

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

До захисту допущено
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

« _____ » _____ 2025 р.

Дипломна робота
на здобуття ступеня бакалавра
за освітньо-професійною програмою «Системи, технології та математичні
методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Оцінювання кіберрезильєнтності енергопідприємств

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи **ФБ-13**
(шифр групи)

Левашова Світлана Дмитрівна
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент кафедри ІБ, к.т.н., доцент Гальчинський Л. Ю.
(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 – 2025 року

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«__» _____ 2025 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Левашової Світлани Дмитрівни
(прізвище, ім'я, по батькові)

1. Тема роботи: «Оцінювання кіберрезильєнтності енергопідприємств»,

керівник роботи: доцент кафедри ІБ, к.т.н., доцент Гальчинський Л. Ю.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від 26 травня 2025 р. № 1761-С.

2. Термін подання здобувачем вищої освіти роботи: 13 червня 2025 р.
3. Вихідні дані до роботи: аналіз літературних джерел із кіберрезильєнтності, особливостей енергосистем та кібератак на енергетичні об'єкти; дослідження методології R4, методу аналізу ієрархій (АНР), шкали Лайкерта; використання Python, HTML, CSS та JavaScript.
4. Зміст роботи: Робота присвячена дослідженню методології R4 та розробці веб-застосунку для оцінки кіберрезильєнтності енергетичних підприємств. Вона розпочинається з теоретичного аналізу поняття кібервідмовостійкості та

специфіки енергосистем, а також розглянуто реальні приклади кібератак на критичну інфраструктуру, що підкреслюють актуальність роботи. На основі дослідженої методології R4 сформульовано набір питань для веб-опитувальника із використанням шкали Лайкерта. Для визначення вагових коефіцієнтів метрик застосовано метод аналізу ієрархій (АНР) із залученням групи експертів. Розроблений веб-застосунок автоматизує процес збору відповідей респондентів, обчислює загальний рівень кіберрезильєнтності та візуалізує результати у вигляді діаграм. Робота завершується перевіркою коректності алгоритмів обчислення та аналізом тестових даних, демонструючи ефективність розробленого веб-застосунку та його практичну користь для керівників енергетичних підприємств у контексті підвищення їхньої кіберрезильєнтності.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація.
6. Дата видачі завдання: 04 листопада 2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання завдання та тематики дипломної роботи	04.11.2024-18.11.2024	виконано
2	Пошук та опрацювання літературних джерел	18.11.2024-23.12.2024	виконано
3	Дослідження поняття кіберрезильєнтності та особливості енергосистем	23.12.2024-27.01.2025	виконано
4	Аналіз прикладів кібератак на об'єкти критичної інфраструктури	27.01.2025-10.02.2025	виконано
5	Дослідження методології "R4" для оцінки кіберрезильєнтності енергопідприємств	10.02.2025-10.03.2025	виконано
6	Створення анкети для опитування	10.03.2025-14.04.2025	виконано
7	Проведення експертного оцінювання вагових коефіцієнтів	14.04.2025-28.04.2025	виконано
8	Розробка веб-застосунку для оцінки кіберрезильєнтності	28.04.2025-19.05.2025	виконано
9	Тестування веб-застосунку	19.05.2025-26.05.2025	виконано
10	Оформлення дипломної роботи відповідно до методичних вказівок	26.05.2025-09.06.2025	виконано
11	Передзахист дипломної роботи	13.06.2025	
12	Захист дипломної роботи	20.06.2025	

Здобувач вищої освіти

(підпис)

Світлана ЛЕВАШОВА

(Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи

(підпис)

Леонід ГАЛЬЧИНСЬКИЙ

(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг дипломної роботи 105 сторінок, 47 ілюстрацій, 14 таблиць, 2 додатки і 40 джерел літератури.

Об'єкт дослідження: Кіберрезильєнтність енергопідприємств та методика її оцінювання.

Предмет дослідження: Методи та засоби оцінювання кіберрезильєнтності енергопідприємств.

Мета дослідження: Розробка підходу до оцінювання кіберрезильєнтності енергопідприємств шляхом створення веб-застосунку, що проводить опитування, обробляє інформацію та генерує відповідні оцінки на основі конкретних індикаторів.

Методи дослідження (етапи):

- Аналіз літературних джерел та нормативних документів;
- Системний аналіз;
- Математичне моделювання;
- Збір та обробка даних;
- Програмна реалізація;
- Візуалізація результатів.

Результати роботи були представлені на XXIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених [1].

Ключові слова: кіберрезильєнтність, SCADA, енергопідприємство, метрики кіберстійкості, шкала Лайкерта, метод аналізу ієрархій.

ABSTRACT

The volume of the work is 105 pages, 47 illustrations, 14 tables, 2 appendices and 40 sources of literature.

Object of research: Cyber resilience of energy enterprises and the methodology for its assessment.

Subject of research: Methods and tools for assessing the cyber resilience of energy enterprises.

Aim of research: Developing an approach to evaluate the cyber resilience of energy enterprises by creating a web application that conducts the survey, processes information and generates appropriate estimates based on certain indicators.

Research methods (stages):

- Analysis of literature sources and regulatory documents;
- System analysis;
- Mathematical modeling;
- Data collection and processing;
- Software implementation;
- Visualization of results.

The results were presented at the 28th All-Ukrainian scientific and practical conference of students, postgraduates, and young scientists [1].

Keywords: cyber resilience, SCADA, energy enterprise, cyber resilience metrics, Likert scale, Analytic Hierarchy Process (AHP).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	9
ВСТУП.....	11
1 ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРРЕЗИЛЬЄНТНОСТІ ЕНЕРГОПІДПРИЄМСТВ.....	13
1.1 Поняття кіберрезильєнтності	13
1.2 Особливості енергосистем.....	15
1.3 Приклади кібератак на об’єкти критичної інфраструктури.....	20
Висновки до розділу 1	27
2 МЕТОДОЛОГІЯ ОЦІНКИ КІБЕРРЕЗИЛЬЄНТНОСТІ	29
2.1 Метрики стійкості.....	29
2.2 Анкета для опитування	36
2.3 Обчислення вагових коефіцієнтів метрик.....	40
2.4 Обчислення загального показника кіберрезильєнтності.....	43
Висновки до розділу 2	45
3 ПРАКТИЧНІ РЕЗУЛЬТАТИ.....	47
3.1 Обчислення ваг за допомогою методу аналізу ієрархій (АНР)	47
3.2 Реалізація веб-застосунку	56
3.3 Візуалізація результатів	73
Висновки до розділу 3	76
ВИСНОВКИ.....	78
ПЕРЕЛІК ДЖЕРЕЛ І ПОСИЛАНЬ	80
ДОДАТОК А КОД PYTHON ДЛЯ ОБЧИСЛЕННЯ ВАГ АНР	86

ДОДАТОК Б КОД JAVASCRIPT COMPUTE.JS 90

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ICS – Industrial Control System(s) (промислові системи керування);

SCADA – Supervisory Control and Data Acquisition (системи диспетчерського керування та збору даних);

DCS – Distributed Control System (розподілена система керування);

WAMS – Wide Area Monitoring System(s) (система(и) широкомасштабного моніторингу);

EPS – Electric Power System (електроенергетична система);

MES – Manufacturing Execution System (система управління виробничими процесами);

ERP – Enterprise Resource Planning (система управління ресурсами підприємства);

EWS – Engineering Workstation (інженерна робоча станція);

HMI – Human-Machine Interface (людино-машинний інтерфейс);

PMU – Phasor Measurement Unit (пристрій вимірювання синхрофазорів);

GNSS – Global Navigation Satellite System (глобальна навігаційна супутникова система);

TS – Time Synchronization (синхронізація часу);

MTU – Master Terminal Unit (головний термінальний блок);

RTU – Remote Terminal Unit (віддалений термінальний блок);

PLC – Programmable Logic Controller (програмовані логічні контролери);

PDC – Phasor Data Concentrator (концентратор фазорних даних);

CDO – Central Dispatch Office (центральний диспетчерський офіс);

IDO – Interconnected Dispatch Office (офіс диспетчеризації міжрегіонального рівня);

RDO – Regional Dispatch Office (регіональний диспетчерський офіс);

ODC – Operational-Dispatch Control (оперативно-диспетчерське керування);

R4 – Структура стійкості (robustness, redundancy, resourcefulness, rapidity);

CRAM – Cyber Resilience Assessment Methodology (методологія оцінювання кіберрезильєнтності);

AHP – Analytic Hierarchy Process (метод аналізу ієрархій);

ECS – Expected Composite Score (очікуваний зважений бал);

OCS – Overall Composite Score (загальний комплексний бал);

DS – Domain Score (оцінка домену);

CSF – Critical Service Functionality (критично важлива функціональність)\;

R – Кіберрезильєнтність (Cyber Resilience).

ВСТУП

У процесі розвитку технологій з'явилося чимало переваг для забезпечення комфортного життя людства. Одним із найважливіших засобів для існування сучасного світу є електроенергія, без якої неможливо уявити нормальне функціонування суспільства. Вона надає широкий спектр можливостей: від заряджання та використання електронних пристроїв до підтримки стабільного існування бізнесу будь-якого масштабу. Безперебійне постачання електроенергії підтримує функціонування житлових будинків, офісів, промислових підприємств та інших об'єктів.

Останнім часом питання забезпечення безперебійного електропостачання у всі куточки України набуло особливої актуальності. До традиційних ризиків природнього або техногенного походження додалися загрози, пов'язані зі збройною агресією з боку РФ, що охоплюють фізичне руйнування об'єктів критичної інфраструктури та кібератаки на її системи. Для кожного українця моніторинг графіків вимкнення електроенергії та планування свого часу відповідно до них стали щоденною реальністю. Станом на початок 2025 року внаслідок ракетних атак було зруйновано понад 80% потужностей теплових електростанцій (ТЕС) та понад 40% гідроелектростанцій (ГЕС), загальний збиток оцінюється приблизно в \$1млрд. Також було зафіксовано ряд кібератак на енергетичний сектор, кількість яких, за деякими джерелами, у період з 2020 по 2023 рік оцінюються приблизно в 4500 таких випадків [2]. Найвідомішими з атак залишаються: на енергетичні компанії (2015 рік) та на НЕК "Укренерго" (2016 рік). Дані події чітко окреслюють необхідність підвищення рівня безпеки енергосистем.

Відновлення пошкодженої інфраструктури потребує величезних фінансових ресурсів і часу. До того ж, не треба забувати про те, що відновлювальні роботи можуть тривати роками. Але для того, щоб вчасно виявляти вразливості та

оцінювати стан захищеності енергопідприємств на основі специфічних показників, необхідне дослідження універсального алгоритму. Це дасть змогу працювати над слабкими місцями – такими, як фізичні та технічні, так і такими, що пов'язані з організаційними аспектами. Простіше кажучи – необхідно оцінити стійкість системи. Відповідно до досліджень NIAC (2010 рік), ефективність стійкої інфраструктури або підприємства визначається їхньою здатністю передбачати, сприймати, адаптуватися та/або швидко відновлюватися після результату руйнівної події [3]. Тому, у контексті кібербезпеки, буде доцільною розробка інструменту, що оцінюватиме кіберрезильєнтність (кібервідмовостійкість) енергетичного підприємства та надаватиме візуалізацію вразливих аспектів.

Окреслимо поняття:

Об'єкт дослідження: Кіберрезильєнтність енергопідприємств та методика її оцінювання.

Предмет дослідження: Методи та засоби оцінювання кіберрезильєнтності енергопідприємств.

Мета дослідження: Розробка підходу до оцінювання кіберрезильєнтності енергопідприємств шляхом створення веб-застосунку, що проводить опитування, обробляє інформацію та генерує відповідні оцінки на основі конкретних індикаторів.

1 ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРРЕЗИЛЬЄНТНОСТІ ЕНЕРГОПІДПРИЄМСТВ

1.1 Поняття кіберрезильєнності

Термін “кіберрезильєнність” (від англ. Cyber Resilience, дослівно — кібервідмовостійкість) з кожним роком все більше закріплюється в сучасному кіберінфопросторі. Інформаційні технології проникли у всі сфери життєдіяльності – від побуту та державних установ до критичної інфраструктури й бізнес-процесів. Закон, сформульований Ісааком Ньютоном – “на кожному дію знайдеться протидія”, – також актуальний у випадку інформаційних технологій: на кожен метод захисту знайдеться спосіб обходу, а на кожному кібератаку – метод протидії. Для підприємств, зокрема об’єктів критичної інфраструктури, створюється необхідність не лише протистояти інцидентам безпеки, а й швидко відновлювати операційну діяльність після атак. Для цього і підходить поняття кібервідмовостійкості. Розглянемо його детальніше:

Залежно від сфери застосування, визначення “стійкості” можуть відрізнятися. Національна академія наук США (NAS) визначає стійкість як «здатність підготуватися, спланувати, поглинути, відновитися або успішніше адаптуватися до реальних чи потенційних несприятливих подій» [4].

Ерік Холнагель, професор та дослідник у галузі інженерії відмовостійкості, визначає чотири ключові елементи стійкості: навчання (осмислення минулого досвіду), реагування (дії у відповідь), моніторинг (відстеження змін) і передбачення (прогнозування майбутніх подій) [5].

Бруно та ін. експерти у галузі сейсмічної стійкості, виділяють чотири складові: міцність (robustness), надлишковість (redundancy), винахідливість (resourcefulness) і швидкість реагування (rapidity). Міцність означає здатність протистояти руйнуванням; надлишковість – наявність запасних елементів, які

можуть замінити пошкоджені; винахідливість – можливість ефективно використовувати доступні ресурси; а швидкість реагування визначає як швидко система повертається до нормальної роботи. Цей підхід назвали структурою стійкості R4 [6].

Лінков та ін. пропонують матрицю кіберстійкості, яка поєднує чотири етапи управління подіями: планування та підготовка, виявлення, відновлення та адаптація. Та чотири домени: фізичний, інформаційний, когнітивний та соціальний. Планування передбачає підготовку до кібератак, поглинання – здатність витримати атаку, відновлення – повернення до роботи, адаптація – покращення системи. Домени охоплюють технічні, інформаційні, управлінські та соціальні аспекти, підкреслюючи роль рішень і культури в стійкості [7].

Рейгер та ін. фахівці з проектування стійких керуючих систем, визначають стійку систему управління як систему, яка зберігає обізнаність про свій стан і прийнятний рівень функціонування у відповідь на порушення, включаючи загрози несподіваного та зловмисного характеру [8].

IBM, у свою чергу, охарактеризовує кіберстійкість як здатність організації запобігати інцидентам кібербезпеки, протистояти їм і відновлюватися після них. Організація повинна забезпечувати виконання своїх цілей навіть за умов серйозних кіберзагроз, природних катастроф чи економічних криз [9].

Тепер окремо розглянемо поняття відмовостійкості. NIST (2013) [10] визначає відмовостійкість як властивість системи зберігати повну або часткову працездатність у випадках відмов окремих елементів, що не пов'язані із зовнішніми нерегламентованими діями [11].

У чому ж різниця між кібервідмовостійкістю та кібербезпекою? Кібербезпека орієнтується на проактивні заходи, які допомагають компанії боротися зі зростаючим поширенням кібератак. Тоді як кіберрезильєнтність фокусується на потенціалі організації мінімізувати наслідки атаки, обмежити втрати та відновити роботу у звичному режимі. Обидва поняття тісно пов'язані

між собою: джерела кібервідмовостійкості походять із практик кібербезпеки [12].

Як визначити чи ефективна кіберрезильєнтність організації?

Ефективна кіберрезильєнтність – це стратегія, що містить у собі комплексну оцінку ризиків для всієї організації.

Відповідно до напрацювань Cisco, до її основних компонентів належать [13]:

- Кібербезпека – технічні, організаційні та фізичні заходи, що забезпечують конфіденційність, цілісність і доступність даних;
- Управління ризиками – спрямоване на виявлення потенційних загроз, що можуть вплинути на роботу організації (людські помилки, збої апаратного забезпечення, стихійні лиха, відключення електроенергії, кібератаки та фізичні атаки);
- Безперервність – здатність підтримувати життєдіяльність організації та продовжувати надавати послуги після інциденту;
- Організаційна культура та підготовка – навчання співробітників, підготовка процедур, інструментів та політик для забезпечення безперервного функціонування організації.

Аналіз цих факторів вимагає ретельної експертної оцінки та буде розглянутий у другому розділі.

1.2 Особливості енергосистем

Сучасні інтелектуальні електроенергетичні системи – приклад кіберфізичних систем, у яких ІТ-технології тісно поєднані з фізичними процесами. А отже, кожен компонент системи безпосередньо впливає на моніторинг, управління та стабільність енергомережі. Дана залежність дозволяє отримувати в режимі реального часу інформацію про стан мережі, прогнозувати навантаження, координувати регулювання частоти та потужності. Проте, оскільки

зв'язок між інформаційною, комунікаційною та фізичною складовими стає сильнішим, кібератаки можуть мати все більш помітний вплив на нормальне функціонування енергосистем (Electric Power System – EPS) [14].

Контроль операцій EPS вимагає високоякісної інформації: важливими є повнота функцій, надійність компонентів системи збору, передачі та обробки даних, а також стійкість програмного забезпечення. Оскільки цифрові пристрої керують фізичними процесами на основі різних інформаційних потоків, система стає критично вразливою до кіберзагроз. Кібератаки, включаючи спеціально розроблені ШПЗ (деякі з яких детальніше згадані у розділі 1.3) Stuxnet, BlackEnergy, Sreprise Crash та Trisis/Trident, спрямовані на відключення оперативного-диспетчерського контролю (Operational-Dispatch Control – ODC) EPS [15]. Це підкреслює необхідність не лише покращення кібербезпеки, а й забезпечення кіберрезильєнтності у будь-яких умовах.

Кібервідмовостійкість має особливе значення для ODC кіберфізичних систем, оскільки наслідки кібератак можуть спричинити збої у функціонуванні систем управління [16].

У контексті оцінювання кіберрезильєнтності енергопідприємств доцільно розглянути всю сукупність технічних засобів, інакше кажучи – енергосистеми, що забезпечують їх функціонування.

Енергосистема відноситься до промислових систем керування (Industrial Control System – ICS), загального терміна для різних типів систем керування та пов'язаних із ними приладів. Залежно від галузі кожна ICS функціонує по-різному, адаптуючись для ефективного електронного керування завданнями. Пристрої та протоколи ICS застосовуються майже у всіх галузях промисловості та критичної інфраструктури, зокрема й у сфері енергетики.

Існує декілька типів ICS, найпоширенішими з яких є системи диспетчерського керування та збору даних (SCADA) і розподілені системи керування (DCS). Енергосистеми працюють на основі концепції Supervisory

Control and Data Acquisition (SCADA). Для початку розглянемо загальну інформацію про SCADA.

SCADA [17] – це комплекс програмно-апаратних засобів, що дозволяє організаціям контролювати та моніторити промислові процеси шляхом безпосередньої взаємодії з обладнанням і перегляду даних у реальному часі. Його функціональні можливості доповнює WAMS. Wide Area Monitoring Systems (WAMS) [18] – розширене програмне рішення для моніторингу та контролю масштабних енергетичних мереж. WAMS покращує ситуаційну обізнаність та управління, особливо під час аварій.

Для кращого розуміння організації взаємодії між обладнанням і програмним забезпеченням, варто розглянути функціональні рівні ICS (рисунок 1.1) [19]:

- Рівень 0 – польові пристрої. Містить датчики та виконавчі механізми (тискові сенсори, двигуни тощо). Вони безпосередньо взаємодіють із технологічним процесом, контролюючи різні фізичні параметри;
- Рівень 1 – контролери введення/виведення (I/O) та програмовані логічні контролери (PLC/RTU). Обробляють сигнали від датчиків Рівня 0 та передають команди на виконавчі механізми;
- Рівень 2 – диспетчерські комп'ютери (Supervisory Computers) та SCADA-сервери. Відповідають за збір, зберігання, обробку даних із контролерів Рівня 1 та відображення оператору через Human-Machine Interface (HMI);
- Рівень 3 – рівень керування виробництвом. Використовується для збору статистики, аналізу продуктивності та прогнозування можливих відмов. На цьому рівні також працюють Manufacturing Execution System (MES), що інтегрують виробничі процеси та управлінські системи підприємства;
- Рівень 4 – рівень планування виробництва. Відповідає за управління бізнес-процесами, стратегічне планування та взаємодію з Enterprise Resource Planning (ERP) системами підприємства.

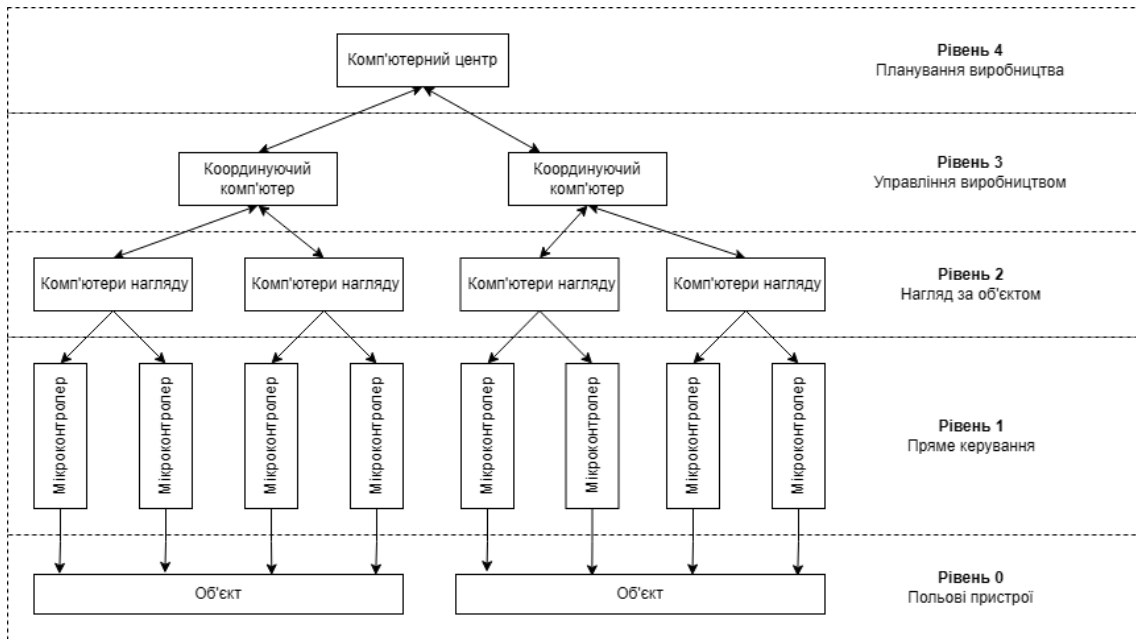


Рисунок 1.1 – Структура рівнів промислового керування

Отже, розглянемо ієрархічну структуру системи оперативно-диспетчерського керування та систем моніторингу роботи енергетичних систем, щоб вивчити питання кіберрезильєнтності [18, 20]:

Верхній рівень диспетчерського управління:

- CDO (Central Dispatch Office) – центральний диспетчерський офіс, що виконує найвищий рівень координації в енергосистемі;
- IDO (Interconnected Dispatch Office) – офіс диспетчеризації міжрегіонального (взаємопов'язаного) рівня;
- RDO (Regional Dispatch Office) – регіональний диспетчерський офіс.

Ці три рівні забезпечують ієрархічну модель управління: від регіональних задач (RDO) до глобальних операцій (CDO).

WAMS (Wide Area Measurement System):

- GNSS (Global Navigation Satellite System) – глобальна навігаційна супутникова система для забезпечення синхронізації часу (TS);
- PDC (Phasor Data Concentrator) – концентратор фазорних даних (величин, що описують амплітуду та фазу змінного сигналу в комплексній формі), що

збирає інформацію від PMU;

- PMU (Phasor Measurement Unit) – фазорні вимірювальні пристрої, що фіксують електричні параметри (напругу, струм, частоту, фазу) з часовою синхронізацією GNSS.

SCADA (Supervisory Control and Data Acquisition):

Control Centre – центр управління, що містить:

- HMI (Human-Machine Interface) – людино-машинний інтерфейс для оператора;
- EWS (Engineering Workstation) – інженерна станція для глибшого аналізу та налаштувань;
- MTU (Master Terminal Unit) – головний термінальний блок, що приймає та відправляє дані з/до віддалених пристроїв;
- RTU (Remote Terminal Unit) – віддалений термінальний блок, який збирає дані з датчиків, вимірювальних приладів та передає їх у MTU (або навпаки, отримує команди від центру керування для керування обладнанням).

Завдяки глибокій інтеграції інформаційних та фізичних компонентів, енергосистеми стають вразливими до низки кіберзагроз:

1. Атаки з піддробкою даних – втручання в роботу RTU, PMU та каналів зв'язку для внесення помилкових даних. Як наслідок, відбувається викривлення інформації про стан мережі, що може призвести до хибних дій диспетчерів та автоматизованих систем;
2. Атаки на синхронізацію часу – втручання у роботу GNSS. Втрата коректного часу призводить до спотворення вимірювань та помилкового реагування систем захисту;
3. Атаки відмови в обслуговуванні – перевантаження серверів моніторингу або SCADA, що може паралізувати управління системою;
4. Динамічні атаки на систему – перехоплення та повторне передавання старих

даних для створення хибної картини стану мережі;

5. Комплексні атаки – поєднання кількох атак для створення каскадних збоїв (наприклад, спочатку DoS-атака для блокування моніторингу, потім injection-атака для викривлення контрольних параметрів).

Отже, сучасні енергосистеми, інтегровані в системи керування, є складними кіберфізичними системами. Вони працюють на основі SCADA, WAMS та інших технологій, що були розглянуті у цьому підпункті, та забезпечують моніторинг та керування енергосистемами в режимі реального часу. Але, через стрімкий технічний прогрес та зростаючу кількість кібератак (розглянемо у наступному підпункті), енергосистеми стають вразливими до атак. Тому критично важливо оцінювати рівень кіберрезильєнтності таких систем для їх подальшого покращення.

1.3 Приклади кібератак на об'єкти критичної інфраструктури

Кібернетичні атаки на системи критичної інфраструктури набирають все більших обертів. Якщо раніше злочинці діяли з метою перевірки своїх здібностей, через конкуренцію чи заради фінансової вигоди, то зараз це стало інструментом політичного тиску та методом психологічного впливу на населення.

Як зазначає Джейк Салліван, радник з безпеки США, енергетичні системи у світі постійно піддаються кібератакам і залишаються вразливими до збоїв [21]. За даними Check Point Research, підрозділу досліджень кібербезпеки компанії Check Point Software Technologies, кількість кібератак на комунальні служби США у 2024 році збільшилась на 70% у порівнянні з 2023 роком [22]. Вразливість критичної інфраструктури зростає, оскільки активи розширюються, а проблема застарілих утиліт та програмного забезпечення з кожним роком стає все більш гострою.

У 2021 році американська нафтопровідна компанія Colonial Pipeline зазнала кібератаки програмою-вимагачем DarkSide. Атака сталася через зламаний пароль неактивного облікового запису, який не мав багатофакторної автентифікації. У результаті цього оператор компанії був змушений призупинити роботу трубопроводу, що транспортував майже 45% пального, що призвело до кризи постачання, режиму надзвичайної ситуації та викликало панічні настрої серед населення [23].

“За останні 10 років кібератаки вплинули на вітроенергетичні організації та об’єкти принаймні в семи країнах: sPower у США; ENERCON, Deutsche Windtechnik і Nordex SE в Німеччині; системи SCADA вітрових турбін в Азербайджані; численні комунальні послуги в Данії; офшорна вітроенергетична установка в Індії; а також європейські та міжнародні постачальники офшорних вітрових електростанцій у Південно-Китайському морі. Кібератаки на українські електроенергетичні об’єкти також дають важливі уроки для сектору вітроенергетики”, – йдеться на офіційному веб-сайті Міністерства енергетики США (U.S. Department of Energy) [24].

Кібернетичні атаки на критичну інфраструктуру України, зокрема на енергосистеми, є одним із ключових елементів гібридної війни, що веде Росія проти нашої держави. Починаючи з 2013 року фіксується все більше випадків, що дестабілізують або намагаються дестабілізувати безперервну роботу енергосистем. Атаки еволюціонували від шпигунських кампаній до цілеспрямованих деструктивних дій. Розглянемо хронологію, використані методи та їх наслідки детальніше:

Зародження. 2013р:

У 2013 році під час масових протестів було здійснено перші кібератаки на інформаційні системи приватних підприємств та державних установ України.

Початкові атаки. 2014-2015рр:

У 2014 році було виявлено використання троянського програмного

забезпечення BlackEnergy для кібершпигунства проти державних установ України. Це ШПЗ було здатне заразити промислові системи управління (SCADA), що свідчило про можливість майбутніх атак на енергосистеми [25].

23 грудня 2015 року сталася перша у світі відома успішна кібератака на енергетичну систему. Під удар потрапило три енергопостачальні компанії – “Прикарпаттяобленерго”, “Київобленерго” та “Чернівціобленерго”. Атакуючі використовували методи соціальної інженерії, розсилаючи фішингові листи, захопили управління автоматизованими системами (АС) та вимкнули підстанції. Для знищення залишкових слідів на серверах застосовувався KillDisk, а комунікацію ускладнювали через DDoS-атаки на телефонні лінії кол-центрів. Дана атака продемонструвала високий рівень загроз для енергетичної інфраструктури та необхідність підвищення кібербезпеки [26].

Атака Industroyer. 2016р:

17 грудня 2016 року Україна знову стала жертвою кібератаки на енергосистему. Злочинна група Sandworm Team використала шкідливе програмне забезпечення Industroyer (за деякими джерелами – CrashOverride) для атаки на підстанцію "Північна" компанії "Укренерго". Як і у випадку 2015 року, ШПЗ потрапило в систему через зловмисні фішингові дії. Атака стала можливою через вразливі промислові протоколи, що розроблялися десятиліття тому, коли системи були ізольованими та не мали вбудованого захисту. Industroyer мав виконуваний файл, компонент очищення даних та два бекдори для комунікації з віддаленими серверами – основний та резервний, через які зловмисники отримували доступ до системи. Як наслідок, атака призвела до серйозних збоїв у роботі підстанції та підкреслила необхідність модернізації систем безпеки [27].

Зростання кіберзагроз. 2017-2021рр:

У цей період зловмисники продовжують випробовувати різноманітне шкідливе програмне забезпечення. У 2017 році те ж угруповання Sandworm створило та запустило нове ШПЗ NotPetya [28]. Так як у хакерів уже був досвід

атак на державні структури України, саме звідси й почалась історія згаданого вірусу. Його масове розповсюдження почалося з зараження сервера компанії Linkos (через фішингові листи), який розсилає оновлення програми М.Е.Дос (бухгалтерська звітність та документообіг). Протягом декількох місяців вірус розійшовся по всьому світу. За оцінками Білого дому, загальні збитки від атаки сягнули \$10 млрд. Вірус уразив понад 2000 організацій. В Україні наслідки були особливо руйнівними: було заражено усі комп'ютери кожного міністерства, численні термінали та банкомати, 10% ПК по всій країні тощо (рисунок 1.2) [29]:

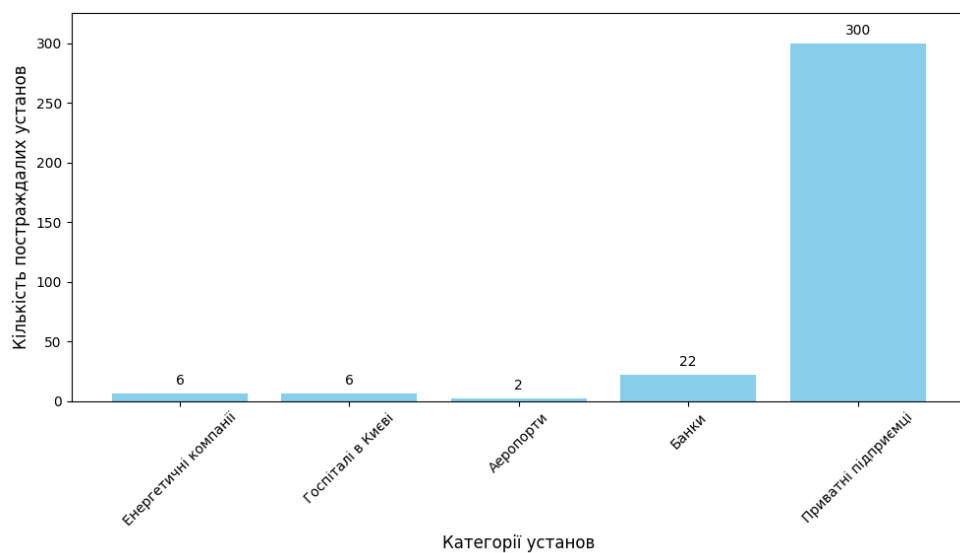


Рисунок 1.2 – Кількість постраждалих установ України від кібератаки NotPetya

NotPetya шифрував файли та вимагав викуп за відновлення доступу до інформації. Таким чином, вірус показав слабкі місця в світових системах та підкреслив глобальний характер кіберзагроз.

У наступні роки посилювались спроби атак та тестувались інші ШПЗ для кібершпигунства, саботажу та розвідки.

2022-2024рр:

З початку повномасштабної війни у 2022 році інтенсивність атак на найбільший приватний енергохолдинг України – ДТЕК – зросла на 20%, – повідомляє його прес-служба. ІТ-фахівці державної компанії “Укренерго”

зафіксували збільшення кількості кібератак на систему ще в січні 2022 року, зазначає член правління та IT-директор компанії Сергій Галаган. Після 24 лютого 2022 року кількість кіберінцидентів зросла втричі порівняно з попереднім роком.

Російські хакери застосовують широкий спектр методів – від сканування IT-периметру до масових DDoS-атак. Під час однієї з таких атак на “Укренерго” кількість запитів сягнула понад 5 млн за декілька годин. У 2022 році DDoS-атаки здійснювалися вдесятеро частіше, ніж у 2021 році, зазначає Сафаров із Міністерства енергетики України. А у 2024 році Державна служба спеціального зв'язку та захисту інформації опрацювала 4315 кіберінцидентів, що на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз (джерело – Укрінформ).

Для порівняння на рисунку 1.3 наведено графік кібератак у 2021-2023рр [30]:

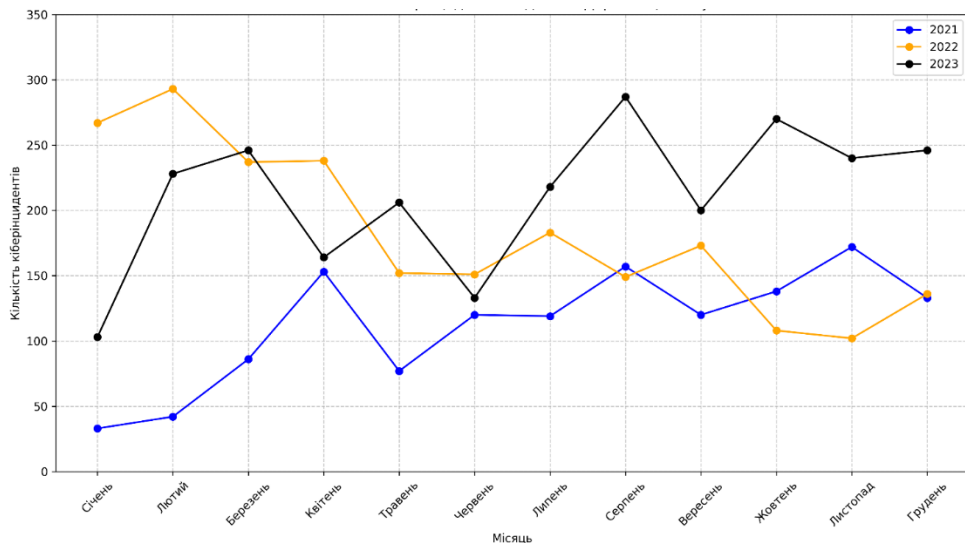


Рисунок 1.3 – Кількість кіберінцидентів за даними Держспецзв’язку

Таким чином, сумарна кількість кіберінцидентів за кожен рік зображена на рисунку 1.4:

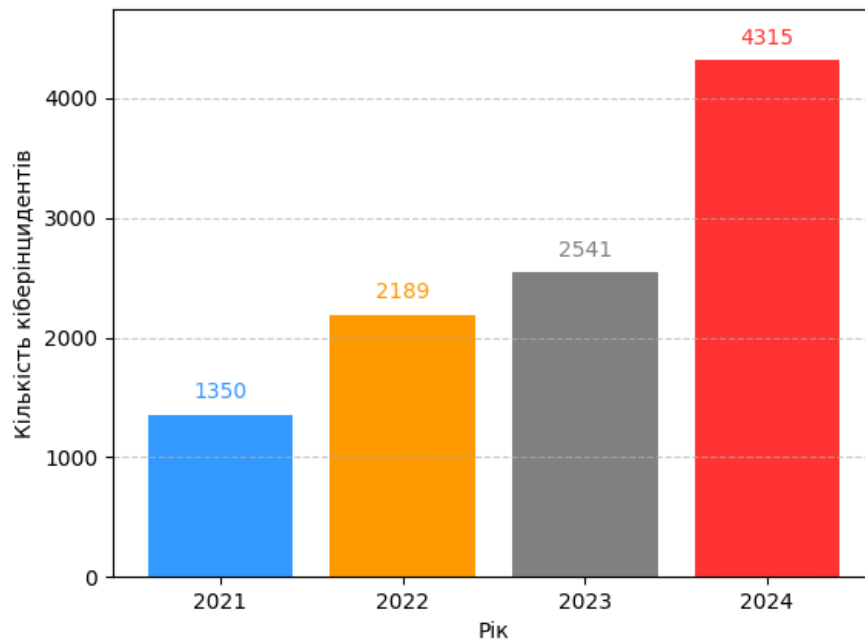


Рисунок 1.4 – Кількість кіберінцидентів за роками

На початок повномасштабної війни припало і утворення хакерського угруповання KillNet. Протягом квітня-вересня 2022 року ця група здійснила серію DoS- і DDoS-атак на державні установи та приватні компанії Румунії, Молдови, Чехії, Італії, Литви, Норвегії, Латвії, США, Японії, Грузії, Німеччини та України. Зловмисники навіть намагалися заблокувати сайт пісенного конкурсу “Євробачення” під час виступу України у травні 2022 року. Згодом атакували сайт Національної поліції України [31].

У наслідок цього, розвідувальний альянс “Five Eyes” (США, Великобританія, Австралія, Канада та Нова Зеландія) оприлюднив спільне попередження щодо кібербезпеки. Повідомлення закликає організації критичної інфраструктури негайно вжити заходів захисту, зокрема виправляти відомі уразливості, оновлювати програмне забезпечення, використовувати багатофакторну автентифікацію та посилювати моніторинг віддалених доступів [32].

У 2016 році, відбулась уже згадана атака на підстанцію "Північна" національної енергетичної компанії "Укренерго", а вже у 2022 році – атака на

високовольтні підстанції України з використанням нової версії – Industroyer2. Разом із ним зловмисники використали CaddyWiper – шкідливе ПЗ для знищення даних [33].

Окрім кібератак, здійснювались і фізичні атаки. Окупація української території Російською Федерацією призвела до втрати приблизно 18 гігават потужностей. Запорізька атомна електростанція, захоплена у березні 2022 року, раніше забезпечувала близько 20% потреб України в електроенергії. Великі теплові та гідроелектростанції на сході країни також суттєво підтримували енергосистему. Постійні бойові дії призводили до пошкодження ліній електропередач і підстанцій, що щоденно залишало без світла сотні тисяч людей у прилеглих населених пунктах.

До квітня 2023 року українська енергосистема втратила майже половину своєї доступної потужності через окупацію та руйнування. Крім того, було пошкоджено 45% автотрансформаторів класу 220-750 кВ, що ускладнило постачання електроенергії населенню. Взимку 2023-2024 років Україна могла виробляти лише 17,8 гігават електроенергії на годину, тоді як пікове споживання сягало 18,5 гігават на годину.

Якщо в 2022-2023 роках російські атаки здебільшого були спрямовані на об'єкти передачі електроенергії, то в 2024 році основна увага приділялася саме генеруючим потужностям. У 2024 році було пошкоджено втричі більше блоків ТЕС, ніж узимку 2022-2023 років. Також кількість атак на гідроелектростанції та дамби майже потроїлася [34].

Хакери, у свою чергу, почали використовувати більш точні та складні методи кібератак, які дедалі більше шкодять енергосистемі України.

Можна виділити декілька способів, за допомогою яких найчастіше відбуваються кібератаки:

- Фішингові листи, посилення та вкладення;
- ПЗ – кейлогери, що можуть не тільки викрадати паролі користувачів через

відстежування натискання клавіш, а й робити знімки екрана та викрадати облікові дані через віддалений доступ;

- ШПЗ, завантажене через сторонні сервіси/носії інформації.

Кількість і складність кібератак на системи критичної інфраструктури (зокрема на енергопідприємства) у світі та особливо в Україні, стрімко зростає. Вони еволюціонували від локальних шпигунських кампаній до масштабних операцій з серйозними економічними, соціальними та політичними наслідками. У таких складних умовах особливо важливо мати інструмент, що дозволить оцінити кіберрезильєнтність енергопідприємств за специфічними критеріями та надасть візуалізацію стану різних аспектів (фізичних, організаційних та технічних).

Висновки до розділу 1

Отже, кібервідмовостійкість – важливий аспект безпеки енергосистем та забезпечення безперебійного електропостачання. Дане поняття включає елементи кіберстійкості та відмовостійкості, що в загальному формує визначення – здатність інформаційних систем та організаційних процесів зберігати повну або часткову функціональність при виникненні внутрішніх збоїв або зовнішніх кіберзагроз, причому дає змогу системі працювати в непередбачених умовах, мінімізуючи наслідки та своєчасно відновлюючись до передінцидентного рівня.

Особливості енергосистем, які працюють на основі SCADA, WAMS та ін. технологіях, роблять їх вразливими до кібератак через низку специфічних особливостей. Аналіз кібератак на об'єкти критичної інфраструктури дозволив прослідкувати еволюцію від шпигунських кампаній до масштабних операцій із серйозними наслідками. Українська енергосистема є однією з головних цілей кібер- та фізичних атак через свою критичну важливість для функціонування держави. Приклади кібератак на енергопостачальні компанії світу та України

(зокрема BlackEnergy та Industroyer) демонструють необхідність розробки ефективних методів оцінювання та підвищення рівня захисту енергетичних підприємств.

Тому, актуальним завданням є розробка інструменту оцінки кіберрезильєнтності енергопідприємств, який у зручний для користувача спосіб (опитування) дозволить проаналізувати стан підприємства, обрахувати загальний рівень резильєнтності та візуалізувати стан фізичних, організаційних та технічних аспектів енергосистеми.

А отже, потребує оцінки питання: які методи та критерії будуть найбільш ефективними для оцінки кібервідмовостійкості енергосистем у реальних умовах експлуатації? Це питання розглянемо у другому розділі.

2 МЕТОДОЛОГІЯ ОЦІНКИ КІБЕРРЕЗИЛЬЄНТНОСТІ

2.1 Метрики стійкості

Оцінка кіберрезильєнтності енергопідприємства потребує системного підходу. Існує низка способів та підходів для її вимірювання. Майже всі з них охоплюють загальну ідею здатності системи протистояти несподіваним змінам, що включає: силу (міцність, *robustness*), замінність (*substitutability*, *redundancy*), системні та організаційні ресурси (для моніторингу, виявлення та захисту) та швидке відновлення (*rapidity*). У даному випадку використовуються метрики [35] – міри, які дозволяють отримати числове значення деяких властивостей системи, у нашому випадку оцінити кіберрезильєнтність підприємства. За основу візьмемо вже згаданий у розділі 1 підхід стійкості “чотирьох R”. Згідно з ним, систему слід вважати стійкою, якщо вона містить в собі міцність (*robustness*), надлишковість (*redundancy*), винахідливість (*resourcefulness*) і швидкість реагування (*rapidity*). При цьому:

- Міцність (*robustness*) – це здатність системи продовжувати виконувати свої безпосередні функції без значного/повного зниження рівня обслуговування під час кібератак або несподіваних змін;
- Надлишковість (*redundancy*) – це наявність холодних або гарячих резервних копій та реплікацій (програмного забезпечення) та дубльованих ресурсів (обладнання, каналів зв’язку, даних), які можуть замінити пошкоджені елементи;
- Винахідливість (*resourcefulness*) – це здатність організації ефективно і своєчасно моніторити, виявляти, аналізувати та комбінувати наявні ресурси для протидії новим кібератакам;
- Швидкість реагування (*rapidity*) – це здатність системи швидко виявляти інциденти та відновлювати нормальну роботу після збою або кібератаки.

На рисунку 2.1 показано елементи, від яких залежать стратегічні метрики [36].

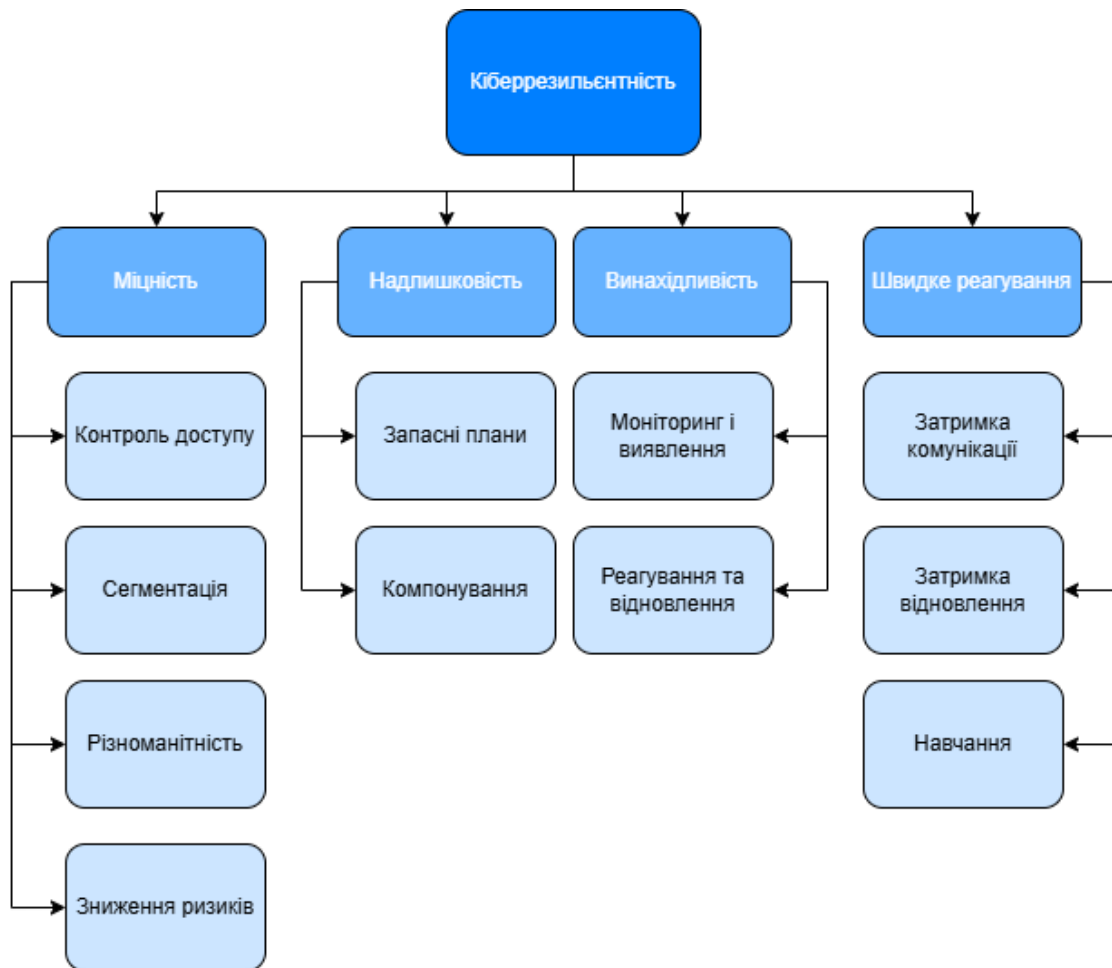


Рисунок 2.1 – Елементи стратегічних метрик

- Контроль доступу – набір заходів (ідентифікація/аутентифікація користувачів, політики доступу до RTU/PMU і сервісів SCADA та ін.), які керують несанкціонованим доступом до ресурсів енергосистеми;
- Сегментація – логічне та фізичне розподілення мережі, що обмежує поширення атак та мінімізує зону ураження;
- Різноманітність – використання пристроїв і ПЗ від різних вендорів та в декількох екземплярах;
- Зниження ризиків – набір заходів (оцінка вразливостей, аналіз ризиків та ін.), які зменшують ймовірність успішної кібератаки;
- Запасні плани – задокументовані та широко продумані сценарії та процедури

дій на випадок кіберінцидентів;

- Компонування – архітектурне поєднання основних та резервних елементів;
- Моніторинг і виявлення – неперервний збір і аналіз подій для оперативного знаходження аномалій;
- Реагування та відновлення – налагоджені дії реагування на інцидент, відновлення цілісності даних та повернення системи до робочого стану за мінімально можливий час;
- Затримка комунікації – показник часу від ініціації команди до отримання даних у центрі управління;
- Затримка відновлення – час між виявленням відмови/кібератаки та повним відновленням функціональності об'єкта;
- Навчання – збір знань після інцидентів (аналіз атак, оновлення процедур безпеки, тренінги за реальними кейсами) для покращення подальшого захисту та реагування.

Кожна із чотирьох стратегічних метрик поділяється на три доменні метрики та відповідні їм нижчі за рівнем підметрики (операційні метрики). Доменні метрики:

- Фізична – охоплює аспекти безпеки та витривалості фізичної інфраструктури (обладнання, пристрої, мережеві елементи, інженерні системи та ін.);
- Організаційна – фокусується на управлінських, процедурних і кадрових аспектах;
- Технічна – охоплює програмне та апаратне забезпечення, мережі та системи.

Детальніше про аспекти доменних метрик на рисунку 2.2 [36]:

Cyber Resilience Assessment Model			
	Фізичний	Організаційний	Технічний
Міцність	<p>Політика фізичного контролю доступу</p> <p>Ідентифікація загроз та вразливостей</p> <p>План пом'якшення наслідків вразливостей</p>	<p>Ідентифікація внутрішніх векторів загроз</p> <p>Система моніторингу</p> <p>Диверсифіковані продукти, ресурси тощо</p>	<p>Моніторинг портів, протоколів, трафіку тощо</p> <p>Пристрої захисту енергосистеми</p> <p>Модулі оцінки вразливостей і загроз</p>
Надлишковість	<p>Система резервного копіювання</p> <p>Різноманітність обладнання</p> <p>Фізична взаємодія між рівнями промислового керування</p>	<p>Планування та реалізація організаційної діяльності</p> <p>Впровадження нового організаційного процесу</p>	<p>План аварійного відновлення</p> <p>Впровадження нових технологій чи пристроїв</p> <p>Взаємодія та сумісність компонентів ПЗ</p>
Винахідливість	<p>Моніторинг фізичного середовища</p> <p>Виявлення аномальних подій і повідомлень</p> <p>Здатність відновлювати чи ремонтувати обладнання</p>	<p>Організаційний механізм реагування та відновлення</p> <p>Політика аудиту системи та управління змінами</p> <p>Процес розслідування внутрішніх загроз</p>	<p>Моніторинг журналу подій/системи</p> <p>Виявлення аномальної поведінки</p> <p>Динамічне налаштування конфігурації</p>
Швидкість реагування	<p>Швидкість перемикання операцій (затримка)</p> <p>Відновлення сервісів у короткий термін</p> <p>Механізми навчання та адаптації</p>	<p>Система управління та звітування про кібератаки</p> <p>Швидке розгортання альтернативної системи</p> <p>Швидкість відновлення системи</p>	<p>Швидкість виявлення, ізоляції та реагування на аномалії</p> <p>Швидкість системи аналізу та навчання</p>

Рисунок 2.2 – CRAM залежність між стратегічними та доменними метриками

Підметрики, що особливо важливі для енергопідприємств наведені на рисунку 2.3:



Рисунок 2.3 – Ієрархія метрик кіберрезильєнтності

Пояснення:

1. Фізичний контроль доступу – забезпечення суворої авторизації вхідних зон підстанцій і диспетчерських центрів за допомогою карт доступу, біометрії, тощо (для працівників та гостей);
2. Фізична різноманітність – розміщення резервних датчиків та виконавчих механізмів структуровано у різних фізичних локаціях, щоб зменшити ризик одночасного виведення з ладу цілого класу пристроїв;

3. Контроль доступу на основі ролей (RBAC) – побудова чіткого розподілу прав, щоб запобігти випадковим або зловмисним змінам у конфігураціях енергосистем;
4. Аудит та звітність – детальне логування усіх команд НМІ, доступів до серверів SCADA/WAMS, змін у прошивках PLC/RTU та з'єднаннях PMU;
5. Управління внутрішніми загрозами – моніторинг поведінки співробітників;
6. Сегментація мережі - відокремлення SCADA/WAMS від офісних і загальних ІТ-мереж за допомогою міжмережєвих екранів, VLAN, VPN-тунелів тощо;
7. Шифрування та аутентифікація зв'язку – використання протоколів, що шифрують трафік, а також забезпечення криптографічної автентифікації PMU-PDC;
8. Логічний контроль доступу – мультифакторна аутентифікація для входу в НМІ, EWS, PDC; часові обмеження сесій та жорсткі політики паролів для користувацьких та сервісних облікових записів;
9. Резервування пристроїв - дублювання критичного обладнання (PLC, RTU, PMU та ін.) у “гарячому” (hot-standby) режимі;
10. Резервування каналів зв'язку та джерел живлення – наявність альтернативних каналів зв'язку та джерел безперебійного живлення для кожної підстанції (або кожного сегменту);
11. План дій у надзвичайних ситуаціях – документовані процедури на випадок різноманітних інцидентів;
12. Політика управління змінами – документовані процедури тестування та впровадження оновлень та конфігурацій;
13. Резервне копіювання серверів та носіїв даних – автоматичні резервні копії конфігурацій систем;
14. Різноманітність вендорів – використання PLC, RTU, PMU та ін. від кількох виробників на випадок виявлення зловмисником вразливості на одній з них;
15. Фізичний моніторинг – відео- і сенсорне спостереження за ключовими

- елементами енергосистеми;
16. Захист даних – шифрування даних та збереження їх на окремих носіях; збереження історії подій і тривоги щоб не можна було видалити випадково чи навмисно;
 17. Централізований моніторинг та виявлення (SOC) – централізований SOC, який моніторить всі підстанції та агрегує логи WAMS;
 18. Організація реагування та відновлення – чіткі інструкції реагування на інциденти, відновлення та навчання них;
 19. Пом'якшення наслідків та аналіз – поінцидентний аналіз причин і наслідків (Root Cause Analysis), що веде до зміни політики безпеки та оновлення навчальних сценаріїв для персоналу;
 20. Ефективність внутрішнього спілкування - налагоджені канали спілкування між диспетчерами, інженерами та керівництвом для швидкого обміну інформацією під час інциденту;
 21. Система виявлення вторгнень (IDS) – IDS із сигнатурним та аномальним аналізом мережевих патернів протоколів SCADA/WAMS (Modbus, DNP3 тощо);
 22. Система оновлення та виправлення вразливостей – регулярне оновлення прошивок RTU/PMU та патчів ОС, що закривають виявлені уразливості CVE для ICS-компонентів;
 23. Реєстрація та аналіз інцидентів безпеки – накопичення та аналіз логів подій безпеки та проведення кореляційних запитів;
 24. Забезпечення фізичного доступу – розробка процедури швидкого доступу аварійних бригад до обладнання у надзвичайних ситуаціях;
 25. Безперебійна доступність – гарантування безперебійного швидкого доступу до необхідного обладнання;
 26. Управління надзвичайними ситуаціями – регламенти швидкої евакуації, переключення оперативного центру на резервну локацію та ін.;

27. Навчання та підвищення обізнаності – регулярні навчання для відпрацювання сценаріїв кібератак/інших надзвичайних ситуацій, щоб персонал міг одразу застосувати процедури реагування.;
28. Управління внутрішніми загрозами – швидке блокування скомпрометованих облікових записів, розслідування підозрілої діяльності та ін.;
29. Обробка та прийняття рішень на рівні системи – впровадження автоматизованих правил на випадок швидкого реагування при виявленні аномальних подій у SCADA/WAMS;
30. Мережеве широкомасштабне забезпечення зв'язку – використання резервних каналів з QoS-пріоритезацією трафіку SCADA, щоб команди керування та тривожні сповіщення завжди доставлялися навіть при збоях основної мережі.

На основі показників R4 було створено загальну структуру кіберрезильєнтності та розроблено методологію обчислення відповідних метрик стійкості, адаптованих до ІКС, у тому числі енергетичних підприємств.

2.2 Анкета для опитування

До основних способів проведення досліджень належать кількісні та якісні. Кількісні методи фокусуються на числових даних та статистиці, тоді як якісні методи на суб'єктивній оцінці респондента на рахунок того чи іншого питання. У цьому дослідженні дані для оцінки енергосистеми збираються якісним підходом шляхом опитування n експертів. Чому саме якісний підхід? Цей метод дозволяє вивчити питання (думку експерта або працівника енергопідприємства на рахунок конкретно поставленого запитання), які складно піддаються кількісній оцінці.

Для відображення якісних та кількісних властивостей на впорядковану множину чисел використовуються шкали вимірювання. Існує декілька основних шкал [37]:

- Номінальна (найменувань) – якісна шкала, змінні якої різняться одна від

одної, при цьому між ними немає упорядкованого чи величинного відношення; використовується для позначення приналежності до класів чи груп;

- Порядкова (ординальна) – якісна шкала, що впорядковує категорії за зростанням чи спаданням, проте не дозволяє кількісно оцінити інтервали між ними; використовується для приписування порядкового місця в класі чи групі;
- Інтервальна – кількісна шкала, що забезпечує рівномірні та інтерпретовані інтервали між значеннями; не має абсолютного нуля;
- Співвідношення – кількісна шкала з інтервалами та абсолютним нулем;, відображає у скільки разів властивість одного об'єкта переважає властивість іншого;
- Абсолютна – кількісна шкала, результати вимірювання якої – числа в звичайному значення цього слова.

Для оцінювання розробляється анкета-опитувальник з n-кількістю питань (про які буде йти мова пізніше), де питання згруповано відповідно до метрик, доменів та підметрик. Відповіді на питання оформлені за шкалою Лайкерта – інтервальною шкалою оцінювання, що використовується для вимірювання думок, ставлення учасників опитування; використовує ряд варіантів відповідей, починаючи від одного крайнього ставлення до іншого, а посередині – нейтральний варіант. Отже, у цій роботі використовується така шкала Лайкерта: Оцінка від користувача (від 1 до 5) (таблиця 2.1).

Таблиця 2.1 – Оцінка від користувача (1-5)

	Варіанти відповіді на питання				
Відповідь користувача	Повністю згоден	Переважно згоден	Частково згоден, частково не згоден	Переважно не згоден	Повністю не згоден
Змінна по шкалі Лайкерта	5	4	3	2	1

Відповідно до таблиці 2.1 варіанти відповіді “Повністю згоден”, “Переважно згоден”, “Частково згоден, частково не згоден”, “Переважно не згоден” та “Повністю не згоден” відповідають рівню згоди 100 %, 75 %, 50 %, 25 % та 0 % відповідно.

Описані вище речі реалізуються у розділі 3 у вигляді веб-застосунку з метою опитування експертів та працівників енергосистем, що містить відповідні питання по метрикам стійкості з відповідями за шкалою Лайкерта.

Для зручності кожна операційна метрика групується в блоки питань (тверджень) за принципом в таблиці 2.2 (операційні метрики синім, оранжевим, жовтим та червоним кольорами відповідають стратегічним метрикам міцність, надлишковість, винахідливість та швидкість реагування відповідно):

Таблиця 2.2 – Групування операційних метрик у блоки питань

Блок	Операційна метрика
Фізична безпека	Фізичний контроль доступу
	Фізична різноманітність
	Фізичний моніторинг
	Забезпечення фізичного доступу
Мережева безпека	Сегментація мережі
	Шифрування та аутентифікація зв'язку
	Мережеве широкомасштабне забезпечення зв'язку
Контроль доступу	Контроль доступу на основі ролей (RBAC)
	Логічний контроль доступу
Надійність і резервування	Резервування пристроїв
	Резервування каналів зв'язку та джерел живлення
	Резервне копіювання серверів та носіїв даних
	Різнманітність вендорів
	Безперебійна доступність
Моніторинг і виявлення	Аудит та звітність
	Централізований моніторинг та виявлення (SOC)
	Система виявлення вторгнень (IDS)
	Реєстрація та аналіз інцидентів безпеки
	Обробка та прийняття рішень на рівні системи

Кінець таблиці 2.2

Реагування на інциденти та відновлення	План дій у надзвичайних ситуаціях
	Організація реагування та відновлення
	Пом'якшення наслідків та аналіз
	Управління надзвичайними ситуаціями
	Управління внутрішніми загрозами
Організаційні заходи та політики	Політика управління змінами
	Ефективність внутрішнього спілкування
	Навчання та підвищення обізнаності
	Управління внутрішніми загрозами
Оновлення та захист систем	Захист даних
	Система оновлення та виправлення вразливостей

Відповідно до блоків формуються твердження, які зазначені у третьому розділі.

2.3 Обчислення вагових коефіцієнтів метрик

Для того, щоб максимально достовірно та точно розрахувати оцінку кіберрезильєнтності енергопідприємства для початку необхідно визначити важливість кожної метрики. Адже кожна метрика, домен та підметрика, з точки зору експертів, має різне значення. Тому, для того, щоб “урівноважити” їх використовується метод ієрархічного аналізу (Analytic Hierarchy Process – АНР), адаптований під R4 методологію. Метод ієрархічного аналізу [38] – структурований підхід до прийняття рішень, що поєднує експертні оцінки та математичні обчислення для вибору найкращого варіанту з-поміж альтернатив. Використовується алгоритм обчислення АНР взятий з [39], де парні порівняння m

критеріїв між собою формують матрицю C розміром $m \times m$. Кожний елемент матриці відображає суб'єктивне порівняння критеріїв C_i та C_j . Матриця парних порівнянь має вигляд:

$$C = \begin{pmatrix} 1 & C_{12} & \cdots & C_{1m} \\ 1/C_{12} & 1 & \cdots & C_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 1/C_{1m} & 1/C_{2m} & \cdots & 1 \end{pmatrix}, \quad (2.1)$$

де:

$$C_{ji} = \frac{1}{C_{ij}}, \quad (2.2)$$

Нормалізована матриця C_N знаходиться з матриці C , використовуючи обрахунки нижче:

$$C_N = \begin{pmatrix} C_N(1,1) & C_N(1,2) & \cdots & C_N(1,m) \\ C_N(2,1) & C_N(2,2) & \cdots & C_N(2,m) \\ \cdots & \cdots & \cdots & \cdots \\ C_N(m,1) & C_N(m,2) & \cdots & C_N(m,m) \end{pmatrix}, \quad (2.3)$$

де:

$$C_N(i,j) = \frac{C_{ij}}{\sum_{k=1}^m C_{kj}}, \quad (2.4)$$

Ваги критеріїв обчислюються як нормалізований правий власний вектор матриці C :

$$W = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix}, \quad (2.5)$$

де:

$$w_i = \frac{1}{m} \sum_{j=1}^m C_N(i,j), \quad (2.6)$$

Для перевірки узгодженості обчислень обчислюють коефіцієнт узгодженості (CR):

$$CR = \frac{CI}{RI}, \quad (2.7)$$

$$CI = \frac{\lambda_{\max} - m}{m - 1}, \quad (2.8)$$

$$\lambda_{\max} = \sum_{j=1}^m \left(\sum_{i=1}^m C_{ij} \right) \times w_i, \quad (2.9)$$

RI – випадковий індекс (таблиця 2.3) [40].

Таблиця 2.3 – Середній випадковий індекс (RI) на основі розміру матриці (n)

Розмір матриці (n)	Випадковий індекс (RI)
1	0,00
2	0,00
3	0,52
4	0,89
5	1,11
6	1,25
7	1,35
8	1,40
9	1,45

Кінець таблиці 2.3

10	1,49
11	1,51
12	1,48

Порівняння вважають прийнятним, якщо $CR \leq 0,1$.

Обрахунки та результати експертного оцінювання ваг метрик зазначені у розділі 3.

2.4 Обчислення загального показника кіберрезильєнтності

Для обчислення метрик кіберрезильєнтності було використано методологію [39]. Нехай $S_{i_{u_n}}$ позначає кількісне значення за шкалою Лайкерта відповіді на питання Q_i користувачем u_n .

Далі для кожної підметрики обраховується Expected Composite Score (ECS) [39] – зважене середнє балів відповідей користувачів (RS) для субметрики (або підметрики) SM , де SM залежить від відповідей на питання Q_1, \dots, Q_q , що обчислюється за такою формулою:

$$ECS_{M_D SM u_n} = \frac{1}{q} \sum_{i=1}^q S_{i_{u_n}}, \quad (2.10)$$

Потім ці результати агрегуються загальним комплексним балом Overall Composite Score (OCS) [39] – це геометричне середнє ECS n користувачів i позначається як $OCS_{M_D SM}$ для субметрики SM в межах метрики M та домену D та визначається за формулою:

$$OCS_{M_{DSM}} = \left[\prod_{j=1}^n ECS_{M_{DSM_{u_j}}} \right]^{1/n}, \quad (2.11)$$

Далі у кожному домені D для метрики M підметрики SM підсумовуються з урахуванням ваг (метод АНР) – $W_{M_{D_{SM_i}}}$. Тоді Domain Score (DS) [39] – бал домену для домену D за метрикою M, який дорівнює сумі добутків OCS підметрик на їхні ваги:

$$d_{M_D} = \sum_{i=1}^N OCS_{M_{DSM_i}} \times W_{M_{DSM_i}}, \quad (2.12)$$

Чотири основні метрики обчислюються як зважена сума доменних балів із вагами фізичного, організаційного та технічного доменів:

$$R_i = w_{\text{фіз}} * d_{R_{i_{\text{фіз}}}} + w_{\text{орг}} * d_{R_{i_{\text{орг}}}} + w_{\text{тех}} * d_{R_{i_{\text{тех}}}}, \quad (2.13)$$

Після цього кожна метрика нормалізується:

$$R_{iN} = \frac{R_i - 1}{4}, \quad (2.14)$$

Далі знаходимо критичну функціональність сервісу Critical Service Functionality (CSF) [39] – мінімальний очікуваний рівень обслуговування, який має підтримуватися системою у разі кібератаки, що залежить від міцності, надлишковості, винахідливості та швидкості реагування системи. Таким чином, CSF безпосередньо залежить від оцінки користувачем R4-метрик стійкості.:

$$CSF = SP_{\min} \sum_{i=1}^4 w_{r_i} \times R_{iN}, \quad (2.15)$$

Після інциденту рівень функціональності описується експоненційною моделлю:

$$Q_r(t) = (SP_{\min}) \times e^{rt}, \quad (2.16)$$

$$r = \frac{1}{T} \ln \left(\frac{1}{SP_{\min}} \right), \quad (2.17)$$

де T – розрахунковий період відновлення. $T = t_i^{cr} - t_i^{ri}$, t_i^{ri} – момент початку процесу відновлення після інциденту ($t_i^{ri} = 0$), t_i^{cr} – момент повного відновлення функціональності системи до вихідного рівня.

Звідси, кіберрезильєнтність системи визначається як середнє значення функціональності на проміжку від початку відновлення до моменту повного відновлення:

$$R = \frac{1}{T} \int_{t_i^{ri}}^{t_i^{cr}} Q_r(t) dt, \quad (2.18)$$

Спростуючи формулу 2.18 маємо:

$$R = \left(\frac{1}{T} \right) \left(\frac{1}{r} \right) SP_{\min} (e^{r \times T} - 1), \quad (2.19)$$

Підставивши формули 2.16 та 2.17 у 2.19 отримуємо загальну формулу обчислення кіберрезильєнтності:

$$R = \frac{1 - SP_{\min}}{\ln \frac{1}{SP_{\min}}}, \quad (2.20)$$

Висновки до розділу 2

У результаті проведеного дослідження у межах другого розділу було виокремлено та проаналізовано методологію якісного та кількісного оцінювання кіберрезильєнтності енергопідприємств.

За основу покладено методологію сейсмічної стійкості R4, адаптовану під критичну інфраструктуру, зокрема енергосистеми. Ієрархічна структура R4 охоплює три рівні: стратегічні метрики (міцність, надлишковість, винахідливість та швидкість реагування), доменні метрики (фізичні, організаційні та технічні) та сукупність із 30 операційних підметрик, детальніше розглянутих у цьому розділі.

Досліджено застосування методу аналізу ієрархій (АНР) для визначення вагових коефіцієнтів кожної метрики та передбачено проведення експертного опитування з метою отримання попарних порівнянь та їх подальшого перетворення у числові значення, що відображають відносну важливість кожної метрики.

Крім того, було досліджено механізм комбінування вагових коефіцієнтів для метрик, отриманих від експертів, та відповідей на питання від користувачів в анкеті-опитувальнику для обчислення загального рівня кіберрезильєнтності. Якісний збір даних у веб-застосунку буде організовано через опитувальник, де користувачі оцінюють твердження за п'ятибальною шкалою Лайкерта. Це дозволяє перетворити суб'єктивні відповіді респондентів на числові показники.

Таким чином, досліджено цілісну методологію оцінювання стійкості системи, що поєднує системний підхід, експертні оцінки та математичні алгоритми. На основі цього матеріалу в третьому розділі передбачено проведення експертного оцінювання вагових коефіцієнтів метрик та реалізацію веб-застосунку опитувальника, який автоматизує процес збору і обробки даних, обчислює загальний рівень кіберрезильєнтності енергопідприємства та надає візуалізацію результатів у вигляді діаграм.

3 ПРАКТИЧНІ РЕЗУЛЬТАТИ

3.1 Обчислення ваг за допомогою методу аналізу ієрархій (АНР)

Оскільки не всі метрики стійкості однаково важливі, було проведено опитування десяти експертів із кібербезпеки для визначення ваг за методом аналізу ієрархій (АНР). Усього було сформовано 148 попарних порівнянь стратегічних, доменних та операційних метрик. Опитування проводилося за початковою шкалою, яка надалі конвертувалася у шкалу Лайкерта (таблиця 3.1). Наведена нижче таблиця відображає відповідність між початковою шкалою оцінювання, шкалою Лайкерта та їхньою інтерпретацією:

Таблиця 3.1 – Відповідність шкал в опитуванні

Шкала в опитуванні	Шкала Лайкерта	Що означає?
4	5	Надзвичайно сильна перевага першої метрики
3	4	Сильна перевага першої метрики
2	3	Помірна перевага першої метрики
1	2	Слабка перевага першої метрики
0	1	Обидві метрики рівнозначні
1'	1/2	Слабка перевага другої метрики
2'	1/3	Помірна перевага другої метрики
3'	1/4	Сильна перевага другої метрики
4'	1/5	Надзвичайно сильна перевага другої метрики

Було визначено важливість фізичного, організаційного та технічного доменів за допомогою трьох попарних порівнянь, наведених нижче, використовуючи метод АНР, проілюстрований у попередньому розділі, та шкалу Лайкерта від 1 до 5.

Відповіді експертів мають вигляд (таблиця 3.2):

Таблиця 3.2 – Початкові відповіді експертів для доменних метрик

Відповіді експертів за шкалою 4-4'	Фізична vs Організаційна	Фізична vs Технічна	Організаційна vs Технічна
Експерт 1	4'	0	1
Експерт 2	2'	2'	1
Експерт 3	2	0	1'
Експерт 4	2	1'	3'
Експерт 5	2'	3'	0
Експерт 6	2'	2'	1'
Експерт 7	2'	1	1'
Експерт 8	3	0	1'
Експерт 9	2'	2	1
Експерт 10	3	0	1'

Після конвертації відповіді експерта мають такий вигляд (таблиця 3.3):

Таблиця 3.3 – Відповіді експертів для доменних метрик за шкалою Лайкерта

Відповіді експертів за шкалою 1-5	Фізична vs Організаційна	Фізична vs Технічна	Організаційна vs Технічна
Експерт 1	1/5	1	2
Експерт 2	1/3	1/3	2
Експерт 3	3	1	1/2
Експерт 4	3	1/2	1/4

Кінець таблиці 3.3

Експерт 5	1/3	1/4	1
Експерт 6	1/3	1/3	1/2
Експерт 7	1/3	2	1/2
Експерт 8	4	1	1/2
Експерт 9	1/3	3	2
Експерт 10	4	1	1/2

Далі геометричне середнє усіх парних порівнянь доменних метрик між собою формують матрицю порівнянь (з формул 2.1 та 2.2), яка має такий вигляд (таблиця 3.4):

Таблиця 3.4 – Матриця попарних порівнянь доменних метрик

Домени	Фіз	Орг	Тех
Фіз	1	21/26	39/50
Орг	26/21	1	72/95
Тех	50/39	95/72	1
Сума	3,5198	3,1274	2,5378

Нормалізована матриця (формули 2.3 та 2.4) з вагами W (формули 2.5 та 2.6) має такий вигляд (таблиця 3.5):

Таблиця 3.5 – Нормалізована матриця попарних порівнянь доменних метрик

ДомениN	Фіз	Орг	Тех	W
Фіз	0,2841	0,2583	0,3073	0,2833
Орг	0,3516	0,3197	0,2986	0,3233
Тех	0,3642	0,4219	0,3940	0,3934

Таким чином, $w_{\text{фіз}} = 0,28$, $w_{\text{орг}} = 0,32$ та $w_{\text{тех}} = 0,39$. $\lambda_{\text{max}} = 3,0065$ (за формулою 2.9); $m = 3$; коефіцієнт узгодженості (формула 2.7) $CR = 0,56\% \leq 10\%$, а отже попарне порівняння прийнятне та узгоджене.

Аналогічно обчислюються ваги для міцності (М), надлишковості (Н), винахідливості (В) та швидкості реагування (Ш) – стратегічних метрик. Для них усього 6 попарних порівнянь.

Відповіді експертів зазначені в таблиці 3.6:

Таблиця 3.6 – Початкові відповіді експертів для стратегічних метрик

Відповіді експертів за шкалою 4-4'	М vs Н	М vs В	М vs Ш	Н vs В	Н vs Ш	В vs Ш
Експерт 1	2	3	2'	2	3'	3
Експерт 2	3	1'	1	2'	2'	1
Експерт 3	0	2	3	2	0	2'
Експерт 4	2	3	0	1	2'	4'
Експерт 5	2	2'	3'	0	2'	0
Експерт 6	2	1'	0	2'	2'	0
Експерт 7	1	3	1	3	1	1'

Кінець таблиці 3.6

Експерт 8	1	1'	3	2'	3'	2'
Експерт 9	2	2	2	1'	1	1
Експерт 10	2	3	0	1	2'	3'

Сконвертовані відповіді зазначені в таблиці 3.7:

Таблиця 3.7 – Відповіді експертів для стратегічних метрик за шкалою Лайкерта

Відповіді експертів за шкалою 1-5	М vs Н	М vs В	М vs Ш	Н vs В	Н vs Ш	В vs Ш
Експерт 1	3	4	1/3	3	1/4	4
Експерт 2	4	1/2	2	1/3	1/3	2
Експерт 3	1	3	4	3	1	1/3
Експерт 4	3	4	1	2	1/3	1/5
Експерт 5	3	1/3	1/4	1	1/3	1
Експерт 6	3	1/2	1	1/3	1/3	1
Експерт 7	2	4	2	4	2	1/2
Експерт 8	2	1/2	4	1/3	1/4	1/3
Експерт 9	3	3	3	1/2	2	2
Експерт 10	3	4	1	2	1/3	1/4

Матриця попарних порівнянь (таблиця 3.8):

Таблиця 3.8 – Матриця попарних порівнянь стратегічних метрик

Метрики	М	Н	В	Ш
М	1	2 27/49	1 11/19	1 23/72
Н	20/51	1	1 10/97	1/2
В	19/30	68/75	1	52/71
Ш	72/95	1 95/96	1 19/52	1
Сума	2,7834	6,4470	5,0468	3,5546

Нормалізована матриця (таблиця 3.9):

Таблиця 3.9 – Нормалізована матриця попарних порівнянь стратегічних метрик

МетрикиN	М	Н	В	Ш	W
М	0,3593	0,3957	0,3128	0,3712	0,3597
Н	0,1408	0,1551	0,2186	0,1414	0,1640
В	0,2276	0,1406	0,1981	0,2061	0,1931
Ш	0,2723	0,3086	0,2705	0,2813	0,2832

Звідси, $w_M = 0,36$, $w_N = 0,16$, $w_B = 0,20$ та $w_{Ш} = 0,28$. $\lambda_{\max} = 4,0364$; $m = 4$; коефіцієнт узгодженості $CR = 1,35\% \leq 10\%$, а отже попарне порівняння прийнятне та узгоджене. Як видно, міцність та швидкість реагування найважливіші на думку експертів.

Аналогічно обчислюються ваги для операційних метрик. Відповідно відбувається 28 попарних порівнянь фізичних підметрик, 66 попарних порівнянь організаційних підметрик та 45 попарних порівнянь технічних підметрик. Для того,

щоб не проводити вручну такі обрахунки та не перенавантажувати розділ великими таблицями, було розроблено програмний код на мові Python (додаток А), який автоматизує обраховування матриці попарних порівнянь, принципового власного значення λ_{\max} та коефіцієнта узгодженості CR для всіх підметрик.

Для перевірки правильності роботи коду спочатку здійснимо обчислення в Excel та порівняємо результати для доменних метрик (рисунок 3.1):

Обчислення ваг для категорії «Доменні метрики» (3 метрик, 3 порівнянь)

Матриця попарних порівнянь для ['Фізична', 'Організаційна', 'Технічна']:

	Фізична	Організаційна	Технічна
Фізична	1.000000	0.807939	0.779977
Організаційна	1.237717	1.000000	0.757858
Технічна	1.282089	1.319508	1.000000

$\lambda_{\max} = 3.0065$, CI = 0.0033, CR = 0.0056

	Метрика	Вага
0	Фізична	0.2832
1	Організаційна	0.3233
2	Технічна	0.3935

Рисунок 3.1 – Обрахунки для доменних метрик

Як видно, усі обрахунки ідентичні тим, що в таблицях 3.4 та 3.5. А отже, можна розраховувати й інші (рисунок 3.2, 3.3 та 3.4).

Обчислення ваг для категорії «Фізичні підметрики» (8 метрик, 28 порівнянь)

Матриця попарних порівнянь для ['Фізичний контроль доступу', 'Фізична різноманітність', 'Резервування пристроїв',

	Фізичний контроль доступу	...	Безперебійна доступність
Фізичний контроль доступу	1.000000	...	0.459176
Фізична різноманітність	1.148698	...	0.343915
Резервування пристроїв	1.782602	...	0.851340
Резервування каналів зв'язку та джерел живлення	2.194641	...	1.196231
Фізичний моніторинг	0.794328	...	0.517925
Захист даних	1.834630	...	1.472733
Забезпечення фізичного доступу	0.715485	...	0.533041
Безперебійна доступність	2.177816	...	1.000000

[8 rows x 8 columns]

$\lambda_{\max} = 8.1122$, CI = 0.0160, CR = 0.0114

	Метрика	Вага
0	Фізичний контроль доступу	0.0870
1	Фізична різноманітність	0.0775
2	Резервування пристроїв	0.1528
3	Резервування каналів зв'язку та джерел живлення	0.1596
4	Фізичний моніторинг	0.0689
5	Захист даних	0.2002
6	Забезпечення фізичного доступу	0.0903
7	Безперебійна доступність	0.1636

Рисунок 3.2 – Обрахунки для фізичних підметрик

Звідси, найбільшу вагу за думками експертів мають захист даних, безперебійна доступність та резервування пристроїв, каналів зв'язку і джерел живлення. $\lambda_{\max} = 8,1122$; $m = 8$; коефіцієнт узгодженості $CR = 1,14\% \leq 10\%$.

Обчислення ваг для категорії «Організаційні підметрики» (12 метрик, 66 порівнянь)

Матриця попарних порівнянь для ['Контроль доступу на основі ролей (RBAC)', 'Аудит та звітність', 'Управління внутрішніми загрозами (1)', 'Контроль доступу на основі ролей (RBAC) ... Управління внутрішніми загрозами (2)']

	Контроль доступу на основі ролей (RBAC)	Аудит та звітність	Управління внутрішніми загрозами (1)
Контроль доступу на основі ролей (RBAC)	1.000000	0.870551	0.372504
Аудит та звітність	0.870551	1.000000	0.923254
Управління внутрішніми загрозами (1)	0.372504	0.923254	1.000000
План дій у надзвичайних ситуаціях	1.071773	1.148698	1.876028
Політика управління змінами	0.860357	1.148698	1.876028
Централізований SOC	1.148698	1.148698	1.876028
Організація реагування та відновлення	1.876028	1.148698	1.876028
Пом'якшення наслідків та аналіз	1.182224	1.148698	1.876028
Ефективність внутрішнього спілкування	0.860357	1.148698	1.876028
Управління надзвичайними ситуаціями	1.761730	1.148698	1.876028
Навчання та підвищення обізнаності	0.860357	1.148698	1.876028
Управління внутрішніми загрозами (2)	1.643752	1.148698	1.876028

[12 rows x 12 columns]

$\lambda_{\max} = 12.1228$, $CI = 0.0112$, $CR = 0.0073$

	Метрика	Вага
0	Контроль доступу на основі ролей (RBAC)	0.0761
1	Аудит та звітність	0.0902
2	Управління внутрішніми загрозами (1)	0.0354
3	План дій у надзвичайних ситуаціях	0.0962
4	Політика управління змінами	0.0582
5	Централізований SOC	0.1156
6	Організація реагування та відновлення	0.1071
7	Пом'якшення наслідків та аналіз	0.0766
8	Ефективність внутрішнього спілкування	0.0619
9	Управління надзвичайними ситуаціями	0.1151
10	Навчання та підвищення обізнаності	0.0664
11	Управління внутрішніми загрозами (2)	0.1012

Рисунок 3.3 – Обрахунки для організаційних підметрик

Таким чином, найбільша вага у централізованого моніторингу та виявлення, управління надзвичайними ситуаціями та організації реагування і відновлення. $\lambda_{\max} = 12,1228$; $m = 12$; коефіцієнт узгодженості $CR = 0,73\% \leq 10\%$.

Обчислення ваг для категорії «Технічні підметрики» (10 метрик, 45 порівнянь)

Матриця попарних порівнянь для ['Сегментація мережі', 'Шифрування та аутентифікація зв'язку', 'Логічний контроль доступу', 'Резервне копіювання серверів та носіїв даних', 'Різноманітність вендорів', 'Система виявлення вторгнень (IDS)', 'Система оновлення та виправлення вразливостей', 'Реєстрація та аналіз інцидентів безпеки', 'Обробка та прийняття рішень на рівні системи', 'Мережеве широкомасштабне забезпечення зв'язку']

	Сегментація мережі	...	Мережеве широкомасштабне забезпечення зв'язку
Сегментація мережі	1.000000	...	0.633538
Шифрування та аутентифікація зв'язку	1.447923	...	1.282089
Логічний контроль доступу	1.000000	...	0.895958
Резервне копіювання серверів та носіїв даних	1.643752	...	1.267077
Різноманітність вендорів	0.324283	...	0.350243
Система виявлення вторгнень (IDS)	1.169834	...	0.856852
Система оновлення та виправлення вразливостей	1.148698	...	0.794328
Реєстрація та аналіз інцидентів безпеки	1.597138	...	1.182224
Обробка та прийняття рішень на рівні системи	1.282089	...	0.719223
Мережеве широкомасштабне забезпечення зв'язку	1.578437	...	1.000000

[10 rows x 10 columns]
 $\lambda_{\max} = 10.0877$, $CI = 0.0097$, $CR = 0.0065$

	Метрика	Вага
0	Сегментація мережі	0.0834
1	Шифрування та аутентифікація зв'язку	0.1442
2	Логічний контроль доступу	0.1013
3	Резервне копіювання серверів та носіїв даних	0.1251
4	Різноманітність вендорів	0.0332
5	Система виявлення вторгнень (IDS)	0.0936
6	Система оновлення та виправлення вразливостей	0.1037
7	Реєстрація та аналіз інцидентів безпеки	0.1244
8	Обробка та прийняття рішень на рівні системи	0.0798
9	Мережеве широкомасштабне забезпечення зв'язку	0.1113

Рисунок 3.4 – Обрахунки для технічних підметрик

Як видно, найбільша важливість для шифрування і аутентифікації зв'язку, резервного копіювання серверів і носіїв даних та реєстрації і аналізу інцидентів безпеки. $\lambda_{\max} = 10,0877$; $m = 10$; коефіцієнт узгодженості $CR = 0,65\% \leq 10\%$.

Враховуючи вищевказані ваги всіх метрик, буде здійснюватися оцінка кіберрезильєнтності енергопідприємства в межах веб-застосунок.

3.2 Реалізація веб-застосунок

Було розроблено веб застосунок [41], що містить опитування для оцінки кіберрезильєнтності енергопідприємства. Клієнтська частина (front-end) – браузер користувача. Серверна частина не реалізована, оскільки робота зосереджена на аналізі та дослідженні методології оцінювання кіберрезильєнтності, тобто усі обчислення виконуються спрощено – локально в браузері.

Файлова архітектура проєкту зазначена на рисунку 3.5:

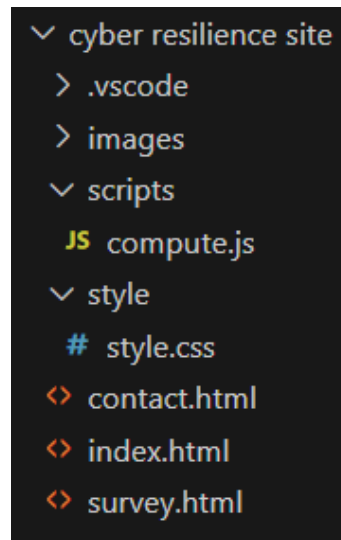


Рисунок 3.5 – Структура файлової системи веб-сайту для оцінки кіберрезильєнтності енергопідприємства

Де:

- .vscode – службова папка середовища VSCode з конфігураційними файлами;
- images – папка, що містить зображення для веб-сторінок;
- compute.js – скрипт із реалізацією алгоритму обчислення кіберрезильєнтності;
- style.css – стильове оформлення сторінки (кольори, шрифти тощо);
- index.html – головна сторінка сайту, що містить короткий опис про що цей проєкт та посилається на опитування;
- contact.html – сторінка контактів;
- survey.html – сторінка опитування (основний функціонал).

Основними файлами є survey.html, що відповідає за інтерфейс користувача та compute.js (додаток Б), що відповідає за реалізацію інтерактивності та логіки системи.

3.2.1 Опис survey.html

Сторінка поділена на логічні секції:

- Інструкція щодо використання сайту:

Перед початком опитування уважно ознайомтеся з цією інструкцією. Вона допоможе Вам правильно пройти опитування та отримати точні результати.

1. Ознайомлення з абрєвіатурами

Перед проходженням опитування **необхідно ознайомитися з абрєвіатурами**, які використовуються у питаннях. Це допоможе Вам краще зрозуміти зміст тверджень.

2. Вибір способу проходження опитування

Оберіть один із двох способів проходження опитування:

- **З вагами від експертів.** У цьому режимі всі ваги для стратегічних і доменних метрик встановлені на основі експертного оцінювання*. Вам не потрібно вводити жодних додаткових даних.
- **Задати ваги самостійно.** У цьому режимі ви зможете **самостійно** ввести ваги для стратегічних і доменних метрик, що дозволить налаштувати опитування під специфіку Вашого підприємства.

***Експертне оцінювання** — це метод, при якому ваги для метрик встановлюються на основі думок і досвіду фахівців у галузі кібербезпеки та енергетики.

3. Введення ваг (лише для режиму "Задати ваги самостійно")

Якщо Ви обрали **задати ваги самостійно**, Вам потрібно буде ввести ваги для:

- **Стратегічних метрик (R1, R2, R3, R4).** Введіть ваги для кожної з чотирьох метрик (Міцність, Надлишковість, Винахідливість, Швидкість реагування). Сума цих ваг повинна дорівнювати 1.

- **Доменних метрик (Фізичний, Організаційний, Технічний).** Введіть ваги для кожної з трьох метрик. **Сума цих ваг повинна дорівнювати 1.**

Важливо: Ваги для **30 операційних метрик** завжди беруться від експертів, незалежно від обраного режиму. Вам не потрібно вводити ці ваги задля швидкості та зручності проходження опитування.

4. Проходження опитування

Оцініть кіберрезильєнтність (кібервідмовостійкість) Вашого енергопідприємства за **8 розділами**: фізична безпека, мережева безпека, контроль доступу, надійність і резервування, моніторинг і виявлення, реагування на інциденти, організаційні політики, оновлення та захист.

Для кожного твердження оберіть одну з опцій:

- **Повністю згоден (100% згоди);**
- **Переважно згоден (75% згоди);**
- **Частково згоден, частково не згоден (50% згоди);**
- **Переважно не згоден (25% згоди);**
- **Повністю не згоден (0% згоди).**

Порада: Для максимально точних результатів відповідайте чесно за фактичним станом у компанії.

5. Результати опитування

Після завершення опитування ви отримаєте:

- **Загальну оцінку кіберрезильєнтності Вашого енергетичного підприємства;**

- **Радарні діаграми:** Показують оцінки операційних метрик для кожної стратегічної метрики (Міцність, Надлишковість, Винахідливість, Швидкість реагування) у відповідних доменах;
- **Кругову діаграму:** Ілюструє розподіл стратегічних метрик на основі Ваших відповідей;
- **Стовпчикову діаграму:** Відображає оцінки доменних метрик (Фізичний, Організаційний, Технічний) для кожної стратегічної метрики.
- Перелік використаних аббревіатур;
- Вибір способу проходження опитування (рисунок 3.6);

Оберіть спосіб проходження опитування:

Бажаю пройти опитування з вагами від експертів

Бажаю задати ваги самому

Продовжити

Рисунок 3.6 – Інтерфейс вибору способу проходження опитування

- Область введення ваг для метрик (опціонально) (рисунок 3.7);

Оберіть спосіб проходження опитування:

Бажаю пройти опитування з вагами від експертів

Бажаю задати ваги самому

Продовжити

Введіть ваги для стратегічних метрик:

Сума ваг для метрик Міцність (R1), Надлишковість (R2), Винахідливість (R3) та Швидкість реагування (R4) повинна дорівнювати 1.

Міцність (R1)	Міцність (robustness) – це здатність системи продовжувати виконувати свої безпосередні функції без значного/повного зниження рівня обслуговування під час кібератак або несподіваних змін.	0,01
Надлишковість (R2)	Надлишковість (redundancy) – це наявність холодних або гарячих резервних копій та реплікацій (програмного забезпечення) та дубльованих ресурсів (обладнання, каналів зв'язку, даних), які можуть замінити пошкоджені елементи.	
Винахідливість (R3)	Винахідливість (resourcefulness) – здатність організації ефективно і своєчасно моніторити, виявляти, аналізувати та комбінувати наявні ресурси для протидії новим кібератакам.	
Швидкість реагування (R4)	Швидкість реагування (rapidity) – це здатність системи швидко виявляти інциденти та відновлювати нормальну роботу після збою або кібератаки.	

Введіть ваги для доменних метрик:

Сума ваг для Фізичного, Організаційного та Технічного доменів повинна дорівнювати 1.

Фізичний домен	Охоплює аспекти безпеки та витривалості фізичної інфраструктури (обладнання, пристрої, мережеві елементи, інженерні системи та ін.).	
Організаційний домен	Фокусується на управлінських, процедурних і кадрових аспектах.	
Технічний домен	Охоплює програмне та апаратне забезпечення, мережі та системи.	

Зберегти ваги

Рисунок 3.7 – Інтерфейс введення користувацьких ваг для стратегічних та доменних метрик

- Форма опитування (фрагмент на рисунку 3.8), складається з тверджень:
- Фізична безпека
 - У нашій енергокомпанії фізичний доступ до об'єктів (підстанцій, диспетчерських центрів тощо) суворо контролюється (наприклад, за допомогою пропускних систем, біометрії);
 - Резервні датчики та виконавчі пристрої критичних підстанцій розміщені в різних фізичних локаціях, що мінімізує ризик одночасної відмови всього класу обладнання;
 - Ключові елементи енергосистеми знаходяться під постійним фізичним наглядом (відеоспостереженням, сенсорними сигналами);
 - У разі надзвичайної ситуації існує чітка процедура швидкого фізичного

доступу аварійних груп до критичного обладнання (швидке відмикання дверей, ключі резервного доступу тощо).

- **Мережева безпека**

- Мережі промислового контролю (SCADA/WAMS) відокремлені від корпоративних мереж за допомогою сегментації (VLAN, міжмережеві екрани тощо);
- Уся комунікація між пристроями енергосистеми (WAMS-SCADA, PMU-PDC тощо) захищена за допомогою шифрування та криптографічної аутентифікації;
- Для мережевих каналів SCADA запроваджено резервні канали з QoS-пріоритезацією трафіку управління та тривожних повідомлень, щоб забезпечити їх доставку навіть у разі відмови основної мережі.

- **Контроль доступу**

- Згідно корпоративної політики безпеки всі співробітники мають лише ті права доступу, які відповідають їхнім ролям (RBAC), і не можуть змінювати конфігурації енергосистем поза своїми повноваженнями;
- Доступ до HMI/EWS/PDC/SCADA-серверів та інших критичних ресурсів вимагає мультифакторної аутентифікації з часовими обмеженнями сесій та суворих політик паролів.

- **Надійність і резервування**

- Критичне обладнання (PLC/RTU/PMU) дублюється у режимі гарячого резерву (hot-standby) для автоматичного переключення у разі відмови першого пристрою;
- Кожен критичний вузол енергосистеми має альтернативний канал зв'язку та резервне джерело живлення;

- Конфігураційні файли SCADA-серверів та критичних даних регулярно автоматично резервуються та зберігаються у безпечному місці;
 - В енергосистемі використовуються пристрої RTU/PLC/PMU та ін. від кількох виробників задля зниження ризику однотипних вразливостей;
 - Гарантується безперебійний та швидкий доступ до необхідного обладнання у будь-який час.
- Моніторинг і виявлення
 - Ведеться детальне логування всіх команд в HMI, доступів до серверів SCADA/WAMS та змін у прошивках PLC/RTU і з'єднаннях PMU; ці журнали регулярно аналізуються для виявлення незвичних активностей;
 - Працює централізований центр моніторингу безпеки (SOC), який збирає логи та події з усіх підстанцій та виконує їх кореляцію для оперативного виявлення загроз;
 - У мережах SCADA/WAMS використовується система виявлення вторгнень з аналізом специфічних протоколів (наприклад, Modbus, DNP3) та аналізом аномалій трафіку;
 - Усі інциденти безпеки документуються, а відповідні логи подій ретельно аналізуються для встановлення причин та ризиків їх повторення;
 - Система автоматично застосовує заздалегідь налаштовані правила реагування при виявленні аномалій у SCADA/WAMS (наприклад, відключає компрометований компонент).
 - Реагування на інциденти та відновлення
 - У нашій компанії існують задокументовані плани та процедури дій на випадок кібератак та інших надзвичайних ситуацій з деталізованими

- кроками для кожного рівня (оператори, IT, керівництво);
 - Команди реагування на інциденти чітко сформовані з призначеними ролями, а відновлення систем після атаки відбувається згідно затверджених процедур;
 - Після інциденту проводиться ретельний аналіз причин та наслідків (Root Cause Analysis) з подальшим оновленням політики безпеки та покращенням сценаріїв навчання персоналу;
 - У нашій компанії діє система управління надзвичайними ситуаціями, що містить регламенти швидкого переключення диспетчерського центру на резервну локацію, евакуації персоналу при критичних інцидентах тощо;
 - Негайно блокуються скомпрометовані облікові записи та розпочинається розслідування при підозрілих діях співробітників.
- Організаційні заходи та політики
 - Поведінка співробітників моніториться для виявлення внутрішніх загроз та ризиків інсайдерів;
 - Усі зміни конфігурацій SCADA/WAMS та глобальні оновлення ПЗ проходять формалізований процес з тестуванням у відокремленому середовищі та затвердженням згідно з політикою управління змінами;
 - В установі налаштовані надійні канали внутрішнього зв'язку між диспетчерами, інженерами та керівництвом (рації, телекомунікації, чати) для оперативного обміну інформацією під час інцидентів;
 - Персонал регулярно проходить навчання та тренінги з відпрацювання сценаріїв кібер- та інших атак, щоб мати готові алгоритми реагування.
- Оновлення та захист систем
 - Критичні дані систем (бази даних SCADA, конфігурації системи тощо)

зберігаються зашифрованими та доступні лише обмеженому колу авторизованих осіб;

- Програмне забезпечення та операційні системи критичних ресурсів регулярно оновлюються останніми патчами, що закривають відомі вразливості ICS.

1. Фізична безпека

1.1: У нашій енергокомпанії фізичний доступ до об'єктів (підстанцій, диспетчерських центрів тощо) суворо контролюється (наприклад, за допомогою пропускних систем, біометрії).

<input type="radio"/> Повністю згоден	<input type="radio"/> Переважно згоден	<input type="radio"/> Частково згоден, частково не згоден	<input type="radio"/> Переважно не згоден	<input type="radio"/> Повністю не згоден
---------------------------------------	--	---	---	--

1.2: Резервні датчики та виконавчі пристрої критичних підстанцій розміщені в різних фізичних локаціях, що мінімізує ризик одночасної відмови всього класу обладнання.

<input type="radio"/> Повністю згоден	<input type="radio"/> Переважно згоден	<input type="radio"/> Частково згоден, частково не згоден	<input type="radio"/> Переважно не згоден	<input type="radio"/> Повністю не згоден
---------------------------------------	--	---	---	--

1.3: Ключові елементи енергосистеми знаходяться під постійним фізичним наглядом (відеоспостереженням, сенсорними сигналами).

<input type="radio"/> Повністю згоден	<input type="radio"/> Переважно згоден	<input type="radio"/> Частково згоден, частково не згоден	<input type="radio"/> Переважно не згоден	<input type="radio"/> Повністю не згоден
---------------------------------------	--	---	---	--

1.4: У разі надзвичайної ситуації існує чітка процедура швидкого фізичного доступу аварійних груп до критичного обладнання (швидке відмикання дверей, ключі резервного доступу тощо).

<input type="radio"/> Повністю згоден	<input type="radio"/> Переважно згоден	<input type="radio"/> Частково згоден, частково не згоден	<input type="radio"/> Переважно не згоден	<input type="radio"/> Повністю не згоден
---------------------------------------	--	---	---	--

Рисунок 3.8 – Приклад запитань у формі опитування для оцінювання кіберрезильєнтності енергосистеми

- Область виведення результатів та графіків.

3.2.2 Опис compute.js

Вміст compute.js:

- Структура метрик (чотири стратегічні метрики, що розбиті на три домени та на їхні операційні підметрики);
- Ваги метрик (задані експертним оцінюванням із розділу 3.1);
- Функції для збору та обробки відповідей респондента:

- Функція зчитування відповідей та збору всіх відповідей;
- Функція обчислення ECS (рисунок 3.9);

```
// === Обчислення ECS ===
function computeECS(answersForSM) {
  const sum = answersForSM.reduce((acc, v) => acc + v, 0);
  return sum / answersForSM.length;
}
```

Рисунок 3.9 – Функція обчислення зваженого середнього балів відповідей користувачів

- Функція обчислення DS (рисунок 3.10);

```
// === Обчислення DS ===
function computeDomainScore(Rkey, domainKey, allAnswers) {
  let ds = 0;
  for (let sm of metricsStructure[Rkey][domainKey]) {
    const smName = sm.name;
    const answersForSM = allAnswers[Rkey][smName];
    const ecs = computeECS(answersForSM);
    const wSM = submetricsWeights[Rkey][domainKey][smName] || 0;
    ds += ecs * wSM;
  }
  return ds;
}
```

Рисунок 3.10 – Функція обчислення балу домену для домену D

- Функція обчислення R_i та її нормалізації (рисунок 3.11);

```
// === Обчислення Ri (до нормалізації) ===  
function computeCi(Rkey, allAnswers) {  
  const dsPhys = computeDomainScore(Rkey, 'Physical', allAnswers);  
  const dsOrg = computeDomainScore(Rkey, 'Organizational', allAnswers);  
  const dsTech = computeDomainScore(Rkey, 'Technical', allAnswers);  
  
  let wPhys, wOrg, wTech;  
  if (Object.keys(userDomainWeights).length > 0) {  
    wPhys = userDomainWeights['Physical'];  
    wOrg = userDomainWeights['Organizational'];  
    wTech = userDomainWeights['Technical'];  
  } else {  
    wPhys = domainWeights.Physical;  
    wOrg = domainWeights.Organizational;  
    wTech = domainWeights.Technical;  
  }  
  
  return wPhys * dsPhys + wOrg * dsOrg + wTech * dsTech;  
}  
  
// === Нормалізація Ri у [0..1] ===  
function normalizeCi(ci) {  
  return (ci - 1) / 4;  
}
```

Рисунок 3.11 – Функція обчислення чотирьох основних метрик

- Функція обчислення CSF (рисунок 3.12);

```
// === Обчислення CSF ===
function computeCSF(allCiN) {
  let csf = 0;
  for (let Rkey of Object.keys(strategicWeights)) {
    let wRi;
    if (Object.keys(userStrategicWeights).length > 0) {
      wRi = userStrategicWeights[Rkey];
    } else {
      wRi = strategicWeights[Rkey];
    }
    const ciN = allCiN[Rkey];
    csf += wRi * ciN;
  }
  return csf;
}
```

Рисунок 3.12 – Функція обчислення мінімального очікуваного рівня обслуговування

- Функція обчислення кіберрезильєнтності R (рисунок 3.13);

```
// === Обчислення R ===
function computeResilienceR(csf) {
  return (1 - csf) / Math.log(1 / csf);
}
```

Рисунок 3.13 – Функція обчислення загального рівня кіберрезильєнтності енергопідприємства

- Відображення результатів:
 - Функція для радарних діаграм;
 - Функція для кругової діаграми;
 - Функція для стовпчикової діаграми;
- Обробники подій:
 - Обробник кнопки “Продовжити” – при виборі способу опитування;

- Обробник кнопки “Зберегти ваги” – збирає числові поля для стратегічних та доменних метрик та перевіряє необхідні умови;
- Обробник кнопки “Відправити відповіді” – перевіряє наповненість, обчислює метрики, візуалізує діаграми та показує результати.

3.2.3 Перевірка обчислень

Для перевірки правильності реалізації обчислень змодельємо проходження опитування користувачем і порівняємо результати з “еталонними” розрахунками у Excel.

На веб-сторінці виведемо результати обчислення деяких обрахованих значень після проходження опитування (рисунок 3.14):

Результати обчислення кіберрезильєнтності

Стратегічна (R _i) метрика	Значення R _i (1–5)	Нормалізоване R _{iN} (0–1)
R1	4.377	0.844
R2	3.364	0.591
R3	4.130	0.783
R4	3.932	0.733

CSF (Critical Service Functionality): 0.759

Загальний рівень кіберрезильєнтності Вашого енергопідприємства R: 0.874

Рисунок 3.14 – Результати обчислення кіберрезильєнтності за експертними вагами

Ті самі відповіді користувача було оброблено вручну за допомогою Excel. Використовуючи ваги для усіх метрик від експертів (з розділу 3.1) та формули 2.13, 2.14, 2.15 та 2.20 було перевірено правильність машинного обчислення. Як бачимо з таблиці 3.10 (містить частину обрахунків), значення R_i , R_{iN} , CRF та загальний рівень кіберрезильєнтності R абсолютно точно сходяться. А отже, обрахунки на веб-сторінці виконуються правильно.

Таблиця 3.10 – Фрагмент перевірки обчислень за експертними вагами

R1-R4	Домен	Підметрика	Відп.	W(SM)	DS	Ri	RiN	CSF	R
R1	Фізичний	Фізичний контроль доступу	5	0,5289	4,5289	4,377	0,844	0,759	0,874
		Фізична різноманітність	4	0,4711					
	Організаційний	Контроль доступу на основі ролей	5	0,3773	4,5528				
		Аудит та звітність	4	0,4472					
		Управління внутрішніми загрозами 1	5	0,1755					
	Технічний	Сегментація мережі	5	0,2536	4,1231				
		Шифрування та аутентифікація	3	0,4384					
		Логічний контроль доступу	5	0,3080					

Також сайт має функціонал вибору ваг стратегічних та доменних метрик користувачем самостійно. При цьому ваги операційних метрик завжди залишаються від експертів. Припустимо, що респондент бажає поставити однакові ваги для усіх стратегічних (по 0.25 кожній) та усіх доменних (по 0.33 кожній) метрик. Перевіримо правильність обчислення для таких даних. При цьому, відповіді користувача будуть такими ж, як і при минулій перевірці, результати відображені на рисунку 3.15 та подані в таблиці 3.11:

Результати обчислення кіберрезильєнтності

Стратегічна (Ri) метрика	Значення R _i (1–5)	Нормалізоване R _{IN} (0–1)
R1	4.403	0.851
R2	3.368	0.592
R3	4.169	0.792
R4	4.047	0.762

CSF (Critical Service Functionality): 0.749

Загальний рівень кіберрезильєнтності Вашого енергопідприємства R: 0.869

Рисунок 3.15 – Результати обчислення кіберрезильєнтності за користувацькими вагами

Таблиця 3.11 – Фрагмент перевірки обчислень за користувацькими вагами

R1-R4	Домен	Підметрика	Відп.	W(SM)	DS	Ri	RiN	CSF	R
R1	Фізичний	Фізичний контроль доступу	5	0,5289	4,5289	4,403	0,851	0,749	0,869
		Фізична різноманітність	4	0,4711					
	Організаційний	Контроль доступу на основі ролей	5	0,3773	4,5528				
		Аудит та звітність	4	0,4472					
		Управління внутрішніми загрозами 1	5	0,1755					
	Технічний	Сегментація мережі	5	0,2536	4,1231				
		Шифрування та аутентифікація	3	0,4384					
		Логічний контроль доступу	5	0,3080					

Бачимо з рисунка 3.15 та таблиці 3.11, що значення R_i , R_{iN} , CRF та загальний рівень кіберрезильєнтності R ідентичні. Отже, практичні результати сходяться з еталонними та код працює правильно.

3.3 Візуалізація результатів

Розроблений веб-застосунок виконує обчислення загальної кіберрезильєнтності та її основних компонентів. У результаті користувач, що проходить опитування отримує не лише оцінку загальної кіберрезильєнтності, а й детальну інформацію щодо всіх існуючих метрик/доменів/підметрик. Дана інформація є надзвичайно корисною для керівників енергопідприємств, оскільки допомагає визначити області, на які слід зосередити увагу з метою покращення загальної ситуації з кіберрезильєнтністю.

На рисунку 3.16 наведено приклад радарної діаграми для підметрик Міцності (R1), що показує оцінки восьми підметрик на основі відповідей користувача. Нумерація від 1 до 5 позначає рівні оцінювання, де 1 – мінімальний рівень реалізації або підтримки конкретного механізму, а 5 – максимальний. Такий вигляд радарної діаграми дозволяє швидко побачити, у яких аспектах “Міцність” системи найбільш розвинена, а де необхідне подальше вдосконалення.



Рисунок 3.16 – Приклад радарної діаграми для підметрик Міцності (R1)

На рисунку 3.17 відображено кругову діаграму, на якій показано відносні ваги чотирьох ключових стратегічних метрик у загальній оцінці кіберрезильєнтності. Кожному сектору відповідає власний колір та своя оцінка, розрахована за результатами опитування та за формулами з розділу 2. Завдяки такій візуалізації можна легко побачити який саме показник потребує першочергового вдосконалення.

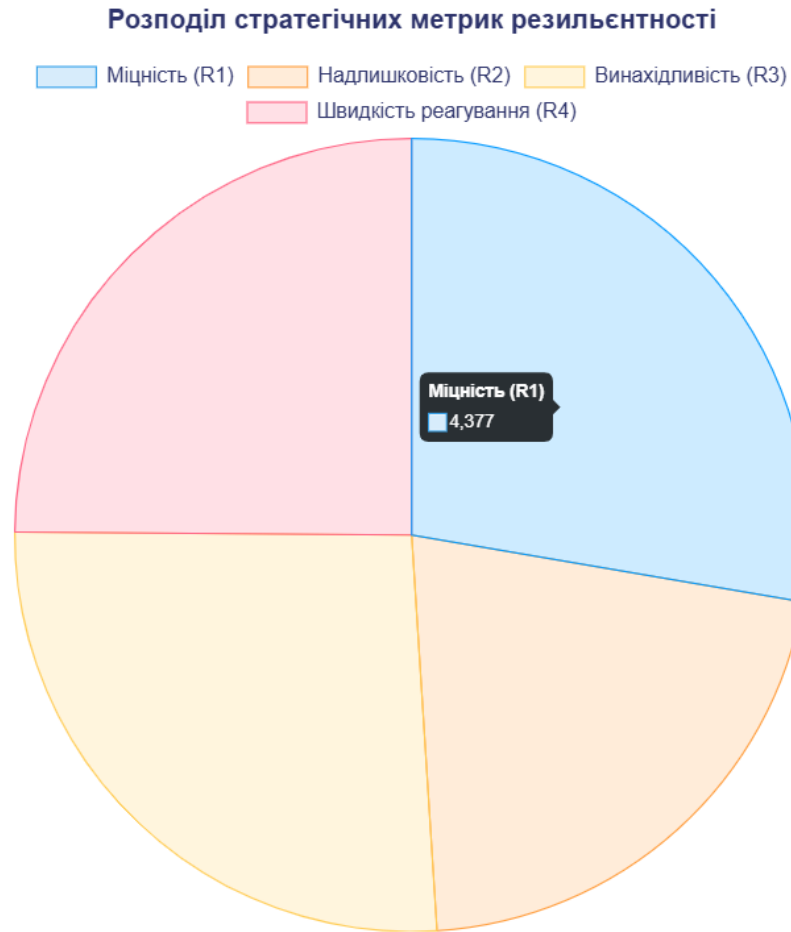


Рисунок 3.17 – Приклад кругової діаграми стратегічних метрик кіберрезильєнтності

На рисунку 3.18 наведено приклад стовпчикової діаграми, що показує оцінку для кожного домену (фізичний, організаційний, технічний) у межах відповідної стратегічної метрики. На ній одразу видно, в яких доменах є прогалини, і це допомагає керівникам спрямувати ресурси у правильному напрямі для поступового підвищення загальної кіберрезильєнтності.

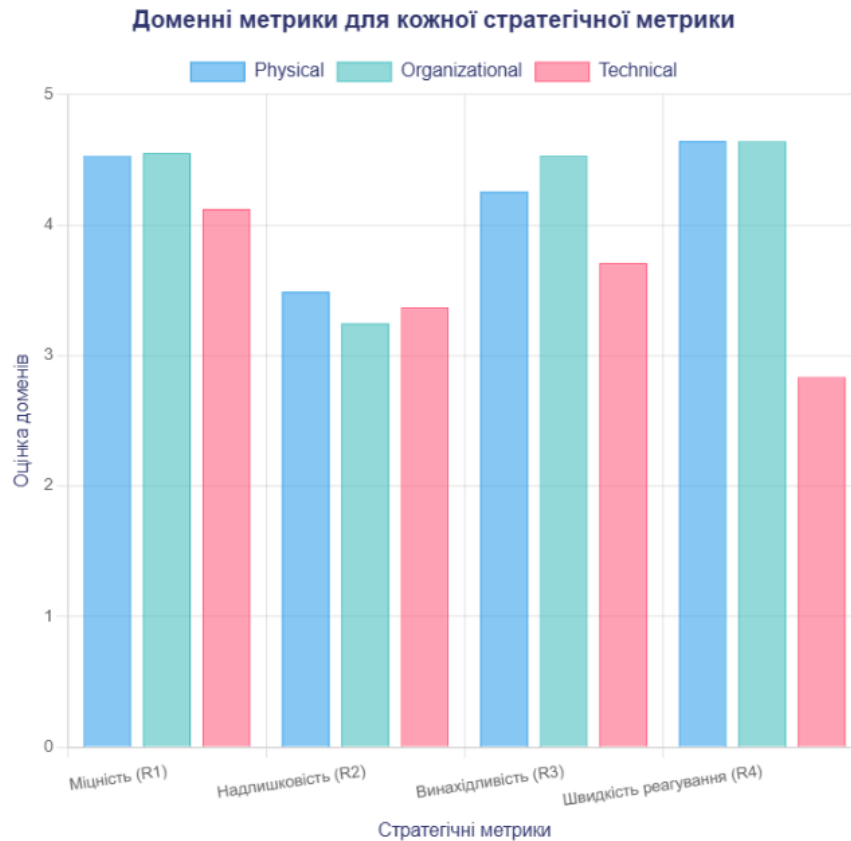


Рисунок 3.18 – Приклад стовпчикової діаграми доменних метрик

Висновки до розділу 3

У рамках третього розділу було виконано декілька етапів роботи.

По-перше, проведено експертне оцінювання вагових коефіцієнтів метрик. Було залучено десять фахівців у сфері кібербезпеки та енергосистем для попарного порівняння стратегічних, доменних та операційних метрик. Використано метод аналізу ієрархій (АНР) для формування матриць попарних порівнянь, обчислення власних векторів та перевірки узгодженості. Також для автоматизації обчислень було розроблено код на мові програмування Python, який генерує матриці попарних порівнянь для 148 зв'язків між метриками, обчислює власний вектор і коефіцієнт

узгодженості для всіх підметрик. Коректність обчислень перевірено шляхом порівняння результатів з ручними обчисленнями в Excel.

По-друге, реалізовано веб-застосунок для проведення опитування працівників (переважно керівництва) енергопідприємств. Створено клієнтську частину, що містить інтерфейс з інструкцією щодо проходження, вибором режиму опитування (експертні ваги або власні ваги користувача) та формою з 30 твердженнями з відповідями за шкалою Лайкерта. При цьому, JavaScript модуль забезпечує обчислення ECS, DS, Ri, нормалізації метрик, CSF та загального показника R згідно з формулами з розділу 2. Коректність обчислень так само перевірено шляхом порівняння з результатами в Excel.

Для зручності забезпечено два режими проходження опитування: за експертними вагами – усі ваги беруться з результатів АНР, користувач обирає лише відповіді на твердження; за власними вагами – користувач задає ваги для чотирьох стратегічних та трьох доменних метрик, тоді як ваги для операційних метрик залишаються експертними (для швидкості проходження опитування).

Нарешті, після завершення опитування, користувач отримує візуалізацію результатів у вигляді діаграм: радарні (розподіл операційних метрик у межах кожної стратегічної метрики), кругову (розподіл ваг стратегічних метрик) та стовпчикову (порівняння доменних метрик для кожної зі стратегічних). Візуалізація дозволяє керівникам енергопідприємств швидко виявити слабкі місця та пріоритетні напрями вдосконалення кіберрезильентності.

ВИСНОВКИ

У ході виконання роботи було успішно реалізовано комплексний інструментарій оцінювання кіберрезильєнтності енергопідприємств, що включає теоретичне обґрунтування, методологічні дослідження та практичну реалізацію.

Було детально вивчено поняття кіберрезильєнтності та розглянуто його складові. Досліджено особливості енергосистем із урахуванням специфіки SCADA та WAMS. Аналіз еволюції кібератак на критичну інфраструктуру світу та України дозволив підтвердити актуальність роботи.

Досліджено модель стійкості R4, адаптовану саме для енергопідприємств. За основу взято ієрархічну структуру метрик: стратегічні (міцність, надлишковість, винахідливість, швидкість реагування), доменні (фізичні, організаційні, технічні) та 30 операційних підметрик.

Проаналізовано комбінований підхід, що поєднує експертне оцінювання вагових коефіцієнтів метрик методом аналізу ієрархій (АНР), анкетне опитування за п'ятибальною шкалою Лайкерта та спосіб перетворення зібраних даних у загальний показник кіберрезильєнтності.

Для проведення експертної оцінки було залучено десять фахівців з кібербезпеки, які виконали попарне порівняння метрик. Результати було оброблено за допомогою скрипта Python.

Було розроблено веб-застосунок опитувальник, який дозволяє користувачеві (керівнику підприємства) обирати між режимом “експертних ваг” та “власних ваг”, вводити відповіді на 30 тверджень за шкалою Лайкерта та автоматично обчислювати ключові показники згідно з дослідженою методологією.

Забезпечено генерацію радарних, кругових та стовпчикових діаграм, які відображають розподіл метрик відповідно до результатів проходження опитування.

Отже, проведене експертне оцінювання гарантує, що вагові коефіцієнти метрик відображають найважливіші компоненти системи. Якщо ж керівник має власне бачення та пріоритети, передбачено ручне введення цих вагових коефіцієнтів. Автоматизація обрахунків робить процес оцінки більш швидким, зручним для респондента та універсальним для енергопідприємств. А візуалізація результатів дозволяє швидко побачити сильні й слабкі сторони у різних площинах. Це сприяє більш обґрунтованому прийняттю управлінських рішень та підвищенню загального рівня кіберрезильєнтності енергопідприємства.

ПЕРЕЛІК ДЖЕРЕЛ І ПОСИЛАНЬ

1. Левашова С. Д. Методика оцінювання кіберрезильєнтності енергопідприємства / С. Д. Левашова, Л. Ю. Гальчинський // XXIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених: Математичні методи кібернетичної безпеки, Київ, 2025 р. – С. 242–245. – Режим доступу: <http://conf.ipt.kpi.ua/archiv/2025-2/>.
2. Летяк В. Дефіцит електрики — Україна відчуватиме до кінця 2025-го: у МВФ оцінили наслідки атак РФ [Електронний ресурс] / Факти ICTV — Режим доступу: <https://fakty.com.ua/ua/ukraine/ekonomika/20240630-deficyt-elektryky-ukrayina-vidchuvatyme-do-kinczya-2025-u-mvf-oczinyly-naslidky-atak-rf/>.
3. National Infrastructure Advisory Council. NIAC Framework for Establishing Resilience Goals: Final Report and Recommendations [Електронний ресурс] / National Infrastructure Advisory Council; Cybersecurity & Infrastructure Security Agency (CISA). – Revision Date: 17 грудня 2020. – Режим доступу: <https://www.cisa.gov/resources-tools/resources/niac-framework-establishing-resilience-goals-final-report-and>.
4. National Research Council. Disaster Resilience: A National Imperative [Електронний ресурс] / National Research Council. – Washington, DC: The National Academies Press, 2012. – Режим доступу: <https://doi.org/10.17226/13457>.
5. Resilience Engineering in Practice: A Guidebook / E. Hollnagel, J. Pariès, D. D. Woods, J. Wreathall. – Farnham; Burlington: Ashgate, 2010. – 362 с.
6. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities [Електронний ресурс] / M. Bruneau, S. Chang, R. Eguchi, G. Lee, T. O'Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, D.

Winterfeldt. – Earthquake Spectra. – 2003. – Т. 19. – Режим доступу: <https://doi.org/10.1193/1.1623497>.

7. Linkov I. Resilience metrics for cyber systems / I. Linkov, D.A. Eisenberg, K. Plourde, T.P. Seager // Environment Systems and Decisions. – 2013. – Vol. 33, No. 4. – DOI: 10.1007/s10669-013-9485-y.
8. Rieger C. Resilient control systems: A multi-agent dynamic systems perspective / C. Rieger, K. Moore, T. Baldwin // IEEE International Conference on Electro Information Technology. – 2013. – С. 1–16. – DOI: [10.1109/EIT.2013.6632721](https://doi.org/10.1109/EIT.2013.6632721).
9. IBM. Cyber resilience [Електронний ресурс] / IBM. – Режим доступу: <https://www.ibm.com/think/topics/cyber-resilience>.
10. U. S. Department of Commerce. NIST Cloud Computing Standards Roadmap: Special Publication 500-291, Version 2. / U. S. Department of Commerce; National Institute of Standards and Technology. – Gaithersburg, MD: National Institute of Standards and Technology, 2013. – (in English).
11. Яскевич В. Методи підвищення відмовостійкості інтернет сервісів / В. Яскевич, О. Ключко // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2019. – Т. 3, № 3. – С. 104–111. – DOI: 10.28925/2663-4023.2019.3.104111.
12. Гальчинський Л. Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження) / Л. Гальчинський, В. Личик // Інформаційні технології та суспільство. – 2023. – Т. 2, № 8. – С. 27–33. – DOI: 10.32689/maur.it.2023.2.3.
13. Левашова С. Д., & Гальчинський, Л. Ю. (2025). Методика оцінювання кієррезильєнтності енергопідприємства XXIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених теоретичні і прикладні проблеми фізики, математики та інформатики, с.242–245, 14 – 17 травня 2025 р., м. Київ, Україна.
14. Chu X. A security assessment scheme for interdependent cyber-physical power systems / X. Chu, M. Tang, H. Huang, L. Zhang // 2017 8th IEEE

International Conference on Software Engineering and Service Science (ICSESS), 23–25 Sept. 2017, Beijing, China. – С. 816–819. – DOI: 10.1109/ICSESS.2017.8343036.

15. Jacobs N. Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example / N. Jacobs, S. Hossain-McKenzie, E. Vugrin // Proc. Resilience Week (RWS), 20–23 Aug. 2018. – С. 38–46. – DOI: 10.1109/RWEEK.2018.8473549.
16. Ashok A. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid / A. Ashok, M. Govindarasu, J. Wang // Proceedings of the IEEE. – 2017. – Т. 105, № 7. – С. 1389–1407. – DOI: 10.1109/JPROC.2017.2686394.
17. Inductive Automation. What is SCADA [Электронный ресурс] / Inductive Automation. – Режим доступа: <https://inductiveautomation.com/resources/article/what-is-scada>.
18. Leirbukt A. Taming the electric grid: Continuous improvement of wide-area monitoring for enhanced grid stability / A. Leirbukt, E. Scholtz, S. Paduraru // 2008 IEEE Power & Energy Society General Meeting, 20–24 July 2008, Pittsburgh, PA, USA. – С. 34–39.
19. Lu X. Research on Real-time Data Acquisition Technology Based on Distribution Automation Technology / X. Lu, Y. Gu, C. Liu, Q. Ye, K. Chen // IOP Conference Series: Earth and Environmental Science. – 2021. – Т. 632. – № 4. – С. 042006. – DOI: 10.1088/1755-1315/632/4/042006.
20. Yadav G. Architecture and security of SCADA systems: A review / G. Yadav, K. Paul // International Journal of Critical Infrastructure Protection. – 2021. – Т. 34. – Article ID: 100433. – ISSN 1874-5482. – DOI: 10.1016/j.ijcip.2021.100433.
21. The White House. Statement from National Security Advisor Jake Sullivan on the Global Effort to Strengthen the Cybersecurity of Energy Supply Chains

[Электронный ресурс] / The White House. – 18.06.2024. – Режим доступа: <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/06/18/statement-from-national-security-advisor-jake-sullivan-on-the-global-effort-to-strengthen-the-cybersecurity-of-energy-supply-chains>.

22. Check Point Research. Surge in Cybercrime: Check Point 2023 Mid-Year Security Report Reveals 48 ransomware groups have breached over 2,200 victims [Электронный ресурс] / Check Point Research. – San Carlos, CA: Check Point Software Technologies Ltd., 23.08.2023. – Режим доступа: <https://www.checkpoint.com/press-releases/surge-in-cybercrime-check-point-2023-mid-year-security-report-reveals-8-spike-in-global-cyberattacks/>.
23. CNN. Colonial Pipeline hackers accessed the system using a compromised password [Электронный ресурс] / CNN. – 04.06.2021. – Режим доступа: <https://edition.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html>
24. U.S. Department of Energy. Protecting Wind Energy Systems from Cyberattacks [Электронный ресурс] / U.S. Department of Energy. – 21.05.2024. – Режим доступа: <https://www.energy.gov/eere/wind/articles/protecting-wind-energy-systems-cyberattacks>.
25. Lipovsky R. BlackEnergy Trojan strikes again: Attacks Ukrainian electric power industry [Электронный ресурс] / R. Lipovsky // WeLiveSecurity. – 04.01.2016. – Режим доступа: <https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/>.
26. CISA. Cyber-Attack Against Ukrainian Critical Infrastructure [Электронный ресурс] / CISA. – Режим доступа: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>.

27. Cherepanov A. Industroyer: Biggest threat to industrial control systems since Stuxnet [Електронний ресурс] / А. Cherepanov // WeLiveSecurity. – 12.06.2017. – Режим доступу: <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.
28. Cloudflare. Petya & NotPetya ransomware [Електронний ресурс] / Cloudflare. – Режим доступу: <https://www.cloudflare.com/ru-ru/learning/security/ransomware/petya-notpetya-ransomware/>.
29. Кібератака NotPetya: що відомо [Електронний ресурс] – Режим доступу: <https://www.imena.ua/blog/notpetya-cyberattack/>.
30. Російські хакери координують дії з військовими та посилюють атаки напередодні зими: як Україна протистоїть кібератакам на енергосистему [Електронний ресурс]. – Forbes Україна. – Режим доступу: <https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosisitemu-08112023-17242>.
31. Killnet [Електронний ресурс]. – Wikipedia. – Режим доступу: <https://en.wikipedia.org/wiki/Killnet>.
32. Cybersecurity Advisory AA22-110A: Russian State-Sponsored Cyber Activity Targeting Ukraine [Електронний ресурс]. – Cybersecurity & Infrastructure Security Agency (CISA). – Режим доступу: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>.
33. Sandworm’s Playbook: How Russia’s GRU Launched a Cyberattack That Blacked Out Ukraine [Електронний ресурс] / Автор не вказаний. – Wired. – Режим доступу: <https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/>.
34. Attacks on Ukraine’s energy infrastructure harm civilian population [Електронний ресурс]. – United Nations in Ukraine. – Режим доступу:

<https://ukraine.un.org/en/278992-attacks-ukraine%E2%80%99s-energy-infrastructure-harm-civilian-population>.

35. QA Group. What is Metrics? [Електронний ресурс]. – QA Group, 2023. – Режим доступу: <https://qagroup.com.ua/publications/what-is-metrics/>.
36. Haque M. A. Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights [Текст] / Md Ariful Haque, Sachin Shetty, Bheshaj Krishnappa, Gael Teyou // 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA. – IEEE, 2018. – DOI: 10.1109/ISI.2018.8587398.
37. Navarro D. A brief introduction to research design / D. Navarro, D. Foxcroft. – Cambridge: Open Book Publishers, 2025. – DOI: 10.11647/obp.0333.02.
38. Whitaker R. The Analytic Hierarchy Process – What It Is and How It Is Used / R. Whitaker // Mathematical Modelling. – 1987. – Т. 9. – С. 161–176. – DOI: 10.1016/0270-0255(87)90473-8.
39. Haque M. A. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems / M.A. Haque, S. Shetty, B. Krishnappa та ін. – 2019. – DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
40. Saaty T.L. Relative measurement and its generalization in decision making: why pairwise comparisons are central in mathematics for the measurement of intangible factors: the analytic hierarchy/network process / T.L. Saaty. – Rev. R. Acad. Cien. Serie A. Mat., 2008. – Т. 102, С. 251–318. – DOI: 10.1007/BF03191825.
41. Левашова С. Д. Веб-застосунок для оцінювання кіберрезильєнтності енергопідприємства [Електронний ресурс] / С. Д. Левашова. – Режим доступу: <https://qhr0d.github.io/site/> – Дата звернення: 11.06.2025.

ДОДАТОК А КОД PYTHON ДЛЯ ОБЧИСЛЕННЯ ВАГ АНР

```

import pandas as pd
import numpy as np

df = pd.read_excel(r'C:\Users\Asus\Desktop\навча\8 сем\диплом\Експертне оцінювання (Відповіді).xlsx')

scale_mapping = {
    '4': 5.0, '3': 4.0, '2': 3.0, '1': 2.0, '0': 1.0,
    "1'": 1/2.0, "2'": 1/3.0, "3'": 1/4.0, "4'": 1/5.0
}

# Обчислює ваги метрик за допомогою Аналізу Ієрархічного Процесу (АНР)
# Створює матрицю попарних порівнянь на основі геометричного середнього значень шкалування
# Перевіряє узгодженість ( $\lambda_{max}$ , CI, CR)
# Обчислює кінцеві ваги як нормалізовані геометричні середні рядків матриці
1 usage
def compute_ahp_weights(metrics, columns):
    n = len(metrics)
    pairs = [(metrics[i], metrics[j]) for i in range(n) for j in range(i + 1, n)]
    matrix = np.ones((n, n))
    for (m1, m2), col in zip(pairs, columns):
        vals = df[col].astype(str).map(scale_mapping).dropna().astype(float)
        agg = np.prod(vals) ** (1.0 / len(vals))
        i, j = metrics.index(m1), metrics.index(m2)
        matrix[i, j] = agg
        matrix[j, i] = 1.0 / agg

    print(f"\nМатриця попарних порівнянь для {metrics}:")
    print(pd.DataFrame(matrix, index=metrics, columns=metrics))

    lambda_max, CI, CR = compute_consistency_ratio(matrix)
    print(f" $\lambda_{max}$  = {lambda_max:.4f}, CI = {CI:.4f}, CR = {CR:.4f}")

```

```

    geo_means = np.prod(matrix, axis=1) ** (1.0 / n)
    weights = geo_means / geo_means.sum()
    return pd.DataFrame({'Метрика': metrics, 'Вага': np.round(weights, decimals: 4)})

# Обчислює індекс узгодженості (Consistency Ratio) для матриці попарних порівнянь
# Обчислює власний вектор ваг через геометричні середні
# Розраховує  $\lambda_{max}$  та CI
# Ділимо CI на випадковий індекс RI для отримання CR
1 usage
def compute_consistency_ratio(matrix):
    n = matrix.shape[0]

    geo_means = np.prod(matrix, axis=1) ** (1.0 / n)
    weights = geo_means / np.sum(geo_means)

    Aw = matrix.dot(weights)
    lambda_max = np.sum(Aw / weights) / n

    CI = (lambda_max - n) / (n - 1)

    RI_dict = {
        1: 0.00, 2: 0.00, 3: 0.58, 4: 0.90, 5: 1.12,
        6: 1.24, 7: 1.32, 8: 1.41, 9: 1.45, 10: 1.49,
        11: 1.51, 12: 1.54
    }
    RI = RI_dict.get(n, RI_dict[max(k for k in RI_dict if k < n)])

    CR = CI / RI if RI != 0 else 0.0

    return lambda_max, CI, CR

```

```

categories = {
  'Стратегічні метрики': {
    'metrics': ['Міцність', 'Надлишковість', 'Винахідливість', 'Швидкість реагування']
  },
  'Доменні метрики': {
    'metrics': ['Фізична', 'Організаційна', 'Технічна']
  },
  'Фізичні підметрики': {
    'metrics': [
      'Фізичний контроль доступу',
      'Фізична різноманітність',
      'Резервування пристроїв',
      'Резервування каналів зв'язку та джерел живлення',
      'Фізичний моніторинг',
      'Захист даних',
      'Забезпечення фізичного доступу',
      'Безперебійна доступність'
    ]
  },
  'Організаційні підметрики': {
    'metrics': [
      'Контроль доступу на основі ролей (RBAC)',
      'Аудит та звітність',
      'Управління внутрішніми загрозами (1)',
      'План дій у надзвичайних ситуаціях',
      'Політика управління змінами',
      'Централізований SOC',
      'Організація реагування та відновлення',
      'Пом'якшення наслідків та аналіз',
      'Ефективність внутрішнього спілкування',
      'Управління надзвичайними ситуаціями',
    ]
  }
}

```

```

        'Навчання та підвищення обізнаності',
        'Управління внутрішніми загрозами (2)'
    ]
},
'Tехнічні підметрики': {
    'metrics': [
        'Сегментація мережі',
        'Шифрування та аутентифікація зв'язку',
        'Логічний контроль доступу',
        'Резервне копіювання серверів та носіїв даних',
        'Різноманітність вендорів',
        'Система виявлення вторгнень (IDS)',
        'Система оновлення та виправлення вразливостей',
        'Реєстрація та аналіз інцидентів безпеки',
        'Обробка та прийняття рішень на рівні системи',
        'Мережеве широкомасштабне забезпечення зв'язку'
    ]
}
}

start_col = 3
for cat_name, cat_info in categories.items():
    metrics = cat_info['metrics']
    n = len(metrics)
    num_pairs = n * (n - 1) // 2
    cols = list(df.columns[start_col:start_col + num_pairs])
    print(f"\nОбчислення ваг для категорії «{cat_name}» ({n} метрик, {num_pairs} порівнянь)")
    weights_df = compute_ahp_weights(metrics, cols)
    print(weights_df, end="\n" + "="*50 + "\n")
    start_col += num_pairs

```

ДОДАТОК Б КОД JAVASCRIPT COMPUTE.JS

```
// === Структура метрик ===
const metricsStructure = {
  R1: {
    Physical: [
      { name: 'Фізичний контроль доступу', ids: ['q1_1'] },
      { name: 'Фізична різноманітність', ids: ['q1_2'] }
    ],
    Organizational: [
      { name: 'Контроль доступу на основі ролей', ids: ['q3_1'] },
      { name: 'Аудит та звітність', ids: ['q5_1'] },
      { name: 'Управління внутрішніми загрозами 1', ids: ['q6_5'] }
    ],
    Technical: [
      { name: 'Сегментація мережі', ids: ['q2_1'] },
      { name: 'Шифрування та аутентифікація', ids: ['q2_2'] },
      { name: 'Логічний контроль доступу', ids: ['q3_2'] }
    ]
  },
  R2: {
    Physical: [
      { name: 'Резервування пристроїв', ids: ['q4_1'] },
      { name: 'Резервування каналів зв'язку та джерел живлення', ids: ['q4_2'] }
    ],
    Organizational: [
      { name: 'План дій надзвичайних ситуаціях', ids: ['q6_1'] },
      { name: 'Політика управління змінами', ids: ['q7_2'] }
    ],
    Technical: [
      { name: 'Резервне копіювання серверів та носіїв даних', ids: ['q4_3'] },
      { name: 'Різноманітність вендорів', ids: ['q4_4'] }
    ]
  },
  R3: {
    Physical: [
      { name: 'Фізичний моніторинг', ids: ['q1_3'] },
      { name: 'Захист даних', ids: ['q8_1'] }
    ]
  }
}
```

```

Organizational: [
  { name: 'Централізований SOC', ids: ['q5_2'] },
  { name: 'Організація реагування та відновлення', ids: ['q6_2'] },
  { name: 'Пом'якшення наслідків та аналіз', ids: ['q6_3'] },
  { name: 'Ефективність внутрішнього спілкування', ids: ['q7_3'] }
],
Technical: [
  { name: 'Система виявлення вторгнень (IDS)', ids: ['q5_3'] },
  { name: 'Система оновлення та виправлення вразливостей', ids: ['q8_2'] },
  { name: 'Реєстрація та аналіз інцидентів', ids: ['q5_4'] }
]
},
R4: {
  Physical: [
    { name: 'Забезпечення фізичного доступу', ids: ['q1_4'] },
    { name: 'Безперебійна доступність', ids: ['q4_5'] }
  ],
  Organizational: [
    { name: 'Управління надзвичайними ситуаціями', ids: ['q6_4'] },
    { name: 'Навчання та підвищення обізнаності', ids: ['q7_4'] },
    { name: 'Управління внутрішніми загрозами 2', ids: ['q7_1'] }
  ],
  Technical: [
    { name: 'Обробка та прийняття рішень на рівні системи', ids: ['q5_5'] },
    { name: 'Мережеве широкомасштабне забезпечення зв'язку', ids: ['q2_3'] }
  ]
}
};

```

```
// === Стратегічні ваги R1..R4 ===
const strategicWeights = {
  R1: 0.3597,
  R2: 0.1640,
  R3: 0.1931,
  R4: 0.2832
};

let userStrategicWeights = {};

// === Ваги доменів ===
const domainWeights = {
  Physical: 0.2833,
  Organizational: 0.3233,
  Technical: 0.3934
};

let userDomainWeights = {};

// === Ваги підметрик ===
const submetricsWeights = {
  R1: {
    Physical: {
      'Фізичний контроль доступу': 0.5289,
      'Фізична різноманітність': 0.4711
    },
    Organizational: {
      'Контроль доступу на основі ролей': 0.3773,
      'Аудит та звітність': 0.4472,
      'Управління внутрішніми загрозами 1': 0.1755
    },
    Technical: {
      'Сегментація мережі': 0.2536,
      'Шифрування та аутентифікація': 0.4384,
      'Логічний контроль доступу': 0.3080
    }
  }
}
```

```

R2: {
  Physical: {
    'Резервування пристроїв': 0.4891,
    'Резервування каналів зв'язку та джерел живлення': 0.5109
  },
  Organizational: {
    'План дій у надзвичайних ситуаціях': 0.6231,
    'Політика управління змінами': 0.3769
  },
  Technical: {
    'Резервне копіювання серверів та носіїв даних': 0.7903,
    'Різноманітність вендорів': 0.2097
  }
},
R3: {
  Physical: {
    'Фізичний моніторинг': 0.2560,
    'Захист даних': 0.7440
  },
  Organizational: {
    'Централізований SOC': 0.3200,
    'Організація реагування та відновлення': 0.2965,
    'Пом'якшення наслідків та аналіз': 0.2121,
    'Ефективність внутрішнього спілкування': 0.1714
  },
  Technical: {
    'Система виявлення вторгнень (IDS)': 0.2910,
    'Система оновлення та виправлення вразливостей': 0.3224,
    'Реєстрація та аналіз інцидентів': 0.3867
  }
},

```

```

R4: {
  Physical: {
    'Забезпечення фізичного доступу': 0.3557,
    'Безперебійна доступність': 0.6443
  },
  Organizational: {
    'Управління надзвичайними ситуаціями': 0.4071,
    'Навчання та підвищення обізнаності': 0.2349,
    'Управління внутрішніми загрозами 2': 0.3580
  },
  Technical: {
    'Мережеве широкомасштабне забезпечення зв'язку': 0.5824,
    'Обробка та прийняття рішень на рівні системи': 0.4176
  }
}
};

// === Функція для зчитування відповіді з одного поля ===
function getAnswerValue(qId) {
  const radio = document.querySelector(`input[name="${qId}"]:checked`);
  return radio ? parseInt(radio.value, 10) : null;
}

// === Збір усіх відповідей у вкладений об'єкт ===
function collectAllAnswers() {
  const result = {};
  for (let Rkey of Object.keys(metricsStructure)) {
    result[Rkey] = {};
    for (let domain of Object.keys(metricsStructure[Rkey])) {
      for (let sm of metricsStructure[Rkey][domain]) {
        const answersForSM = [];
        for (let qId of sm.ids) {
          const val = getAnswerValue(qId);
          answersForSM.push(val);
        }
      }
    }
  }
}

```

```
    }
    result[Rkey][sm.name] = answersForSM;
  }
}
}
return result;
}

// === Обчислення ECS ===
function computeECS(answersForSM) {
  const sum = answersForSM.reduce((acc, v) => acc + v, 0);
  return sum / answersForSM.length;
}

// === Обчислення DS ===
function computeDomainScore(Rkey, domainKey, allAnswers) {
  let ds = 0;
  for (let sm of metricsStructure[Rkey][domainKey]) {
    const smName = sm.name;
    const answersForSM = allAnswers[Rkey][smName];
    const ecs = computeECS(answersForSM);
    const wSM = submetricsWeights[Rkey][domainKey][smName] || 0;
    ds += ecs * wSM;
  }
  return ds;
}

// === Обчислення Ri (до нормалізації) ===
function computeCi(Rkey, allAnswers) {
  const dsPhys = computeDomainScore(Rkey, 'Physical', allAnswers);
  const dsOrg = computeDomainScore(Rkey, 'Organizational', allAnswers);
  const dsTech = computeDomainScore(Rkey, 'Technical', allAnswers);
```

```

let wPhys, wOrg, wTech;
if (Object.keys(userDomainWeights).length > 0) {
  wPhys = userDomainWeights['Physical'];
  wOrg = userDomainWeights['Organizational'];
  wTech = userDomainWeights['Technical'];
} else {
  wPhys = domainWeights.Physical;
  wOrg = domainWeights.Organizational;
  wTech = domainWeights.Technical;
}

return wPhys * dsPhys + wOrg * dsOrg + wTech * dsTech;
}

// === Нормалізація Ri у [0..1] ===
function normalizeCi(ci) {
  return (ci - 1) / 4;
}

// === Обчислення CSF ===
function computeCSF(allCiN) {
  let csf = 0;
  for (let Rkey of Object.keys(strategicWeights)) {
    let wRi;
    if (Object.keys(userStrategicWeights).length > 0) {
      wRi = userStrategicWeights[Rkey];
    } else {
      wRi = strategicWeights[Rkey];
    }
    const ciN = allCiN[Rkey];
    csf += wRi * ciN;
  }
  return csf;
}

```

```

// === Обчислення R ===
function computeResilienceR(csf) {
  return (1 - csf) / Math.log(1 / csf);
}

// === Основна функція, що обчислює всі метрики та R ===
function computeResilienceMetrics(allAnswers) {
  const allCi = {};
  const allCiN = {};

  for (let Rkey of Object.keys(metricsStructure)) {
    const ci = computeCi(Rkey, allAnswers);
    allCi[Rkey] = ci;
    allCiN[Rkey] = normalizeCi(ci);
  }

  const csf = computeCSF(allCiN);

  const resilienceR = computeResilienceR(csf);

  displayResults({ allCi, allCiN, csf, resilienceR });
}

// === Відображення результатів у таблицю ===
function displayResults(data) {
  const container = document.getElementById('results');
  container.innerHTML = '';

  let html = `<h3 class="fw-bold text-blue-3 mt-4">Результати обчислення кіберрезильєнтності</h3>`;
  html += `<table class="table table-bordered mt-3">
  <thead>
  <tr>
  <th>Стратегічна (Ri) метрика</th>
  <th>Значення R<sub>i</sub> (1-5)</th>
  <th>Нормалізоване R<sub>iN</sub> (0-1)</th>

```

```

    </tr>
  </thead>
  <tbody>;

  for (let Rkey of Object.keys(data.allCi)) {
    html += `<tr>
      <td>${Rkey}</td>
      <td>${data.allCi[Rkey].toFixed(3)}</td>
      <td>${data.allCiN[Rkey].toFixed(3)}</td>
    </tr>`;
  }

  html += `</tbody></table>`;
  html += `<p class="fw-bold text-blue-3 mt-3">CSF (Critical Service Functionality): ${data.csf.toFixed(3)}</p>`;
  html += `<p class="fw-bold text-blue-3 mt-3">Загальний рівень кіберрезильєнтності Вашого енергопідприємства R:
  ${data.resilienceR.toFixed(3)}</p>`;

  container.innerHTML = html;
}

const resilienceTitles = {
  R1: 'Міцність',
  R2: 'Надлишковість',
  R3: 'Винахідливість',
  R4: 'Швидкість реагування'
};

const COLOR_MAP = {
  R1: { background: 'rgba(54, 162, 235, 0.2)', border: 'rgba(54, 162, 235, 1)', point: 'rgba(54, 162, 235, 1)' },
  R2: { background: 'rgba(255, 159, 64, 0.2)', border: 'rgba(255, 159, 64, 1)', point: 'rgba(255, 159, 64, 1)' },
  R3: { background: 'rgba(255, 205, 86, 0.2)', border: 'rgba(255, 205, 86, 1)', point: 'rgba(255, 205, 86, 1)' },
  R4: { background: 'rgba(255, 99, 132, 0.2)', border: 'rgba(255, 99, 132, 1)', point: 'rgba(255, 99, 132, 1)' }
};

const DOMAIN_COLORS = {
  Physical: { background: 'rgba(54, 162, 235, 0.6)', border: 'rgba(54, 162, 235, 1)' },
  Organizational: { background: 'rgba(75, 192, 192, 0.6)', border: 'rgba(75, 192, 192, 1)' },
  Technical: { background: 'rgba(255, 99, 132, 0.6)', border: 'rgba(255, 99, 132, 1)' }
};

// === Функція для розбиття тексту на рядки по maxChars символів ===
function wrapText(text, maxChars) {
  const words = text.split(' ');
  const lines = [];
  let current = '';
  for (let word of words) {
    if ((current + ' ' + word).trim().length > maxChars) {
      lines.push(current.trim());
      current = word;
    } else {
      current += ' ' + word;
    }
  }
  if (current) lines.push(current.trim());
  return lines;
}

```

```
// === Візуалізація радарних діаграм ===
function renderRadarChart(canvasId, title, rawLabels, data, colors) {
  const ctx = document.getElementById(canvasId).getContext('2d');
  const labels = rawLabels.map(label => wrapText(label, 10));

  new Chart(ctx, {
    type: 'radar',
    data: {
      labels,
      datasets: [{
        label: title,
        data,
        backgroundColor: colors.background,
        borderColor: colors.border,
        pointBackgroundColor: colors.point,
        pointRadius: 5
      }]
    },
    options: {
      responsive: true,
      scales: {
        r: {
          min: 1,
          max: 5,
          ticks: { stepSize: 1 },
          angleLines: { color: '#ddd' },
          grid: { color: '#eee' },
          pointLabels: { font: { size: 16 }, color: '#2d336b' }
        }
      },
      plugins: {
        legend: { display: false },
        title: { display: true, text: title, font: { size: 18 }, color: '#2d336b' }
      }
    }
  });
}
```

```

// === Функція для побудови радарів за ECS-підметриками ===
function renderAllRadarCharts(allAnswers) {
  for (let Rkey of Object.keys(metricsStructure)) {
    const rawLabels = [];
    const data = [];

    for (let domain of Object.keys(metricsStructure[Rkey])) {
      for (let sm of metricsStructure[Rkey][domain]) {
        const ecs = computeECS(allAnswers[Rkey][sm.name]);
        rawLabels.push(sm.name);
        data.push(+ecs.toFixed(2));
      }
    }

    const colors = COLOR_MAP[Rkey] || COLOR_MAP['R1'];

    const displayTitle = resilienceTitles[Rkey] || Rkey;
    renderRadarChart(`radar-${Rkey}`, displayTitle, rawLabels, data, colors);
  }
}

// === Функція для побудови кругової діаграми ===
function renderStrategicPieChart(allCiN) {
  const ctx = document.getElementById('strategic-pie').getContext('2d');
  const labels = Object.keys(allCiN).map(Rkey => `${resilienceTitles[Rkey]} (${Rkey})`);
  const data = Object.values(allCiN);
  const backgroundColors = Object.keys(allCiN).map(Rkey => COLOR_MAP[Rkey].background);
  const borderColors = Object.keys(allCiN).map(Rkey => COLOR_MAP[Rkey].border);

```

```
new Chart(ctx, {
  type: 'pie',
  data: {
    labels: labels,
    datasets: [{
      data: data,
      backgroundColor: backgroundColors,
      borderColor: borderColors,
      borderWidth: 1
    }]
  },
  options: {
    responsive: true,
    plugins: {
      legend: {
        position: 'top',
        labels: {
          font: { size: 14 },
          color: '#2d336b'
        }
      },
      title: {
        display: true,
        text: 'Розподіл стратегічних метрик резильєнтності',
        font: { size: 18 },
        color: '#2d336b'
      }
    }
  }
});
}
```

```

// === Функція для побудови стовпчикової діаграми ===
function renderDomainBarChart(allDS) {
  const ctx = document.getElementById('domain-bar').getContext('2d');
  const labels = Object.keys(allDS).map(Rkey => `${resilienceTitles[Rkey]} (${Rkey})`);
  const domains = ['Physical', 'Organizational', 'Technical'];

  const datasets = domains.map(domain => ({
    label: domain,
    data: labels.map( (_, idx) => allDS[Object.keys(allDS)[idx]][domain]),
    backgroundColor: DOMAIN_COLORS[domain].background,
    borderColor: DOMAIN_COLORS[domain].border,
    borderWidth: 1
  }));

  new Chart(ctx, {
    type: 'bar',
    data: { labels, datasets },
    options: {
      responsive: true,
      scales: {
        x: { title: { display: true, text: 'Стратегічні метрики', color: '#2d336b', font: { size: 14 } } },
        y: {
          beginAtZero: true,
          max: 5,
          ticks: { stepSize: 1 },
          title: { display: true, text: 'Оцінка доменів', color: '#2d336b', font: { size: 14 } }
        }
      },
      plugins: {
        legend: { position: 'top', labels: { font: { size: 14 }, color: '#2d336b' } },
        title: { display: true, text: 'Доменні метрики для кожної стратегічної метрики', font: { size: 18 }, color: '#2d336b' }
      }
    }
  });
}

```

```

    },
    barPercentage: 0.8,
    categoryPercentage: 0.9
  }
});
}

// === Обробник події для кнопки "Відправити відповіді" ===
document.addEventListener('DOMContentLoaded', () => {
  const form = document.querySelector('#survey form');
  form.addEventListener('submit', function(event) {
    event.preventDefault();

    const allAnswers = collectAllAnswers();

    // Перевірка на пропущені відповіді
    for (let Rkey of Object.keys(allAnswers)) {
      for (let smName of Object.keys(allAnswers[Rkey])) {
        if (allAnswers[Rkey][smName].some(v => v === null)) {
          alert(`Будь ласка, дайте відповідь на питання "${smName}".`);
          return;
        }
      }
    }

    // Обчислення основних метрик
    computeResilienceMetrics(allAnswers);

    // Обчислення даних для графіків
    const allCi = {};
    const allCiN = {};
    const allDS = {};
    for (let Rkey of Object.keys(metricsStructure)) {
      const ci = computeCi(Rkey, allAnswers);
    }
  });
});

```

```

    allCi[Rkey] = ci;
    allCiN[Rkey] = normalizeCi(ci);
    allDS[Rkey] = {
      Physical: computeDomainScore(Rkey, 'Physical', allAnswers),
      Organizational: computeDomainScore(Rkey, 'Organizational', allAnswers),
      Technical: computeDomainScore(Rkey, 'Technical', allAnswers)
    };
  }

  // Рендеринг графіків
  renderStrategicPieChart(allCi);
  renderDomainBarChart(allDS);
  renderAllRadarCharts(allAnswers);

  document.getElementById('results').style.display = 'block';
  document.getElementById('diagrams').style.display = 'block';
});
});

// === Обробник події для кнопки "Продовжити" ===
document.getElementById('proceed-button').addEventListener('click', function() {
  const expertChoice = document.getElementById('expert-weights').checked;
  const customChoice = document.getElementById('custom-weights').checked;
  const weightsSection = document.getElementById('weights');

  if (expertChoice) {
    // Якщо обрано експертні ваги, приховуємо секцію вводу ваг
    weightsSection.style.display = 'none';
    userStrategicWeights = {};
    userDomainWeights = {};
    alert('Ви обрали опитування з вагами від експертів. Починаємо опитування.');
```

```

    } else {
      alert('Будь ласка, оберіть один із варіантів.');
```

```

    }
  });

  // Перевірка введених ваг
document.getElementById('save-weights').addEventListener('click', function() {
  // Перевірка стратегічних метрик
  const strategicInputs = document.querySelectorAll('#strategic-weights-table input[type="number"]');
  let strategicSum = 0;
  let allStrategicFilled = true;
  strategicInputs.forEach(input => {
    const value = parseFloat(input.value);
    if (isNaN(value) || value < 0 || value > 1) {
      allStrategicFilled = false;
    } else {
      strategicSum += value;
    }
  });

  // Перевірка доменних метрик
  const domainInputs = document.querySelectorAll('#domain-weights-table input[type="number"]');
  let domainSum = 0;
  let allDomainFilled = true;
  domainInputs.forEach(input => {
    const value = parseFloat(input.value);
    if (isNaN(value) || value < 0 || value > 1) {
      allDomainFilled = false;
    } else {
      domainSum += value;
    }
  });

  // Перевірка умов
  if (!allStrategicFilled || !allDomainFilled) {
    alert('Будь ласка, заповніть всі ваги коректними значеннями (від 0 до 1).');
    return;
  }

  if (Math.abs(strategicSum - 1) > 0.001) {
    alert('Сума ваг для стратегічних метрик повинна дорівнювати 1.');
```

```

    return;
  }

  if (Math.abs(domainSum - 1) > 0.001) {
    alert('Сума ваг для доменних метрик повинна дорівнювати 1.');
```

```

    return;
  }

  // Збереження стратегічних ваг
  userStrategicWeights['R1'] = parseFloat(document.querySelector('input[name="R1-weight"]').value);
  userStrategicWeights['R2'] = parseFloat(document.querySelector('input[name="R2-weight"]').value);
  userStrategicWeights['R3'] = parseFloat(document.querySelector('input[name="R3-weight"]').value);
  userStrategicWeights['R4'] = parseFloat(document.querySelector('input[name="R4-weight"]').value);

  // Збереження доменних ваг
  userDomainWeights['Physical'] = parseFloat(document.querySelector('input[name="Physical-weight"]').value);
  userDomainWeights['Organizational'] = parseFloat(document.querySelector('input[name="Organizational-weight"]').value);
  userDomainWeights['Technical'] = parseFloat(document.querySelector('input[name="Technical-weight"]').value);

  alert('Ваги збережено успішно!');
});
```