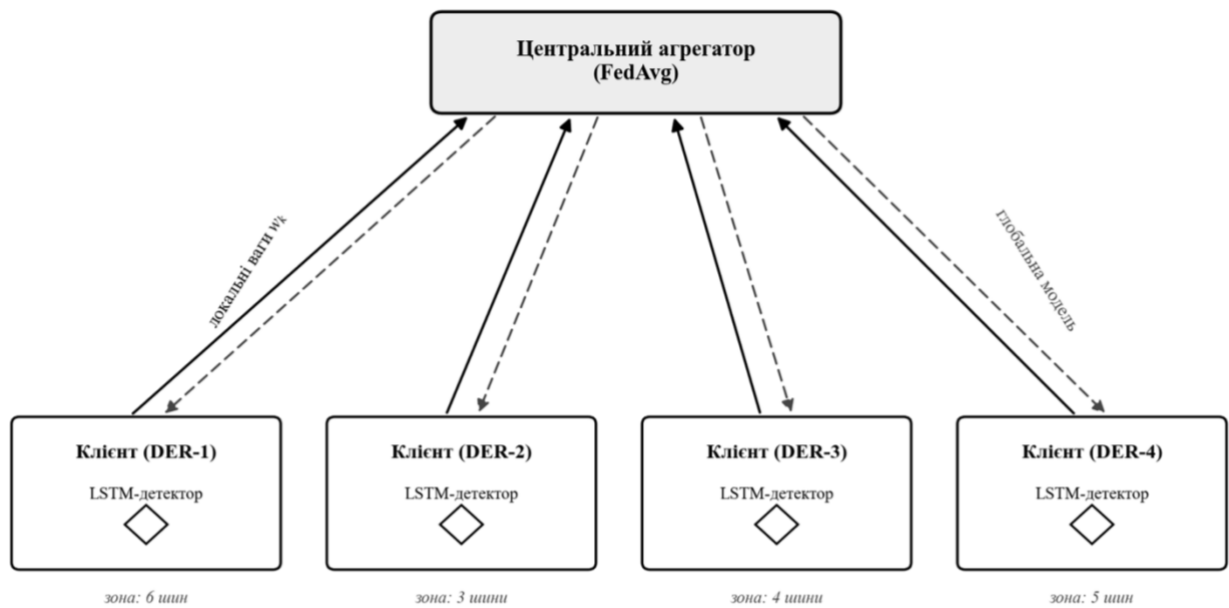


Рисунок 2.2 – Архітектура глобального федеративного навчання (алгоритм FedAvg)

Оскільки перед системою детекції стоїть завдання бінарної класифікації - визначення нормального режиму або кібератаки, як цільова функція втрат (Loss) використовується функція бінарної перехресної ентропії (Binary Cross-Entropy, BCE):

$$L_{BCE} = -\frac{1}{N} \sum_{i=1}^N (y_i \times \log(p_i) + (1 - y_i) \times \log(1 - p_i))$$

де $y_i \in \{0,1\}$ - фактична мітка стану (0 - норма, 1 - атака); N - загальна кількість зразків у навчальному мінібатчі; p_i ймовірність наявності аномалії ($p_i \in [0,1]$), яку передбачила модель для i -го зразка;

Фаза адаптації в рамках циклу кіберрезильєнтності [46] реалізується через донавчання локальних моделей на даних конкретного сценарію після завершення глобального переднавчання, що моделює інкрементальне оновлення після виявленої атаки. Механізм цього процесу із локальною мінімізацією функції L_{BCE} наведено на рисунку 2.3.

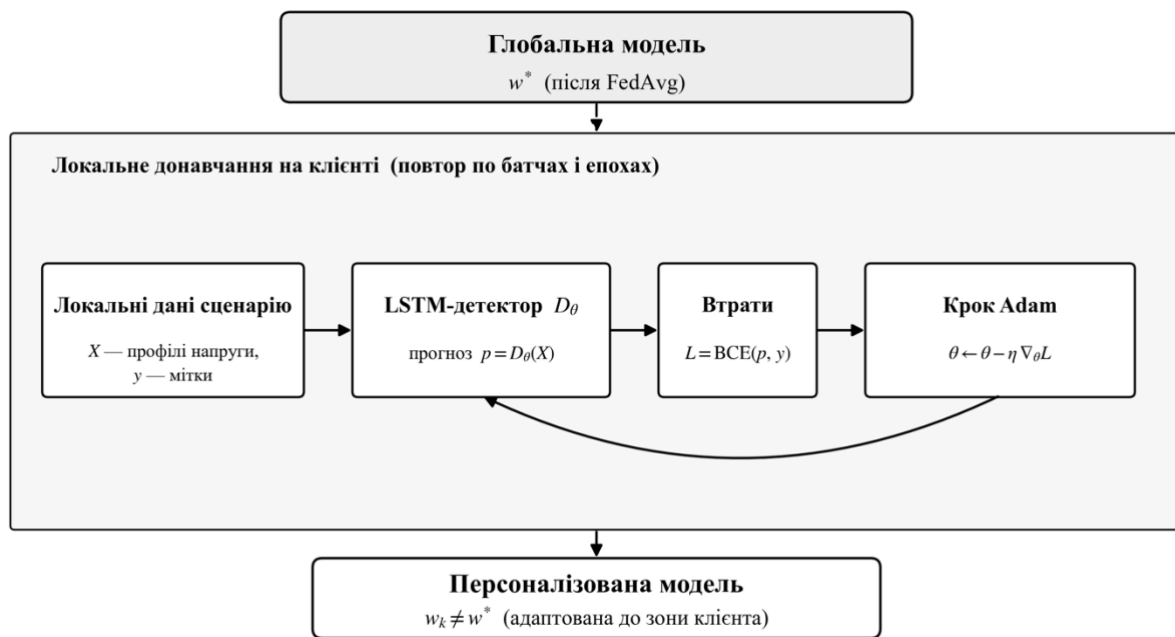


Рисунок 2.3 – Механізм локального персоналізованого донавчання LSTM-детектора

Детекція будується за принципом пріоритетності: основним каналом є LSTM-моделі на вузлах DER, які аналізують профілі напруги у ковзному вікні та підтверджують аномалію після п'яти послідовних спрацювань із кворумом не менше двох клієнтів. Якщо жоден клієнт не підтвердив аномалію протягом максимального вікна спостереження, система повертається до стандартного SCADA-каналу, що гарантує виявлення атаки у будь-якому випадку.

Якість детектора кількісно оцінюється метриками бінарної класифікації, що обчислюються на основі елементів матриці помилок: істинно позитивних (TP), істинно негативних (TN), хибно позитивних (FP) та хибно негативних (FN) спрацювань на валідаційній вибірці [43]. Загальна частка правильних прогнозів моделі оцінюється метрикою Accuracy:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

Оскільки дані про кібератаки в енергосистемах найчастіше є незбалансованими, ключовою метрикою виступає F1-міра - гармонічне середнє між точністю та повнотою [44]:

$$F1 = \frac{2 \times TP}{2 \times TP + FP + FN}$$

Додатково обчислюється метрика AUC, яка інтегрально оцінює здатність LSTM-моделі розрізняти нормальні та аномальні профілі напруги незалежно від обраного порогу класифікації. Математично вона визначається як інтеграл від частки істинно позитивних результатів (TPR) за часткою хибно позитивних результатів (FPR) [43, 44]:

$$TPR = \frac{TP}{TP + FN},$$

$$FPR = \frac{FP}{FP + TN},$$

$$AUC = \int_0^1 TPR d(FPR)$$

Комплексне застосування зазначених метрик дозволяє не лише об'єктивно оцінити точність роботи локальних та глобальної моделей, але й кількісно підтвердити здатність системи федеративного навчання до надійного виявлення кібератак на ранніх стадіях. Саме своєчасна детекція аномалій, верифікована високими значеннями F1-міри та AUC, виступає критичною передумовою для ініціації реконфігурації мережі до моменту досягнення системою максимального провалу резильєнтності.

2.7 Методика комплексної порівняльної оцінки двох архітектур енергомереж

Розроблена методика комплексної порівняльної оцінки базується на наскрізній інтеграції трьох взаємопов'язаних аналітичних моделей та їхньому проектуванні на фізично достовірне тестове середовище. Базовим фундаментом методики є статична модель комплексного показника резильєнтності R , яка кількісно фіксує миттєвий рівень структурної та електричної цілісності мережі. Її доповнює алгоритмічна модель децентралізованої детекції на основі федеративного навчання, завданням якої є визначення критичного часового параметра - швидкості виявлення кібератаки. Зв'язуючою ланкою виступає динамічна фазова модель інциденту $R(t)$, яка синтезує результати перших двох. У даному дослідженні як базовий полігон обрано еталонну розподільчу систему IEEE 33-Bus. Вона є загальноприйнятим стандартом для досліджень кіберрезильєнтності, що забезпечує відтворюваність результатів [34, 36]. Електрично ця система являє собою розподільчу мережу середньої напруги (12.66 кВ), що складається з 33 шин та 32 ліній і живиться від єдиної головної підстанції. Її топологія є репрезентативною для міських мереж: від основної магістралі відходять три бокові гілки з нерівномірним розподілом навантажень. Візуалізацію базової радіальної топології цієї мережі та її модифікації для Smart Grid раніше було наведено на рисунках 1.1 та 1.3 відповідно. Моделювання топології мережі та розрахунок електричних режимів здійснюється ітераційним нелінійним методом Ньютона-Рафсона за допомогою спеціалізованого програмного середовища pandapower, що забезпечує фізичну достовірність профілів напруги [21]. Застосування описаної методики на цій базі дозволяє об'єктивно зіставити дві архітектури розподільчої енергосистеми. Традиційна конфігурація є радіальною мережею без розподілених джерел і засобів детекції. Архітектура Smart Grid розширює її за рахунок розподіленої генерації, перемикачів та забезпечує децентралізоване виявлення інцидентів [43, 45].

Порівняння проводиться на чотирьох сценаріях, побудованих на основі трьох CVE-ідентифікаторів із оцінками від 7.5 до 9.8 за шкалою CVSS [21, 22, 23, 24]: ізоляція вузла, відключення окремих ліній у різних частинах мережі та координована атака з одночасним відключенням двох ліній. Множина сценаріїв забезпечує перевірку стійкості висновків, тому що збереження переваги архітектури при всіх чотирьох сценаріях свідчить про її фундаментальний, а не ситуативний характер [21].

Для кожної пари «архітектура - сценарій» обчислюється комплексний показник резильєнтності та його компоненти для фаз атаки і відновлення, інтегральна резильєнтність обох архітектур та час детекції. Для системи з федеративним навчанням додатково фіксуються метрики якості детектора та ефективність інкрементального донавчання. Усі розрахунки виконуються на тестовій еталонній системі IEEE 33-Bus із бібліотекою pandapower для розрахунку потокорозподілу методом Ньютона-Рафсона, що забезпечує фізичну достовірність профілів напруги [21].

Висновки до розділу 2

Для порівняльної оцінки кіберрезильєнтності двох архітектурних конфігурацій розподільчих енергомереж обрано топологічний підхід на основі теорії складних мереж [21], що задовольняє п'ять необхідних вимог: єдиний числовий показник, явне врахування механізму відновлення, прив'язка до реальних CVE-вразливостей, придатність для етапу моделювання та інтеграція кількох метрик в одну шкалу. П'ять параметрів структурної резильєнтності - алгебраїчна зв'язність, середня найкоротша відстань, середня центральність за посередництвом, діаметр та частка обслугованого критичного навантаження нормуються відносно базового стану мережі та інтегруються у комплексний показник резильєнтності, який набуває значення від нуля до одиниці з рівними вагами [21, 34–40]. Кожен параметр відображає окрему складову кіберрезильєнтності: стійкість до

фрагментації, ефективність передачі, наявність вузьких місць, розтягнутість та функціональну здатність забезпечувати критичних споживачів.

Динамічна модель інциденту описує еволюцію показника резильєнтності через чотири послідовні фази: лінійну деградацію від нормального стану до мінімуму [26, 42], перебування у деградованому стані до моменту детекції, лінійне відновлення після замикання резервних ліній та стабілізацію до кінця горизонту моделювання [41, 46]. Інтегральна резильєнтність, обчислена методом трапецій як нормована площа під кривою $R(t)$, одночасно враховує глибину провалу, тривалість деградованого стану та динаміку відновлення, що робить її основним критерієм порівняння архітектур [25, 26, 41].

Система федеративного навчання організована за топологією «зірка» з чотирма клієнтами на вузлах DER та центральним агрегатором. Кожен клієнт обробляє профілі напруги сусідніх шин у радіусі двох стрибків і навчає двошарову LSTM для виявлення аномалій; агрегація глобальної моделі виконується за зваженим алгоритмом FedAvg [30]. Рання детекція скорочує тривалість деградованого стану та зменшує глибину провалу завдяки ініціації відновлення до досягнення системою мінімального рівня резильєнтності.

Метод порівняльної оцінки охоплює чотири сценарії кібератак на основі трьох CVE-ідентифікаторів із оцінками CVSS від 7.5 до 9.8 [21–24] і забезпечує верифікацію висновків через збереження архітектурної переваги при всіх сценаріях. Розрахунки виконуються на еталонній системі IEEE 33-Bus із бібліотекою pandapower для отримання фізично достовірних профілів напруги методом Ньютона-Рафсона [21].

3 РЕАЛІЗАЦІЯ ІНСТРУМЕНТУ ПОРІВНЯЛЬНОЇ ОЦІНКИ КІБЕРРЕЗИЛЬЄНТНОСТІ

3.1 Моделювання топологій та тестове середовище

Порівняння двох архітектур ґрунтується на спільній основі: обидві системи розгортаються на ідентичній тестовій мережі IEEE 33-Bus, мають однакові задані навантаження та оцінюються за тим самим комплексним показником резильєнтності. Програмний інструмент дає змогу представляти цю спільну електричну основу у двох конфігураціях: традиційній радіальній мережі та Smart Grid. Тому порівняння стосується не різних за потужністю об'єктів, а різних архітектур керування і відновлення для одного й того самого енергетичного полігона.

Розроблену у розділі 2 методику реалізовано у вигляді програмного інструмента мовою Python 3, що поєднує чотири спеціалізовані бібліотеки. Для розрахунку поточкорозподілу ітераційним методом Ньютона-Рафсона із точністю збіжності 10^{-5} МВА використовується бібліотека `pandapower`, яка водночас надає доступ до колекції еталонних мереж [21]. Топологічні метрики обчислюються бібліотекою `networkx` через оптимізовані реалізації алгоритмів пошуку в ширину та спектрального розкладу матриць [34]. Машинне навчання побудовано засобами `PyTorch`, а метрики класифікації отримано через `scikit-learn`. Сумісне застосування цих бібліотек забезпечує наскрізний конвеєр від електричного моделювання до оцінки якості машинного навчання без проміжних ручних перетворень. На цій базі програмний пакет формує дві конфігурації однієї мережі. Традиційна конфігурація зберігає радіальну структуру без DER та автоматичного перемикавання, тому при розриві лінії очікує ручного втручання диспетчера. Smart Grid доповнює ту саму електричну основу розподіленою генерацією, нормально розміжненими резервними лініями та модулем децентралізованого виявлення аномалій. Після атаки для обох конфігурацій виконується розрахунок поточкорозподілу, тому

електричний результат порівнюється фізично однаково, а не лише топологічно. Різниця проявляється у тому, що Smart Grid спочатку може підтримати локальні сегменти в острівному режимі, а далі відновити функцію передачі електроенергії через замикання резервних ліній. Саме через це криві резильєнтності двох архітектур мають різну форму навіть за однакового сценарію атаки.

Генератори розміщено з метою максимального покриття всіх чотирьох зон мережі та забезпечення острівного режиму при різних типах атак. Чотири джерела (0.72–0.80 МВт) розміщено по одному в кожній топологічній зоні, тож кожне здатне жити свій сегмент в острівному режимі. Усі генератори моделюються як статичні джерела з одиничним коефіцієнтом потужності, що є стандартним наближенням для фотоелектричних інверторних систем [10, 11].

Резервні лінії спроектовано так, щоб кожна компенсувала характерний тип розриву, причому вибір пар шин відповідає стандартним конфігураціям для IEEE 33-Bus [21, 36]. Кожен із чотирьох перемикачів (SW1–SW4) компенсує характерний тип розриву, відкриваючи альтернативний маршрут живлення. Електричні параметри всіх ліній уніфіковані, тому вони мають довжину 1 км, опір по 0.3 Ом/км та допустимий струм 1 кА. Критичні навантаження моделюють споживачів першої категорії, перебої живлення яких є неприпустимими, і розподілені між трьома зонами мережі. Сумарна потужність критичних навантажень - 1.89 МВт, з яких близько 75 % припадає на CL-3 у верхній лівій гілці. Чотири сценарії кібератак, описані у підрозділах 1.5 та 2.7, реалізовано як набір конфігурацій із зазначенням типу атаки, цільових елементів та перемикачів відновлення (таблиця 3.1). Сценарії упорядковано за зростанням складності від ізоляції одного периферійного вузла до координованої атаки з одночасним відключенням двох ліній.

Таблиця 3.1 – CVE-вразливості та сценарії кібератак

CVE	CVSS	Тяжкість	Ціль	Перемикач
CVE-2020-10937	7.5	High	Вузол 30	SW3
CVE-2021-40825	8.6	High	Лінія 6–7	SW2
CVE-2021-40825	8.6	High	Лінія 11–12	SW1
CVE-2017-7921	9.8	Critical	Лінії 3-23 та 5-6	SW1, SW4

Перший сценарій - CVE-2020-10937, моделює ізоляцію вузла 30, розташованого у верхній правій гілці між генератором DER-4 на шині 29 та критичним навантаженням CL-4 на шині 31 [22]. Оскільки вузол 30 є єдиним мостом між ними, його ізоляція розриває зв'язок, залишаючи обох у окремих сегментах верхньої правої гілки, проте магістраль та інші гілки залишаються неушкодженими. На верхній частині рисунка 3.1 показник знижується до рівня 0.524, однакового для обох архітектур через периферійне розташування вузла. На нижній частині відображено замикання SW3 (шини 18-33), яке створює альтернативний шлях від кінця магістралі через DER-2 до верхньої правої гілки, піднімаючи показник до 0.585 із приростом +0.061, скромність якого зумовлена тим, що перемикач обходить ізольований вузол, а не повертає його.

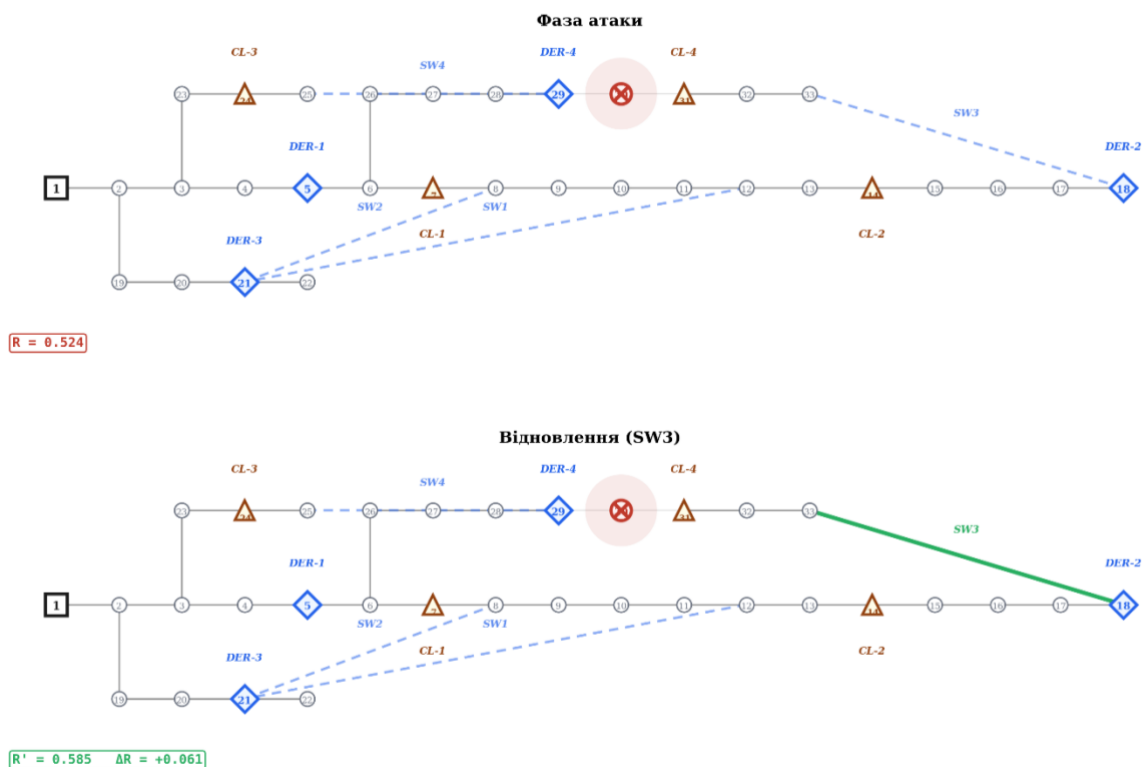


Рисунок 3.1 – Сценарій 1: ізоляція вузла 30

Другий сценарій - CVE-2021-40825 відтворює відключення лінії 6-7 біля точки відгалуження верхньої правої гілки [23]. Розрив ділить мережу на дві великі частини, де ліва зберігає підстанцію, DER-1, нижню та верхню ліву гілки з найбільшим навантаженням CL-3 (1.42 МВт), а права втрачає зв'язок з підстанцією, однак містить DER-2, який переходить в острівний режим і підтримує живлення шин 7-18 з CL-1 та CL-2. На рисунку 3.2 у фазі атаки показник резильєнтності для інтелектуальної мережі складає 0.701, тоді як для традиційної мережі за таких умов він становить 0.667, причому різниця в 0.034 виникає саме завдяки DER-2, без якого правий сегмент повністю знеструмлюється. Замикання SW2 з'єднує правий сегмент із підстанцією через нижню гілку, відновлюючи повноцінне живлення з приростом +0.160.

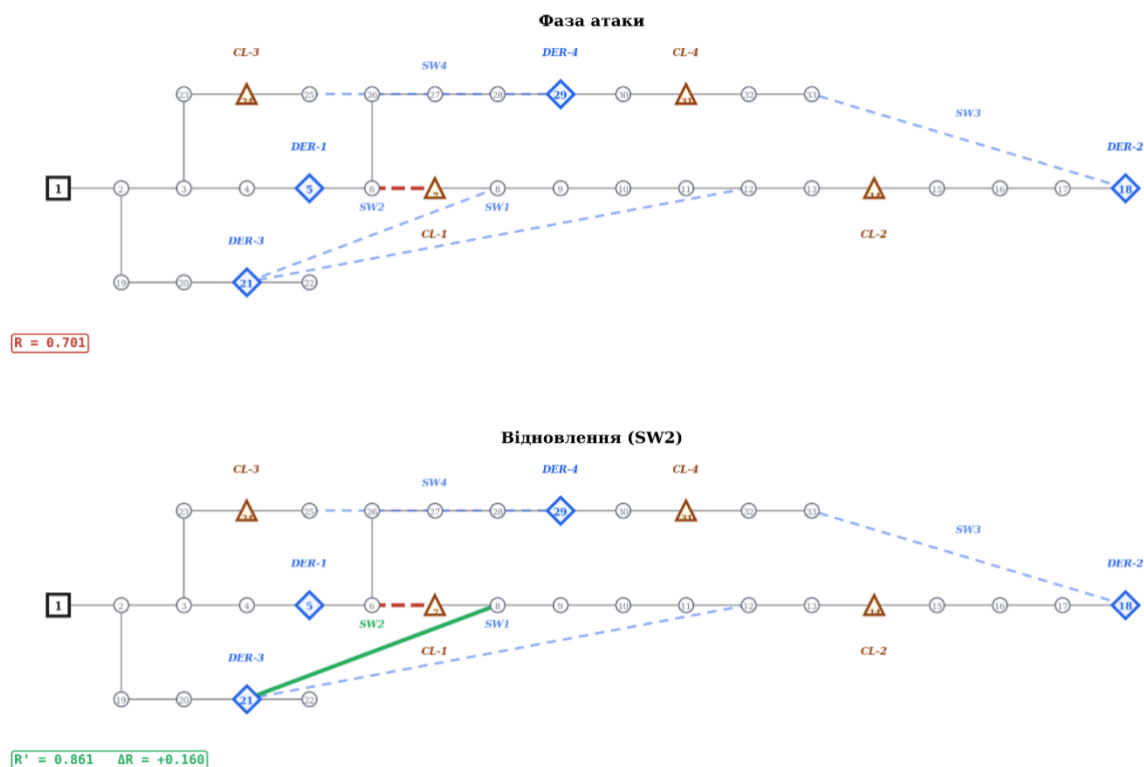


Рисунок 3.2 – Сценарій 2: відключення лінії 6-7

Третій сценарій - CVE-2021-40825, використовує ту саму вразливість для відключення лінії 11-12, проте наслідки суттєво відрізняються через інше розташування розриву. Ізольований сегмент шин 12-18 містить DER-2 та CL-2, тоді як ліва частина магістралі з усіма трьома гілками залишається неушкодженою. На рисунку 3.3 замикання SW1 формує принципово новий маршрут від ізольованого сегмента через нижню гілку з DER-3 назад до підстанції, причому цей маршрут виявляється коротшим за вихідний. Саме тому приріст $+0.335$ удвічі перевищує другий сценарій, а рівень відновлення 0.974 є найвищим серед одиночних атак і свідчить про практично повну компенсацію наслідків.

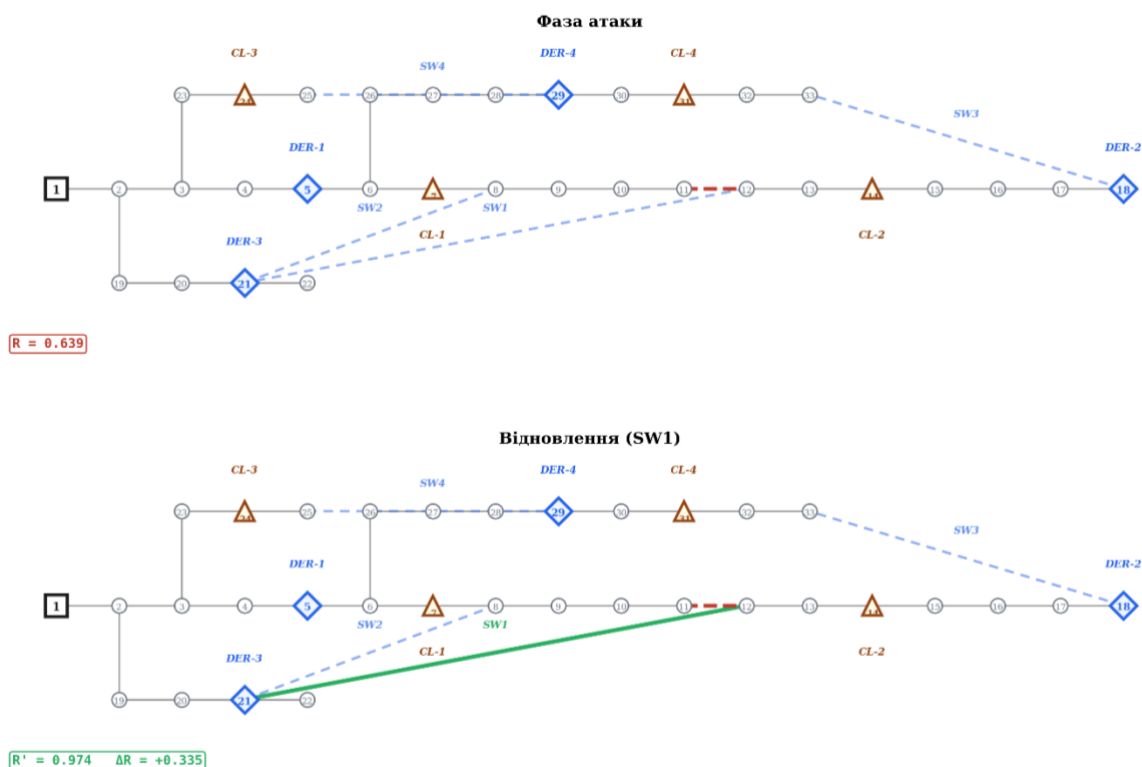


Рисунок 3.3 – Сценарій 3: відключення лінії 11–12

Четвертий сценарій - CVE-2017-7921, моделює координовану атаку з одночасним відключенням ліній 3-23 та 5-6 [23]. Перша лінія з'єднує магістраль з верхньою лівою гілкою, де розташоване найбільше навантаження CL-3, друга розриває магістраль між DER-1 та рештою мережі. Мережа фрагментується на три ізольовані компоненти, де лівий сегмент із підстанцією зберігає лише шини 1-5 з DER-1, а центральний та правий сегменти з трьома гілками втрачають живлення від підстанції, хоча DER-4 у верхній правій гілці та DER-3 у нижній підтримують локальну напругу в острівному режимі. На рисунку 3.4 у верхній частині показник падає до 0.430, абсолютного мінімуму серед усіх сценаріїв. У нижній частині одночасне замикання SW1 та SW4 відновлює зв'язність із рекордним приростом +0.492 до 0.922, що підтверджує ефективність топології з кількома резервними лініями навіть при координованих атаках критичного рівня.

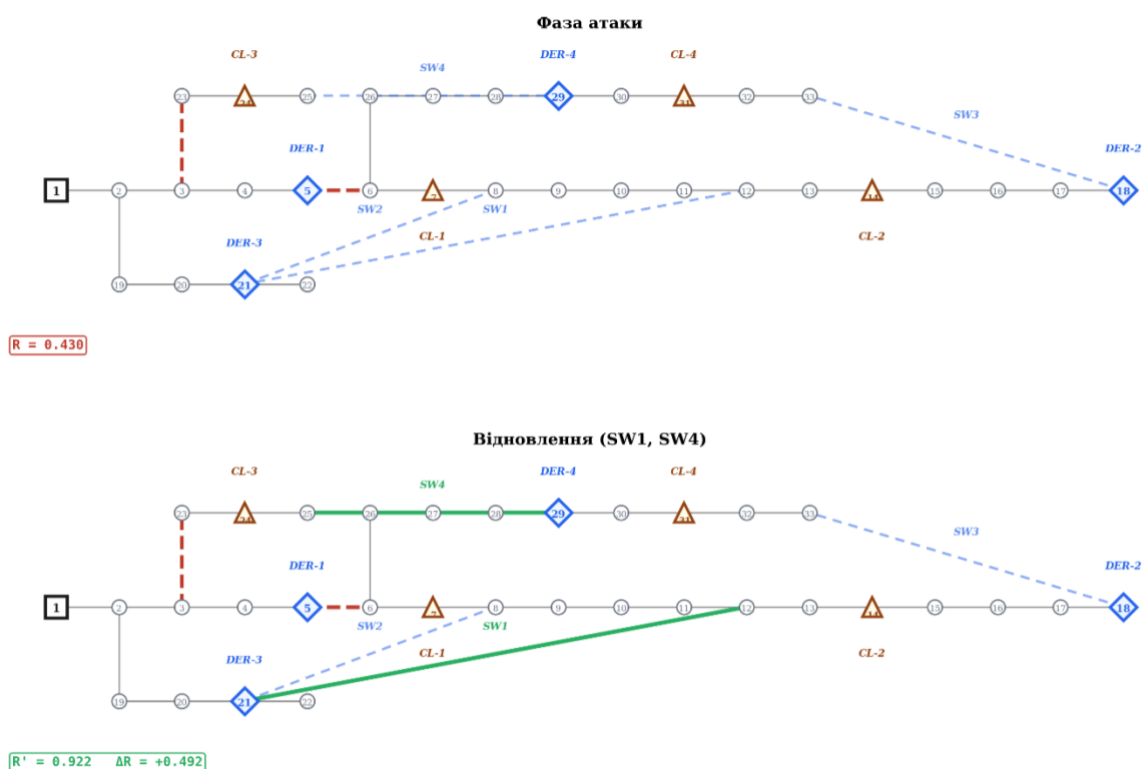


Рисунок 3.4 – Сценарій 4: координована атака

Моделювання атак реалізовано через механізм глибокого копіювання мережі, що гарантує незалежність кожного розрахунку від попередніх. При атаці на вузол деактивуються всі інцидентні лінії, навантаження та генератори ураженої шини, при атаці на лінію деактивується лише зазначена ділянка, а відновлення полягає в активації відповідних перемикачів.

3.2 Реалізація комплексного показника резильєнтності та динамічної моделі інциденту

П'ять структурних параметрів, математичну модель яких описано у підрозділі 2.3, реалізовано як набір функцій, кожна з яких приймає граф мережі та повертає скалярне значення. Перетворення електричної моделі pandapower у граф networkx виконується автоматично із включенням лише активних ліній, тому будь-яка зміна стану мережі, зокрема відключення лінії при атаці або активація

перемикача при відновленні, негайно відображається у топологічних метриках без додаткових ручних перетворень.

Алгебраїчна зв'язність обчислюється через формування матриці Лапласа засобами `networkx` з подальшим спектральним розкладом через `numpy`, де для незв'язних графів повертається нуль. Середня найкоротша відстань визначається пошуком у ширину для кожного вузла, причому для пар без шляху після фрагментації відстань приймається рівною кількості вузлів, що суттєво штрафує розділені мережі. Центральність за посередництвом обчислюється через `networkx`, а при поділі мережі на кілька компонентів додатково застосовується штрафний множник, зворотний кількості компонентів. Діаметр для незв'язних графів приймається рівним 33. Частка обслугованого критичного навантаження є єдиним параметром, що безпосередньо спирається на результати поточкорозподілу, а не лише на топологію. Для кожного сценарію розрахунок потоків електроенергії виконується окремо для традиційної конфігурації та для Smart Grid. У традиційній мережі навантаження вважається обслугованим лише за наявності допустимого електричного режиму та зв'язку з головною підстанцією. У Smart Grid додатково враховується острівний режим: якщо ізольований компонент містить DER і зберігає локальний баланс потужності, критичне навантаження цього сегмента може залишатися обслугованим навіть без зв'язку з головною підстанцією [10, 11]. Саме ця відмінність пояснює статичну перевагу Smart Grid у показнику E_{CL} до замикання резервних ліній.

Агрегація п'яти нормованих компонентів у комплексний показник виконується як середнє арифметичне з рівними вагами та обмеженням зверху одиницею [21]. Для кожної пари «архітектура - сценарій» послідовно обчислюються параметри базового стану, стану після атаки та стану після замикання перемикачів. У традиційній мережі стан після автоматичного перемикання не формується, оскільки відповідний механізм відсутній. Отримані статичні значення R не подаються як проміжний результат у цьому підрозділі, а передаються до підсумкового аналізу наприкінці розділу, де зіставляються з часами

раннього виявлення, метриками федеративного навчання та інтегральною резильєнтністю.

Часова частина моделі реалізована як обчислювальний генератор дискретизованої кривої $R(t)$ з кроком 0.1 секунди на загальному горизонті 90 секунд. Вона не вводить нову формулу резильєнтності, а використовує вже обчислені значення R для нормального, атакованого та відновленого станів. Для кожного сценарію програма задає момент початку атаки, тривалість деградованого режиму, час виявлення та час перемикавання резервних ліній. Завдання цієї частини полягає у тому, щоб показати, як однакові статичні розрахунки перетворюються на різні криві резильєнтності для традиційної мережі та Smart Grid із федеративним навчанням.

Для оцінки тривалості деградованого режиму програма аналізує зміни зв'язних компонентів графа після атаки. Якщо у Smart Grid ізольований сегмент містить джерело розподіленої генерації, у моделі враховується підтримка живлення в острівному режимі, що зменшує швидкість падіння показника та дає системі детекції додатковий час на реакцію. Це розглядається не як окремий алгоритм каскадної деградації, а як технічне доповнення до часової моделі інциденту, потрібне для побудови $R(t)$ на основі вже визначеного показника R .

Час виявлення для централізованого моніторингу складається з трьох послідовних етапів. Перший - циклічне опитування віддалених терміналів з інтервалом 4 секунди відповідно до протоколу IEC 60870-5-104 [48], другий - оцінка стану мережі тривалістю 3 секунди, що включає збір телеметрії та перевірку відповідності моделі, третій - верифікація оператором, тривалість якої варіюється від 5 до 30 секунд згідно зі стандартом NERC CIP [48] і залежить від помітності аномалії. Для традиційної мережі загальний час виявлення становить 15.5-21.6 секунди, тоді як Smart Grid із федеративним навчанням виявляє атаку за 8.8-11.5 секунди. Якщо виявлення відбувається до досягнення найнижчого рівня R , падіння кривої зупиняється на проміжному значенні, після чого ініціюється перемикавання резервних ліній. Для одного перемикача час відновлення прийнято 11 секунд, для двох - 14 секунд, що враховує реконфігурацію системи управління розподілом та

замикання моторизованих роз'єднувачів [16]. Для традиційної мережі автоматичне відновлення відсутнє, тому її крива залишається на мінімальному рівні до кінця горизонту.

Інтегральна резильєнтність обчислюється як нормована площа під кривою методом трапецій [25, 26, 41] і одночасно чутлива до глибини провалу, тривалості деградованого стану та швидкості відновлення. Підсумкові криві $R(t)$ та їхні інтеграли винесено до підрозділу 3.5, де вони розглядаються разом із таблицями статичного R і метриками федеративного детектора.

3.3 Реалізація системи федеративного навчання як механізму раннього виявлення атак

Часова модель інциденту, додана до реалізації показника у підрозділі 3.2, показує, що вирішальним чинником, який визначає і глибину провалу показника резильєнтності, і тривалість деградованого стану, є час виявлення атаки. Саме раннє виявлення відрізняє архітектуру Smart Grid із федеративним навчанням від інтелектуальної мережі з централізованим моніторингом: чим швидше виявлено аномалію, тим раніше ініціюється замикання резервних ліній і тим більшою зберігається нормована площа під кривою $R(t)$. Тому окремий модуль федеративного навчання виконує роль механізму раннього виявлення кібератак безпосередньо на вузлах розподіленої генерації. Архітектуру федеративної системи, математичний апарат якої формалізовано у підрозділі 2.6, програмно реалізовано як клас, що інкапсулює повний цикл розподіленого навчання від ініціалізації клієнтів до оцінки якості. Зона спостереження кожного клієнта визначається алгоритмом пошуку в ширину (BFS) з обмеженням у два стрибки від вузла генератора. Внаслідок цього, наприклад, DER-2 на кінці магістралі спостерігає лише 3 шини, а DER-1 поблизу трьох відгалужень - до 7, що природно створює гетерогенність локальних даних [43, 47].

Детектор аномалій являє собою рекурентну нейронну мережу типу LSTM. Вона складається з двох послідовних рекурентних шарів по 24 нейрони кожен та класифікатора з двома повнозв'язними шарами [44]. Навчальні дані формуються на основі результатів розрахунку поточкорозподілу. Спочатку обчислюються профілі напруги для нормального та атакованого станів; різниця між ними визначає амплітуду аномалії для кожної шини. Далі для нормального класу генеруються часові ряди з авторегресійним шумом першого порядку. Параметри шуму відповідають точності вимірювань PMU [49]. Глобальне переднавчання охоплює 10 раундів з двома локальними епохами у кожному. Клієнти навчаються на суміші всіх сценаріїв, щоб модель розпізнавала загальні патерни, а не конкретні профілі. Процес локального навчання виконується на мінібатчах по 64 зразки, кількість зразків кожного клієнта пропорційна його зоні спостереження, що забезпечує коректну зважену агрегацію за алгоритмом FedAvg [30].

На рисунку 3.5 безпосередньо розраховується та візуалізується динаміка оптимізації математичних параметрів моделі, закладених у підрозділі 2.6. На лівій панелі по осі ординат («Втрати») рахується значення цільової функції бінарної перехресної ентропії (LBCE), яка відображає кількісну похибку класифікатора. Як видно з графіка, алгоритм FedAvg успішно мінімізує цю похибку з початкового рівня 0.69 до 0.15 за десять раундів [30]. На правій панелі паралельно розраховується еволюція метрик якості: Accuracy, F1 та AUC. Синхронне зростання цих показників до рівня 0.94–0.97 математично підтверджує, що глобальна модель успішно навчається розрізняти нормальні та аномальні профілі напруги [43, 44], досягаючи якості, порівнянної з централізованим навчанням.

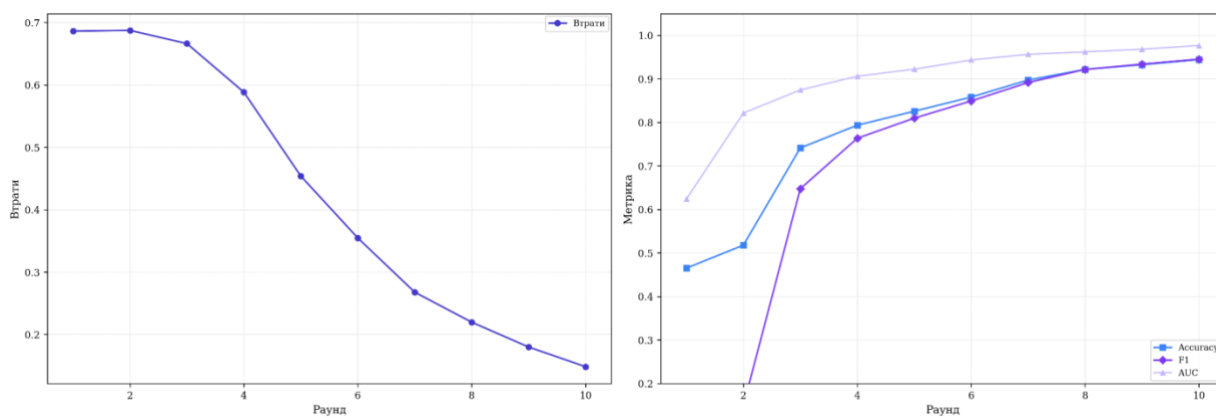


Рисунок 3.5 – Збіжність глобальної моделі

Глобальна модель, навчена на суміші всіх сценаріїв, неминуче є компромісною, оскільки вона усереднює патерни чотирьох різних атак і не може однаково добре розпізнавати кожну з них. Тому після глобального передавання виконується етап персоналізації, який адаптує модель кожного клієнта до конкретного типу загрози. Це дозволяє моделі швидко перебудуватися під новий локальний розподіл, не втрачаючи при цьому загальних знань, здобутих на глобальному етапі [46].

Ефект персоналізації наочно демонструє рисунок 3.6. До донавчання глобальна модель показує різку нерівномірність між клієнтами: ті контролери, що розташовані безпосередньо біля місця розриву, вже мають метрику F1 близько 1.0, оскільки аномалія напруги в їхній зоні є очевидною. Водночас віддалені клієнти починають з F1 від 0.00 до 0.34, бо відхилення напруги на відстані кількох стрибків згасає до рівня фоновому шуму. Після донавчання навіть віддалені клієнти покращують свій показник F1 до 0.57–0.92. Це свідчить про те, що персоналізована модель навчається розпізнавати не лише пряме падіння напруги, а й непрямі ознаки атаки, зокрема зміну кореляційної структури між сусідніми шинами та перерозподіл потоків потужності.

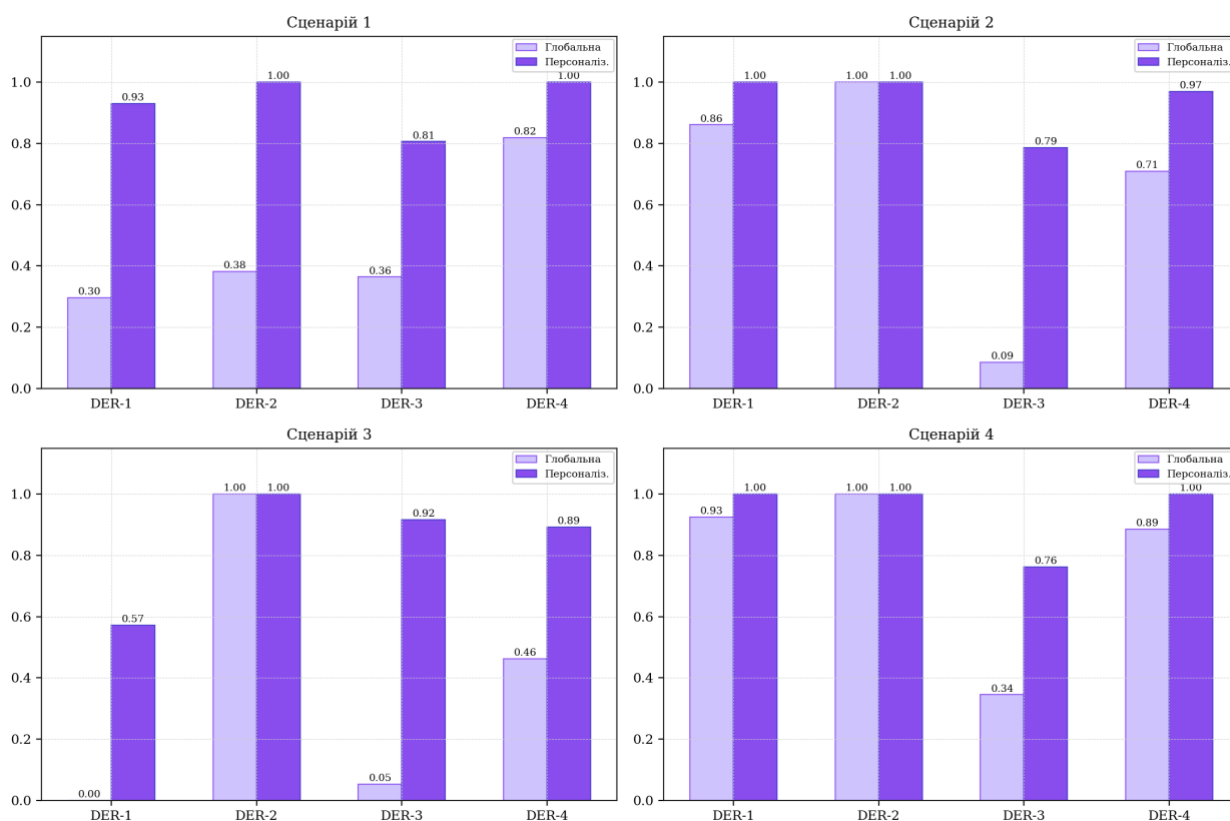


Рисунок 3.6 – F1-міра глобальної та персоналізованої моделей

3.4 Реалізація багаторівневої логіки детекції та прийняття рішень

Модуль федеративної детекції відтворює виявлення атаки у реальному часі на трьох рівнях, описаних у підрозділі 2.6, де кожен рівень визначається набором часових констант. На рівні локального спостереження кожен клієнт аналізує потік вимірювань через ковзне вікно з 20 відліків з інтервалом 0.3 секунди, на кожному кроці модель обробляє вікно за 0.05 секунди та повертає ймовірність аномалії.

На рівні підтвердження атака фіксується після 5 послідовних спрацювань без переривання, цей поріг - компроміс між швидкістю та кількістю хибних тривог. Мінімальний теоретичний час для ідеального детектора, що підтверджує аномалію на перших п'яти кроках, складає приблизно 9.1 секунди.

3.5 Результати експерименту та аналіз

Підсумковий аналіз подано після реалізації двох частин порівняння: статичного розрахунку показника R та динамічної моделі, у якій враховано час виявлення атаки. У таблиці 3.2 зведено миттєві значення R для традиційної мережі, Smart Grid у стані після атаки та Smart Grid після перемикання резервних ліній. Окремо наведено час детекції для централізованого моніторингу SCADA та для федеративного детектора, оскільки саме цей час визначає, наскільки довго система залишається у деградованому стані.

Таблиця 3.2 – Статичний показник резильєнтності та часи детекції

Сценарій	$R(\text{трад.})$	$R(\text{SG, атака})$	$R'(\text{SG})$	ΔR	$t_{FL}, \text{ c}$
Сценарій 1	0.524	0.524	0.585	+0.061	11.5
Сценарій 2	0.667	0.701	0.861	+0.160	11.2
Сценарій 3	0.626	0.639	0.974	+0.335	10.0
Сценарій 4	0.380	0.430	0.922	+0.492	8.8

З таблиці 3.2 видно, що Smart Grid не отримує однакою перевагу в усіх сценаріях одразу після атаки: у першому випадку значення R збігаються, а в інших сценаріях початковий виграш формується за рахунок підтримки частини навантажень розподіленою генерацією в острівному режимі. Основний статичний ефект з'являється після замикання резервних ліній: приріст ΔR зростає від +0.061 у периферійному сценарії до +0.492 за координованої атаки. Ті самі значення візуально порівняно на рисунку 3.7.

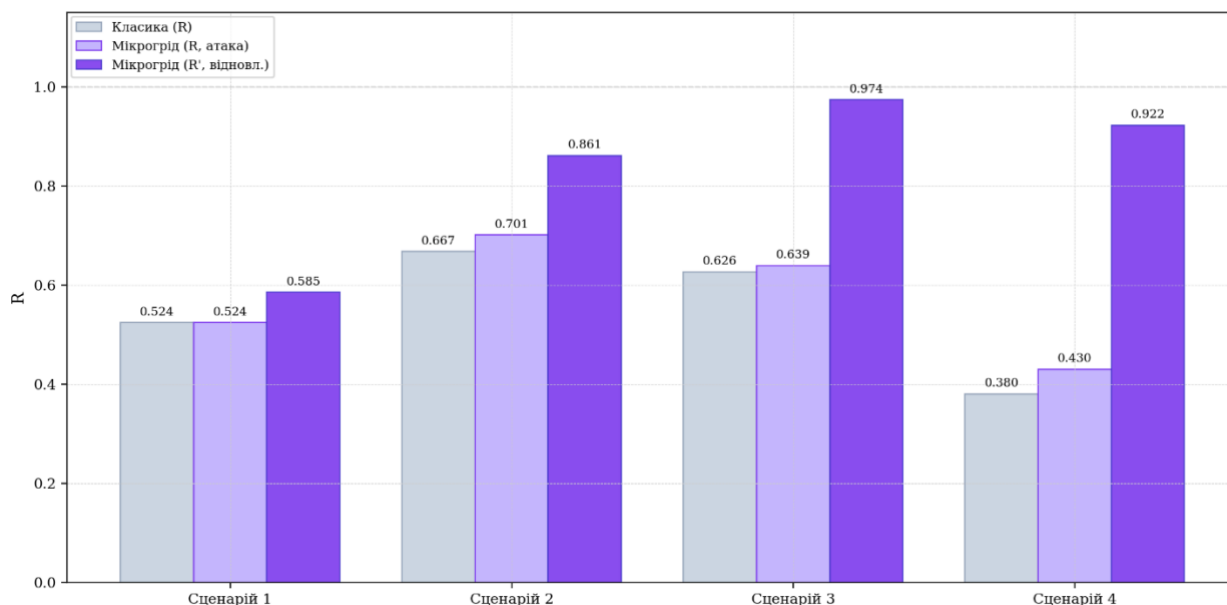


Рисунок 3.7 – Порівняння миттєвого топологічного показника R для двох архітектур та чотирьох сценаріїв

Рисунок 3.7 підкреслює, що перемикання ліній є головним засобом відновлення функції передачі електроенергії у Smart Grid. Чим складніший сценарій і чим більше фрагментується мережа, тим більшим стає ефект реконфігурації. Водночас миттєвий показник R не показує тривалість провалу, тому для оцінки повної поведінки системи потрібна інтегральна резильєнтність, наведена в таблиці 3.3.

Таблиця 3.3 – Інтегральна резильєнтність та якість федеративного детектора

Сценарій	I(трад.)	I(SG+FL)	F1(глоб.)	F1(персон.)
Сценарій 1	0.564	0.689	0.465	0.934
Сценарій 2	0.681	0.857	0.664	0.939
Сценарій 3	0.642	0.917	0.379	0.845
Сценарій 4	0.432	0.926	0.789	0.940

Таблиця 3.3 доповнює статичні результати часовим виміром. У всіх сценаріях інтегральна резильєнтність Smart Grid із федеративним навчанням є вищою, оскільки раннє виявлення скорочує час перебування мережі у деградованому стані

та раніше запускає перемикання ліній. Метрики F1 також показують, що персоналізоване локальне донавчання робить детектор стабільнішим для різних зон спостереження: після персоналізації F1 перебуває в діапазоні 0.845-0.940. Форму відповідних кривих $R(t)$ для кожного сценарію наведено на рисунку 3.8.

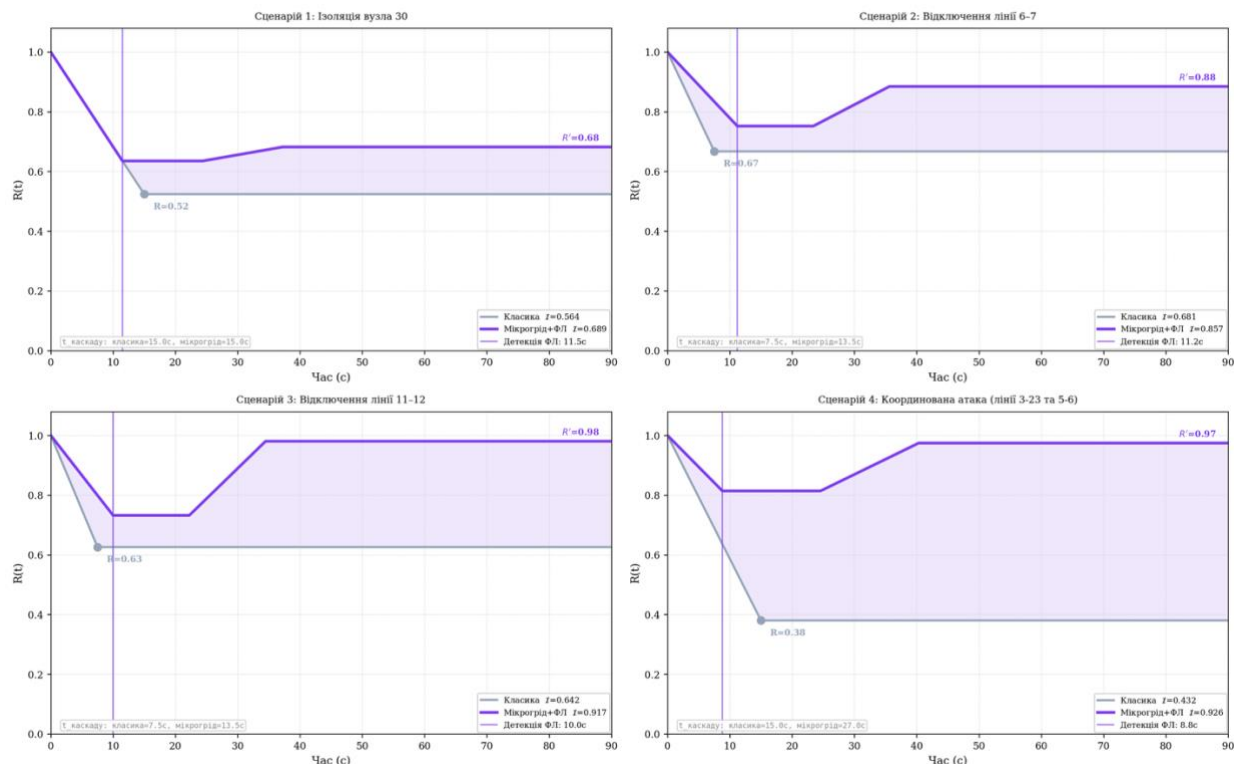


Рисунок 3.8 – Динамічна модель інциденту $R(t)$ для чотирьох сценаріїв

На рисунку 3.8 важливо порівнювати не лише мінімальне значення кривої, а й момент, коли падіння зупиняється. Для традиційної мережі виявлення відбувається пізніше, тому крива довше залишається на нижчому рівні. Для Smart Grid федеративне навчання забезпечує раннє оповіщення, а острівний режим і резервні лінії зменшують глибину та тривалість провалу. Далі ці відмінності розглянуто окремо для кожного сценарію.

У першому сценарії, де розглядається периферійна ізоляція вузла 30, статичний вплив атаки є мінімальним: традиційна мережа у стані після атаки має показник $R=0.524$, оскільки ізолюваний вузол не є критичним транзитним елементом. Замикання SW3 підвищує показник Smart Grid до 0.585, тобто дає

помірний приріст $+0.061$. Динамічна перевага в цьому випадку формується головню завдяки ранньому виявленню: федеративний детектор фіксує атаку за 11.5 с, а інтегральна резильєнтність зростає з 0.564 до 0.689. У другому сценарії розрив лінії 6-7 ізолює праву частину магістралі, але Smart Grid зберігає частину навантажень через DER-2 в острівному режимі, тому її показник після атаки становить 0.701 проти 0.667 у традиційної мережі. Після замикання SW2 показник піднімається до 0.861, а рання детекція за 11.2 с забезпечує інтегральну резильєнтність 0.857 замість 0.681.

Третій сценарій демонструє, що ефективність перемикавання ліній залежить не лише від тяжкості атаки, а й від конкретного місця розриву. Відключення лінії 11-12 дає близькі початкові значення для двох архітектур: 0.626 для традиційної мережі та 0.639 для Smart Grid у стані після атаки. Однак замикання SW1 через нижню гілку з DER-3 формує коротший альтернативний маршрут, тому відновлений показник Smart Grid зростає до 0.974. Федеративне навчання виявляє аномалію за 10.0 с, що підвищує інтегральну резильєнтність до 0.917 порівняно з 0.642.

Четвертий сценарій є найпоказовішим для обґрунтування архітектурної переваги Smart Grid. Координована атака на лінії 3-23 та 5-6 фрагментує мережу на кілька компонентів: у традиційній конфігурації показник падає до 0.380, тоді як Smart Grid навіть до перемикавання утримує 0.430 завдяки острівному режиму DER-3 та DER-4. Після одночасного замикання SW1 і SW4 показник Smart Grid відновлюється до 0.922, тобто приріст від перемикавання становить $+0.492$. Додаткова динамічна перевага виникає через раннє оповіщення: федеративна система фіксує атаку за 8.8 с, не даючи кривій $R(t)$ опуститися до мінімального рівня. У результаті інтегральна резильєнтність Smart Grid із федеративним навчанням становить 0.926, тоді як для традиційної мережі - лише 0.432.

Після сценарного аналізу підсумкове зіставлення інтегральної резильєнтності наведено на рисунку 3.9. Цей рисунок узагальнює табличні результати та показує, яку частку функціональності система зберігає протягом усього інциденту, а не лише в окремий момент після атаки або після відновлення.

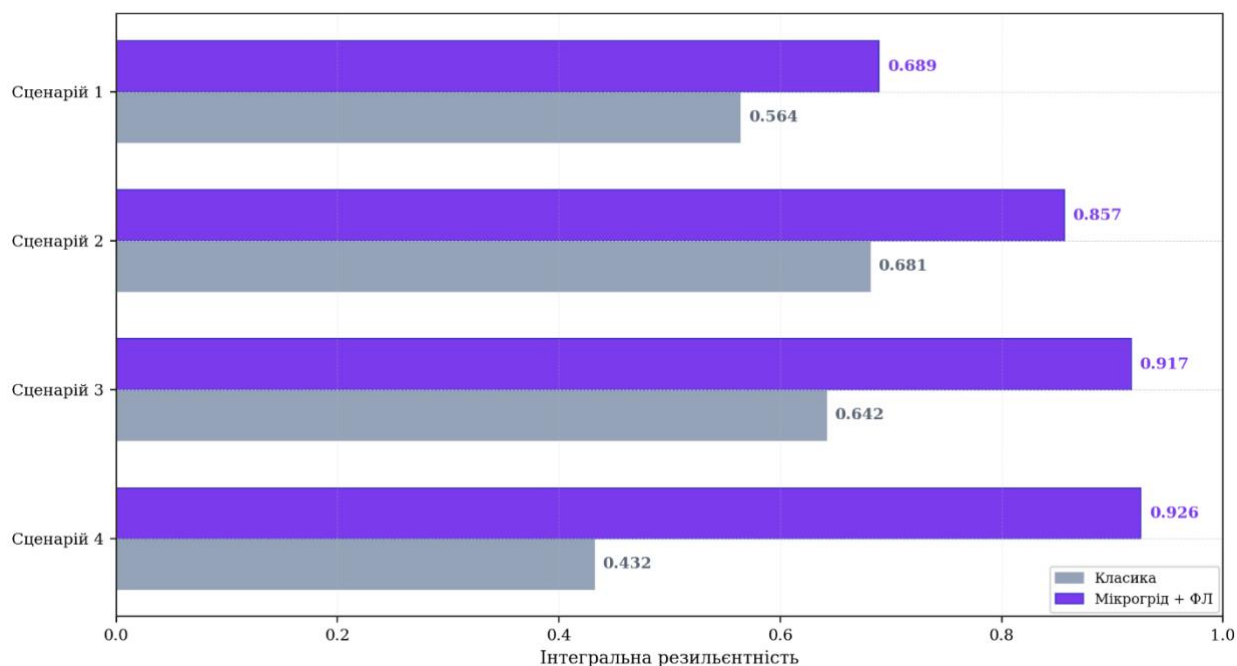


Рисунок 3.9 – Інтегральна резильєнтність для двох архітектур

Зведені результати таблиць 3.2-3.3 і рисунків 3.7-3.9 підтверджують головну ідею роботи: криві резильєнтності двох архітектур мають різну форму навіть за однакової мережі та однакових сценаріїв атаки. Статична перевага Smart Grid виникає з двох технічних причин: острівний режим DER зберігає частину критичних навантажень ще до перемикання, а замикання резервних ліній відновлює функцію передачі електроенергії. Динамічна перевага додається за рахунок федеративного навчання, яке скорочує час виявлення до 8.8-11.5 с і запускає відновлення раніше, ніж традиційний централізований моніторинг. Через це за координованої атаки традиційна архітектура втрачає 57 % інтегральної резильєнтності, тоді як Smart Grid із федеративним навчанням втрачає лише 7 %.

Висновки до розділу 3

У третьому розділі реалізовано програмний інструмент для комплексної порівняльної оцінки кіберрезильєнтності енергомереж. Моделювання здійснювалося на базі еталонної тестової системи IEEE 33-Bus, яка в пакеті представлена у двох конфігураціях: традиційній радіальній та Smart Grid із розподіленою генерацією, резервними лініями і модулем федеративного навчання. Обидві конфігурації мають однакову електричну основу та оцінюються тим самим показником, що забезпечує коректність порівняння.

Оцінювання стійкості базувалося на комплексному показнику резильєнтності R , який інтегрує топологічні параметри та електричну частку обслугованого критичного навантаження. Статичні розрахунки виконувалися через поточкорозподіл для обох архітектур, тому перевага Smart Grid обґрунтована не лише додаванням ребер у графі, а й фізичною здатністю DER підтримувати критичні навантаження в острівному режимі. Динамічна модель не вводила окремий новий показник, а застосовувала вже розрахований R для побудови часових кривих $R(t)$ та інтегральної резильєнтності.

Практичне застосування системи федеративного навчання, побудованої на базі LSTM-детекторів та алгоритму агрегації FedAvg, підтвердило свою ефективність у ролі механізму раннього попередження. Такий децентралізований підхід дозволив суттєво прискорити виявлення аномалій і скоротити час реакції до 8.8-11.5 секунд, проти 16–22 секунд у традиційній мережі. Додатковою перевагою стало застосування механізму локального персоналізованого донавчання, завдяки якому вдалося значно підвищити точність розпізнавання загроз, де середня метрика F1 стрімко зросла з початкових 0.38-0.79 до 0.85-0.94.

Підсумковий аналіз підтвердив, що перевага Smart Grid складається з двох взаємодоповнювальних чинників. Перший є статичним: перемикання резервних ліній відновлює функцію передачі електроенергії, а острівний режим DER зберігає частину критичних навантажень навіть до повної реконфігурації. Другий є динамічним: федеративне навчання забезпечує раннє оповіщення та запускає

відновлення раніше, ніж традиційний централізований моніторинг. Завдяки цьому за координованої атаки традиційна система втрачає до 57 % інтегральної резильєнтності, а Smart Grid із федеративною детекцією - лише 7 %. Отримані результати показують, що перехід до мікрокластерної архітектури у поєднанні з федеративним машинним навчанням є обґрунтованим шляхом підвищення кіберрезильєнтності критичної енергетичної інфраструктури.

ВИСНОВКИ

У дипломній роботі вирішено актуальне науково-прикладне завдання: адаптовано методику та реалізовано програмний інструмент кількісної порівняльної оцінки кіберрезильєнтності розподільчих енергетичних мереж. Це дозволило детально дослідити наслідки переходу від традиційного централізованого керування до інтелектуальної мікрокластерної архітектури на основі федеративного навчання.

1. У результаті аналізу концепції кіберрезильєнтності та архітектурних особливостей встановлено, що традиційна та Smart Grid мережі мають принципово різні профілі захищеності. Традиційна радіальна мережа має вузьку поверхню атаки, проте залишається вразливою до втрати живлення після успішного розриву ключових ліній через відсутність автоматичного відновлення. Натомість Smart Grid свідомо розширює поверхню атаки за рахунок інтеграції IoT, DER та комунікаційних шлюзів, але здобуває здатність ізолювати уражені кластери, підтримувати критичні навантаження в острівному режимі та відновлювати передачу електроенергії через перемикання резервних ліній.

2. Обґрунтовано вибір топологічного підходу на основі теорії складних мереж та сформовано математичний апарат комплексного показника резильєнтності, що інтегрує п'ять нормованих параметрів у єдину шкалу від нуля до одиниці. У результаті отримано метод, який задовольняє п'ять вимог валідності порівняльного аналізу, враховує механізм відновлення та зберігає прив'язку до реальних вразливостей через систему CVSS. Побудовані графові моделі на еталонній системі IEEE 33-Bus забезпечили відтворюваність розрахунків та можливість адаптації до реальних топологій.

3. Реалізовано програмний інструмент симуляції кібератак мовою Python та проведено порівняльний аналіз чотирьох сценаріїв з реальними CVE-ідентифікаторами. У результаті отримано кількісне підтвердження

стабільної ієрархії ефективності, за якої архітектура з федеративним навчанням перевершує традиційну за будь-яких умов. Встановлено, що при координованій атаці з оцінкою CVSS 9.8 традиційна мережа втрачає 57% резильєнтності, а Smart Grid із федеративним навчанням лише 7%, причому ефективність відновлення зростає пропорційно складності атаки.

4. Реалізовано модуль федеративного навчання на основі LSTM-детекторів та алгоритму зваженої агрегації FedAvg і оцінено його вплив на інтегральну резильєнтність через чотирифазну динамічну модель інциденту. У результаті отримано скорочення часу виявлення атаки до 8.8–11.5 секунд проти 16–22 секунд у традиційної мережі. Персоналізоване локальне донавчання підвищило середню метрику F1 з діапазону 0.38–0.79 до 0.85–0.94 при повному збереженні конфіденційності даних, що зменшило як глибину провалу показника, так і тривалість деградованого стану.

Отримані результати фундаментально підтверджують, що перехід до мікрокластерної архітектури Smart Grid у поєднанні з федеративним машинним навчанням є найнадійнішим шляхом захисту критичної інфраструктури. Перспективними напрямками подальших досліджень є диференціація вагових коефіцієнтів комплексного показника та тестування алгоритмів на топологіях реальних регіональних розподільчих мереж.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

- [1] SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Computer Security Resource Center. URL: <https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>
- [2] The President's NIAC Reports and Recommendations. Cybersecurity and Infrastructure Security Agency CISA. URL: <https://www.cisa.gov/resources-tools/groups/presidents-national-infrastructure-advisory-council/niac-reports-and-recommendations>
- [3] Castro J.P. Cyber Resilience: The Learning Phase of the Cybersecurity Compass Framework. The Cybersecurity Compass. 2024. URL: <https://cybersecuritycompass.org/cyber-resilience-the-learning-phase-of-the-cybersecurity-compass-framework-4d6dd51b746c>
- [4] Wang Y. et al. The Vulnerability of the Power Grid Structure: A System Analysis Based on Complex Network Theory // Sensors. — 2021. — Vol. 21(21). — Art. 7097. — DOI: 10.3390/s21217097.
- [5] Critical review of SCADA and PLC in smart buildings and energy sector / G. S. O.V. та ін. Energy Reports. 2024. T. 12. C. 1518–1530. DOI: 10.1016/j.egyr.2024.07.041
- [6] Deka D., Backhaus S. Topology Estimation in Bulk Power Grids: Guarantees on Exact Recovery. arXiv:1707.01596. 2017.
- [7] CISA. Cyber-Attack Against Ukrainian Critical Infrastructure. ICS Alert IR-ALERT-H-16-056-01. Cybersecurity and Infrastructure Security Agency. February 25, 2016. URL: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>
- [8] Lee R.M., Assante M.J., Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. E-ISAC, SANS ICS, 2016. 29 p. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

- [9] The Smart Grid Interoperability Panel Cyber Security Working Group. Guidelines for Smart Grid Cyber Security: T. 1. National Institute of Standards and Technology, 2010. URL: <https://csrc.nist.gov/pubs/ir/7628/final>
- [10] Ediriweera W.E.P.S., Lidula N.W.A. Design and protection of microgrid clusters: A comprehensive review. AIMS Energy. 2022. Vol. 10, No. 3. P. 375–411. DOI: 10.3934/energy.2022020
- [11] Wodicker M.R., Nelson J., Johnson N.G. Unified dispatch of grid-connected and islanded microgrids. Frontiers in Energy Research. 2023. Vol. 11. Article 1257050. DOI: 10.3389/fenrg.2023.1257050
- [12] Liu Y., Du Z., Chen Y., Zhan H. Resilient distributed control of islanded microgrids under hybrid attacks. Frontiers in Energy Research. 2023. Vol. 11. Article 1320968. DOI: 10.3389/fenrg.2023.1320968
- [13] Chen Z. et al. Cyber-physical cascading failure and resilience of power grid: A comprehensive review. Frontiers in Energy Research. 2023. Vol. 11. Article 1095303. DOI: 10.3389/fenrg.2023.1095303
- [14] Venkataramanan V., Macwan R., Abdelmalak M., Paul S. Cyber-resilient design methodology for microgrids. National Renewable Energy Laboratory, 2022. URL: <https://docs.nrel.gov/docs/fy22osti/83482.pdf>
- [15] Ayele E.D., Ferreira Gonzalez J., Teeuw W.B. Enhancing Cybersecurity in Distributed Microgrids: A Review of Communication Protocols and Standards. Sensors. 2024. Vol. 24, No. 3. Article 854. DOI: 10.3390/s24030854
- [16] Jiao P. Two-Stage Stochastic Optimization for the Pre-Position and Reconfiguration of Microgrid Defense Resources against Natural Disasters. Sensors. 2022. Vol. 22, No. 16. Article 6046. DOI: 10.3390/s22166046
- [17] Henze M., Ullrich J., Hiller J., Hohlfeld O., Wehrle K. Cybersecurity in Power Grids: Challenges and Opportunities. Sensors. 2021. Vol. 21, No. 18. Article 6225. DOI: 10.3390/s21186225
- [18] Achaal B., Adda M., Berger M., Ibrahim H., Awde A. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks,

countermeasure techniques, and challenges. Cybersecurity. 2024. Vol. 7, No. 22. DOI: 10.1186/s42400-023-00200-w

[19] CVE Program. About CVE. CVE.org. URL: <https://www.cve.org/About/Overview>

[20] FIRST.Org, Inc. Common Vulnerability Scoring System v3.1: Specification Document. 2019. URL: <https://www.first.org/cvss/specification-document>

[21] Mitikiri S. et al. A Comprehensive Metric for Resilience Evaluation of Power Distribution Systems under Cyber Attacks. arXiv:2501.12094. 2025. URL: <https://arxiv.org/abs/2501.12094>

[22] NVD NIST. CVE-2020-10937. URL: <https://nvd.nist.gov/vuln/detail/CVE-2020-10937>

[23] NVD NIST. CVE-2021-40825. URL: <https://nvd.nist.gov/vuln/detail/CVE-2021-40825>

[24] NVD NIST. CVE-2017-7921. URL: <https://nvd.nist.gov/vuln/detail/CVE-2017-7921>

[25] Friedberg I., McLaughlin K., Smith P. A Cyber-Physical Resilience Metric for Smart Grids. IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). 2017. DOI: 10.1109/ISGT.2017.8086065

[26] Mehran K. Power Systems Resilience Metrics: A Comprehensive Review of Challenges and Outlook. Sustainability. 2020. Vol. 12, No. 22. Article 9698. DOI: 10.3390/su12229698

[27] Шибасєв, г., & Гальчинський, Л. (2025). Довіро-зважена агрегація у федеративному навчанні для мікромереж. Herald of Khmelnytskyi National University. Technical Sciences, 359(6.2), 56-63. <https://doi.org/10.31891/2307-5732-2025-359-77>

[28] Pal D. et al. A Review on Intentional Controlled Islanding in Smart Power Systems and Generalized Framework for ICI in Microgrids. IEEE Systems Journal. 2019. DOI: 10.1016/j.ijepes.2019.105709

[29] Bigham J., Gamez D., Lu N. Safeguarding SCADA systems with anomaly detection. Computer Network Security. Springer, 2003. P. 171–182. DOI: 10.1007/978-3-540-45248-5_14

- [30] McMahan B., Moore E., Ramage D., Hampson S., Arcas B.A. Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS. 2017. P. 1273–1282. arXiv: <https://arxiv.org/abs/1602.05629>
- [31] Гальчинський Л., Личик В. Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство. 2023. Вип. 2(8). С. 27–33. DOI: 10.32689/maup.it.2023.2.3
- [32] Тютюннікова, В. Є. Мікромережі та федеративне навчання як основа кіберстійкої енергетичної інфраструктури / В. Є. Тютюннікова, Л. Ю. Гальчинський // Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXIV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, [Київ], 13–16 травня 2026 р. / КПІ ім. Ігоря Сікорського. – Київ, 2026. – С. 222-224. URL: <https://ela.kpi.ua/items/00f9dab9-52a8-40c3-92a0-cdb443d1e2b4>
- [33] Ahmad T. et al. Data-Driven Approaches for Sustainable and Resilient Smart Cities. Sustainability. 2023. Vol. 15, No. 16. Article 12286. DOI: 10.3390/su151612286
- [34] Fiedler M. Algebraic connectivity of graphs. Czechoslovak Mathematical Journal. 1973. Vol. 23, No. 2. P. 298–305. DOI: 10.21136/CMJ.1973.101168
- [35] Cuadra L. et al. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. Energies. 2015. Vol. 8, No. 9. P. 9211–9265. DOI: 10.3390/en8099211
- [36] Pagani G.A., Aiello M. The Power Grid as a Complex Network: A Survey. Physica A. 2013. Vol. 392, No. 11. P. 2688–2700. DOI: 10.1016/j.physa.2013.01.023
- [37] Gago S., Hurajová J.C., Madaras T. Betweenness centrality in graphs. Quantitative Graph Theory: Mathematical Foundations and Applications. Chapman and Hall/CRC. 2014. P. 233–257 DOI: 10.1201/b17645-12
- [38] Barthélemy M. Betweenness centrality in large complex networks. The European Physical Journal B. 2004. Vol. 38, No. 2. P. 163–168 DOI: 10.1140/epjb/e2004-00111-4
- [39] Hernández J.M., Van Mieghem P. Classification of graph metrics. Delft University of Technology. 2011 URL: <https://www.nas.ewi.tudelft.nl/people/Piet/TUDELFTReports.html>

- [40] Gao H. et al. Resilience-oriented critical load restoration using microgrids in distribution systems. *IEEE Transactions on Smart Grid*. 2016. Vol. 7, No. 6. P. 2837–2848 DOI: 10.1109/TSG.2016.2550625
- [41] Panteli M., Mancarella P. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. *IEEE Systems Journal*. 2017. Vol. 11, No. 3. P. 1733–1742. DOI: 10.1109/JSYST.2015.2389272
- [42] AlMuhaini M., Heydt G.T. A novel method for evaluating future power distribution system reliability. *IEEE Transactions on Power Systems*. 2013. Vol. 28, No. 3. P. 3018–3027. DOI: 10.1109/TPWRS.2012.2230195
- [43] Jithish J., Alangot B., Mahalingam N., Yeo K.S. Distributed anomaly detection in Smart Grids: A federated learning-based approach. *IEEE Access*. 2023. Vol. 11. P. 7157–7179. DOI: 10.1109/ACCESS.2023.3237554
- [44] Guha S., Sarkar D., Chowdhury D.R. LSTM-based anomaly detection in power systems. *Electric Power Systems Research*. 2023. Vol. 220. Article 109351. DOI: 10.1016/j.epsr.2023.109351
- [45] Tabassum A. et al. Federated learning-based anomaly detection for smart grids using LSTM networks. *IEEE Transactions on Industrial Informatics*. 2023.
- [46] Panteli M., Mancarella P., Trakas D.N., Kyriakides E., Hatziaargyriou N.D. Metrics and quantification of operational and infrastructure resilience in power systems. *IEEE Transactions on Power Systems*. 2017. Vol. 32, No. 6. P. 4732–4742. DOI: 10.1109/TPWRS.2017.2664141
- [47] Sarker S.K. et al. Advancing microgrid cyber resilience: Fundamentals, trends and case study on data-driven practices. *Applied Energy*. 2025. URL: <https://www.sciencedirect.com/science/article/pii/S0306261925014837>
- [48] IEC 60870-5-104:2006. Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles. International Electrotechnical Commission, 2006. URL: <https://webstore.iec.ch/en/publication/3751>

[49] IEEE Std C37.118.1-2011. IEEE Standard for Synchrophasor Measurements for Power Systems. IEEE, 2011. DOI: 10.1109/IEEESTD.2011.6111219. URL: <https://standards.ieee.org/ieee/C37.118.1/4902/>