

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

«На правах рукопису»
УДК 004.056

ДО ЗАХИСТУ ДОПУЩЕНО
Завідувач кафедри
_____ Дмитро ЛАНДЕ

«___»_____ 2026 р.

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

на тему: Розробка інформаційного забезпечення для профілювання кіберстійкості
енергетичного об'єкту

Виконала: здобувачка вищої освіти IV курсу, групи ФБ-25

(шифр групи)

Слобода Ірина Василівна

(прізвище, ім'я, по батькові)

(підпис)

Науковий керівник: асистент кафедри ІБ, Личик Владислав Васильович

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

(підпис)

Рецензент: доцент кафедри ММАД, к.т.н. Лавренюк Алла Миколаївна

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

(підпис)

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

Здобувач вищої освіти _____

(підпис)

Київ – 2026 року

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

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 125 «Кібербезпека»

Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ

Завідувач кафедри

Дмитро ЛАНДЕ

(підпис)

«22» червня 2026 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти
Слобода Ірина Василівна
(прізвище, ім'я, по батькові)

1. Тема роботи: «Розробка інформаційного забезпечення для профілювання кіберстійкості енергетичного об'єкту»,

керівник роботи: Личик Владислав Васильович, асистент кафедри ІБ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

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

2. Термін подання роботи здобувачем вищої освіти «12» червня 2026 р.

3. Вихідні дані до роботи: методології та методи для оцінки кіберстійкості об'єктів критичної інфраструктури.

4. Зміст пояснювальної записки: аналіз актуальних кібератак на критичну інфраструктуру та сучасних фреймворків оцінки їх кіберстійкості, формування структури інструмента профілювання, розробка програмного комплексу підтримки прийняття рішень, проведення оцінки та отримання інтегрального показника кіберстійкості тестового об'єкта.

5. Орієнтовний перелік ілюстративного матеріалу: презентація до захисту дипломної роботи.

6. Дата видачі завдання: 13 жовтня 2025 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Визначення напрямку ДР	13.10.2025	Виконано
2	Визначення теми ДР	13.10.2025 – 28.10.2025	Виконано
3	Збір та аналіз літературних джерел	20.10.2025 – 20.02.2026	Виконано
4	Формування напрямків проблематики роботи	15.11.2025 – 26.02.2026	Виконано
5	Аналіз наявних рішень	20.12.2025 – 05.03.2026	Виконано
6	Вибір сегмента для дослідження	05.03.2026 – 26.03.2026	Виконано
7	Побудова власного інструменту оцінки	26.03.2026– 27.04.2026	Виконано
8	Апробація на тестовому об'єкті	17.04.2026 – 20.05.2026	Виконано
9	Виконання перевірки на чутливість даних	13.05.2026 – 29.05.2026	Виконано
10	Підготовка до попереднього захисту ДР	25.05.2026 – 11.06.2026	Виконано
11	Захист дипломної роботи	22.06.2026	Виконано

Здобувач вищої освіти

(підпис)

Ірина СЛОБОДА
(Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи

(підпис)

Владислав ЛИЧИК
(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Дипломна робота складається з 3 розділів, містить 110 сторінок, 17 таблиць, 26 рисунків та 31 джерело за переліком посилань.

Мета роботи – розробити інформаційне забезпечення для профілювання кіберстійкості об’єкта енергетичної інфраструктури, реалізувати його у вигляді програмного прототипу та апробувати на тестовому профілі енергооб’єкта з використанням експертних оцінок, доменно-рольової структури й кількісної інтерпретації результатів.

Об’єкт дослідження – процеси забезпечення кіберстійкості об’єктів енергетичної інфраструктури в умовах впливу кібератак, організаційних вразливостей та взаємозалежності IT- і OT-середовищ.

Предмет дослідження – методи, фреймворки та інструменти профілювання кіберстійкості енергетичних об’єктів, зокрема структура інформаційного забезпечення, що поєднує елементи C2M2, CAF, CRR, Scottish Public Sector Cyber Resilience Framework, експертне оцінювання, рольову крос-верифікацію та адитивне агрегування результатів.

Методи дослідження: аналіз літературних і нормативно-методичних джерел, аналіз відомих кібератак на критичну інфраструктуру, порівняльний аналіз фреймворків оцінювання кіберстійкості, експертне оцінювання, рольова крос-верифікація відповідей респондентів, адитивне агрегування показників, аналіз чутливості результатів і програмна реалізація прототипу автоматизованого інструмента профілювання.

Результати досліджень було апробовано на XXIV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» КПІ ім. Ігоря Сікорського, 13–16 травня 2026 р.

Ключові слова: кіберстійкість, енергетична інфраструктура, профілювання кіберстійкості, фреймворки, критична інфраструктура, адитивна модель, експертна оцінка.

ABSTRACT

This work consists of 3 chapters, contains 110 pages, 17 tables, 26 figures, and 31 references.

The purpose of the work is to develop an information support framework for profiling the cyber resilience of an energy infrastructure facility, implement it as a software prototype, and test it on a sample energy facility profile using expert assessments, a domain-role structure, and quantitative interpretation of the results.

The object of the study is the processes of ensuring and assessing the cyber resilience of energy infrastructure facilities under the influence of cyberattacks, organizational vulnerabilities, and interdependence between IT and OT environments.

The subject of the study is methods, frameworks and tools for assessing the cyber resilience of energy infrastructure facilities, in particular, the integration of C2M2, CAF, CRR, and selected elements of the Scottish Public Sector Cyber Resilience Framework into an information support framework adapted to the Ukrainian context.

Research methods: analysis of scientific, regulatory, and methodological sources, analysis of known cyberattacks on critical infrastructure, comparative analysis of cyber resilience assessment frameworks, expert assessment method, cross-verification of respondents' responses, additive model of indicator aggregation, sensitivity analysis of results, software implementation of a prototype automated profiling tool.

The research results were tested at the XXIV All-Ukrainian Scientific and Practical Conference of Students, Postgraduate Students and Young Scientists "Theoretical and applied problems of physics, mathematics and informatics", of the Kyiv Polytechnic Institute named after Igor Sikorsky, May 13–16, 2026.

Keywords: cyber resilience, energy infrastructure, cyber resilience profiling, frameworks, critical infrastructure, additive model, expert assessment.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	9
ВСТУП.....	10
1 АНАЛІТИЧНИЙ ОГЛЯД СУЧАСНИХ ІНСТРУМЕНТІВ ОЦІНКИ КІБЕРСТІЙКОСТІ	14
1.1 Атаки на критичну інфраструктуру України	14
1.2 Огляд атак на енергетичну інфраструктуру інших країн	19
1.3 Аналіз сучасних систем оцінки кіберстійкості	21
1.4 Порівняльний аналіз фреймворків оцінювання кіберстійкості.....	27
Висновки до розділу 1	32
2 МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОФІЛЮВАННЯ КІБЕРСТІЙКОСТІ	34
2.1 Обґрунтування базового підходу для подальшої адаптації.....	36
2.2 Засади використання допоміжних елементів інших підходів	38
2.3 Формування вимог до адаптованого інструмента профілювання кіберстійкості	46
2.4 Концептуальна побудова адаптованого підходу.....	53
2.5 Методичне обґрунтування використання експертних оцінок	56
Висновки до розділу 2	63
3 РОЗРОБКА ТА ЗАСТОСУВАННЯ ПРАКТИЧНОГО АПАРАТУ.....	65
3.1 Постановка практичного завдання та логіка реалізації	65
3.2 Структура інформаційного забезпечення та формування опитувальника .	66
3.3 Програмна реалізація інструмента профілювання.....	69

3.4	Алгоритм збору, обробки та інтерпретації даних	71
3.5	Проведення апробації інструмента профілювання	74
3.6	Результати профілювання за доменами, ролями та критеріями.....	75
3.7	Перевірка чутливості результатів оцінювання.....	79
3.8	Інтерпретація профілю кіберстійкості та напрями вдосконалення.....	83
3.9	Обмеження апробації та можливості подальшого розвитку	86
	Висновки до розділу 3	87
	ВИСНОВКИ	89
	ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ	92
	ДОДАТОК А	
	ПЕРЕЛІК ІНДИКАТОРІВ ОЦІНЮВАННЯ	96
	ДОДАТОК Б	
	СТРУКТУРА РЕПОЗИТОРІЮ ПРОГРАМНОГО ЗАСТОСУНКУ	106
	ДОДАТОК В	
	КЛЮЧОВІ ФРАГМЕНТИ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ МЕТОДИКИ.....	107

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

APT – Advanced Persistent Threat

CAF – Cyber Assessment Framework

C2M2 – Cybersecurity Capability Maturity Model

CRR – Cyber Resilience Review

CISA – Cybersecurity and Infrastructure Security Agency

IGP – Indicators of Good Practice

ІКС – Інформаційно-комунікаційна система

ІТ – Інформаційні технології

MFA – Multi-Factor Authentication

NIST CSF – NIST Cybersecurity Framework

OT – Operational Technology

ПКППР – програмний комплекс підтримки прийняття рішень

PSCRF – Scottish Public Sector Cyber Resilience Framework

SCADA – Supervisory Control and Data Acquisition

SIEM – Security Information and Event Management

SMART – Specific, Measurable, Achievable, Relevant, Time-bound

VPN – Virtual Private Network

АСУТП – автоматизована система управління технологічними процесами

КІ – критична інфраструктура

ШПЗ – шкідливе програмне забезпечення

ДБЖ – джерела безперебійного живлення

ВСТУП

Сучасна енергетична інфраструктура функціонує як складна кіберфізична система, у якій інформаційні технології, операційні технології, мережеві сервіси, засоби диспетчерського керування та організаційні процеси тісно пов'язані між собою. Цифровізація підвищує ефективність керування енергетичними об'єктами, однак одночасно збільшує залежність технологічних процесів від програмних, мережевих і керуючих компонентів. Унаслідок цього кібератаки можуть впливати не лише на конфіденційність або цілісність даних, а й на доступність критичних функцій, безперервність роботи об'єкта та безпечність фізичних процесів.

Актуальність роботи обумовлена зростанням кількості кібератак на об'єкти критичної інфраструктури, зокрема енергетичної, а також потребою у практичних інструментах, які дають змогу не лише описати стан захисту, а й сформувати кількісний профіль кіберстійкості енергетичного об'єкта. У наявних міжнародних підходах до оцінювання кіберстійкості вже сформовано значну методичну базу. Водночас жоден із цих підходів не може бути механічно перенесений на український енергетичний об'єкт без урахування локального контексту, ролей персоналу, архітектури ІТ/ОТ-середовища, зовнішніх залежностей і умов воєнного стану.

У цій роботі розроблено інформаційне забезпечення для профілювання кіберстійкості енергетичного об'єкта, яке розглядається як сукупність структурованих даних, правил їх збору й обробки, опитувальних форм, шкал інтерпретації та алгоритмів агрегування. Воно поєднує структурні елементи міжнародних підходів, засоби управлінського подання результатів та адитивну модель кількісного оцінювання. Практична реалізація цього інструментарію передбачає формування доменно-рольового опитувальника, збір і крос-верифікацію експертних відповідей, обчислення доменних та інтегрального показників, аналіз чутливості, а також виявлення слабких місць із побудовою підсумкового профілю стійкості.

Мета роботи полягає у розробленні інформаційного забезпечення для профілювання кіберстійкості енергетичного об'єкта, його адаптації до українського контексту, програмній реалізації та апробації на тестовому профілі енергооб'єкта.

Об'єкт дослідження – процеси забезпечення кіберстійкості об'єктів енергетичної інфраструктури в умовах впливу кіберзагроз, організаційних вразливостей і взаємозалежності ІТ- та ОТ-середовищ.

Предмет дослідження – методи та інструменти оцінювання кіберстійкості об'єктів енергетичної інфраструктури, зокрема інформаційне забезпечення профілювання кіберстійкості енергетичного об'єкта, що поєднує міжнародні фреймворки, експертне оцінювання, рольову крос-верифікацію та кількісну адитивну модель.

Завдання дослідження:

1. Проаналізувати сучасні кібератаки на критичну та енергетичну інфраструктуру, визначити їхні наслідки та типові слабкі місця, що впливають на кіберстійкість об'єктів.
2. Дослідити фреймворки оцінювання кіберстійкості та визначити елементи, придатні для побудови інформаційного забезпечення профілювання кіберстійкості.
3. Сформувати структуру інформаційного забезпечення профілювання кіберстійкості.
4. Розробити прототип програмного комплексу підтримки прийняття рішень для збору відповідей, обчислення результатів і експорту профілю кіберстійкості.
5. Провести апробацію розробленого інформаційного забезпечення на тестовому профілі енергетичного об'єкта, виявити критичні прогалини та виконати перевірку чутливості отриманих результатів.

Методи дослідження: аналіз наукових, нормативних і методичних джерел; аналіз відомих кібератак на критичну інфраструктуру; порівняльний аналіз фреймворків оцінювання кіберстійкості; метод експертного оцінювання; крос-верифікація відповідей; переведення якісних відповідей у числові значення; адитивне агрегування показників; аналіз чутливості; програмна реалізація прототипу автоматизованого інструментарію оцінювання; таблична та графічна інтерпретація результатів.

Наукова новизна одержаних результатів полягає у розробленні структури інформаційного забезпечення для профілювання кіберстійкості енергетичного об'єкта. На відміну від використання окремого фреймворку, запропонована структура поєднує доменну логіку C2M2, оцінювання станів CAF, інтерв'ювальний і рольовий механізм CRR, крос-верифікацію відповідей різних груп респондентів, адитивну модель формування інтегрального профілю кіберстійкості та перевірку чутливості результатів.

Практичне значення одержаних результатів полягає у можливості використання розробленого інформаційного забезпечення та прототипу програмного комплексу підтримки прийняття рішень для структурованого профілювання кіберстійкості енергетичного об'єкта. Запропонований інструмент дає змогу збирати експертні відповіді, формувати доменні й рольові оцінки, виявляти критичні прогалини, визначати пріоритети вдосконалення та експортувати результати у форматі, придатному для подальшого аналізу.

Апробація результатів роботи: XXIV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» КПІ ім. Ігоря Сікорського, 13–16 травня 2026 р.

Публікація за результатами досліджень: Слобода І. В., Личик В. В. Розробка гібридного методу оцінки кіберстійкості об'єкта енергетичної інфраструктури. Матеріали XXIV Всеукраїнської науково-практичної конференції

студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» КПІ ім. Ігоря Сікорського (13–16 травня 2026 р., м. Київ, Україна). С. 217-219.

1 АНАЛІТИЧНИЙ ОГЛЯД СУЧАСНИХ ІНСТРУМЕНТІВ ОЦІНКИ КІБЕРСТІЙКОСТІ

Обґрунтування потреби у використанні фреймворків оцінювання кіберстійкості варто почати з аналізу кібератак на критичну інфраструктуру та їхніх наслідків для функціонування об'єктів.

Спочатку розглянуто інциденти, пов'язані з українською критичною інфраструктурою, а далі – окремі закордонні випадки, що дозволяють ширше охарактеризувати проблему кіберстійкості енергетичних та інфраструктурних об'єктів.

1.1 Атаки на критичну інфраструктуру України

1.1.1 Спроба атаки Industroyer2 на українську енергетику (квітень 2022)

З початком повномасштабного вторгнення у 2022 році кібератаки на енергетичну інфраструктуру України стали масштабнішими, поєднуючись із ракетними ударами. Наприклад, у квітні 2022 року було виявлено спробу застосування ШПЗ Industroyer2, яке розглядають як розвиток Industroyer – OT-malware, використаного під час атаки на українську енергосистему у 2016 році.

Метою атаки було порушити роботу енергетичних об'єктів, зокрема систем, пов'язаних із керуванням високовольтними підстанціями [1]. Фахівцям вдалося вчасно ідентифікувати загрозу та зупинити шкідливі процеси до настання значних наслідків. Водночас зловмисники планували застосувати Industroyer2 разом із вайпером CaddyWiper, щоб ускладнити відновлення та перешкодити операторам енергетичної компанії повернути контроль над консолями ІКС [2].

Значення цього інциденту полягає в тому, що він став одним із перших відомих випадків повторного використання коду відомого OT-malware проти нового об'єкта. Це свідчить, що подібні інструменти можуть повторно

адаптуватися до нових цілей, а не залишаються прив'язаними до одного інциденту [3].

Для розроблюваного інструмента цей інцидент важливий тим, що показує потребу окремо оцінювати готовність організації до атак на технологічне середовище, а не лише на корпоративні IT-сервіси. Тому в адаптованому опитувальнику мають бути передбачені питання щодо сегментації IT/OT, контролю доступу до систем керування, резервних сценаріїв роботи та процедур відновлення після впливу на технологічні компоненти.

1.1.2 Кібератака Sandworm (жовтень 2022)

У жовтні 2022 року угруповання Sandworm здійснило нову атаку на українську енергетичну інфраструктуру. За оприлюдненими даними, зловмисники отримали доступ до середовища керування підстанцією і використали не окреме спеціалізоване ШПЗ, а штатні можливості SCADA-системи. У результаті було виконано команди на вимикачі, що спричинило незаплановані відключення електроенергії [4].

Відомо, що всередині встановленого образу було декілька файлів, серед яких: скрипт запуску, bat-файл для продовження виконання та текстовий файл із командами. Далі запускалася штатна утиліта MicroSCADA, через яку передавалися команди для виконання в середовищі керування.

Протягом двох днів після атаки було додатково застосовано новий варіант CaddyWiper, призначений для посилення порушень у роботі та ускладнення відновлення даних [5].

На рисунку 1.1 показано ланцюг виконання атаки у жовтні 2022 року.

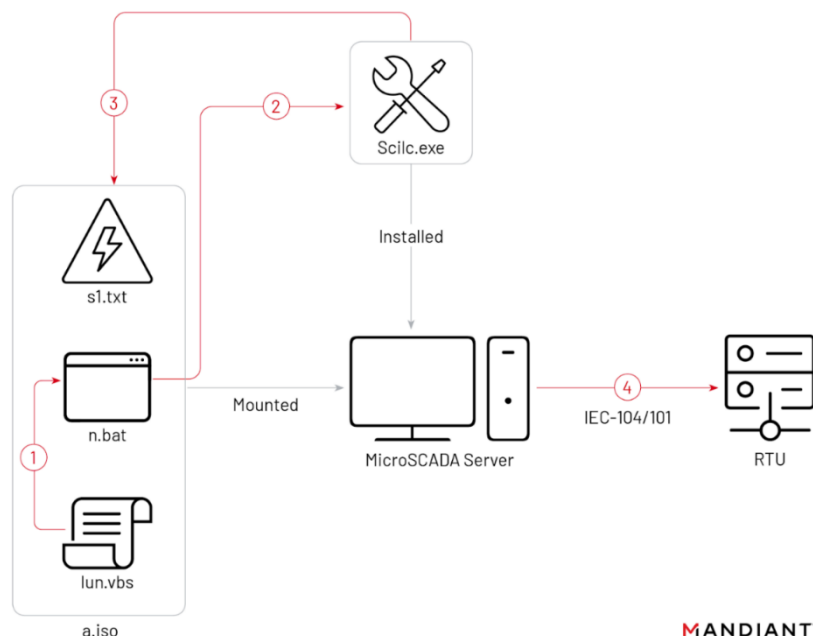


Рисунок 1.1 – Схема реалізації атаки (жовтень 2022) [4]

Цей випадок демонструє, що сучасні кібератаки можуть спиратися не тільки на спеціально створене ШПЗ. Отже, під час профілювання кіберстійкості недостатньо перевіряти лише наявність антивірусного захисту або засобів виявлення ШПЗ. Для енергетичного об'єкта окремого оцінювання потребують права операторів, контроль адміністративних дій, журналювання команд у SCADA-середовищі та здатність персоналу відрізнити штатну технологічну дію від дії, виконаної зловмисником через легітимний інструмент.

1.1.3 Кібератака Sandworm (березень 2024)

У березні 2024 року група Sandworm готувала нову атаку на об'єкти критичної інфраструктури України. Зафіксована активність була спрямована на порушення роботи інформаційно-комунікаційних систем близько двадцяти підприємств. Було підтверджено компрометацію щонайменше трьох ланцюгів водо-, тепло- та енергопостачання у десяти регіонах України, через які зловмисники отримували доступ до середовища підприємств. Цей доступ мав бути використаний для комбінування кібернетичного та фізичного впливу на інфраструктурних об'єктах [6]. Розвитку атаки сприяли недостатні організаційні й

технічні заходи кібербезпеки, зокрема відсутність належної сегментації мережі та слабкий контроль безпеки на рівні постачальників програмного забезпечення.

Цей інцидент можна розглядати як деструктивну кампанію, оскільки CERT-UA інформувала виявлені підприємства, допомагала з налаштуванням серверного й мережевого обладнання, впровадженням засобів захисту та аналізом обставин компрометації [7].

Загалом зловмисне угруповання Sandworm упродовж останніх десяти років використовувало різні шкідливі інструменти для впливу на українську критичну інфраструктуру. Особливо частими ці атаки стали після початку повномасштабного вторгнення. Узагальнену фазову структуру атак Sandworm наведено на рисунку 1.2 [8].

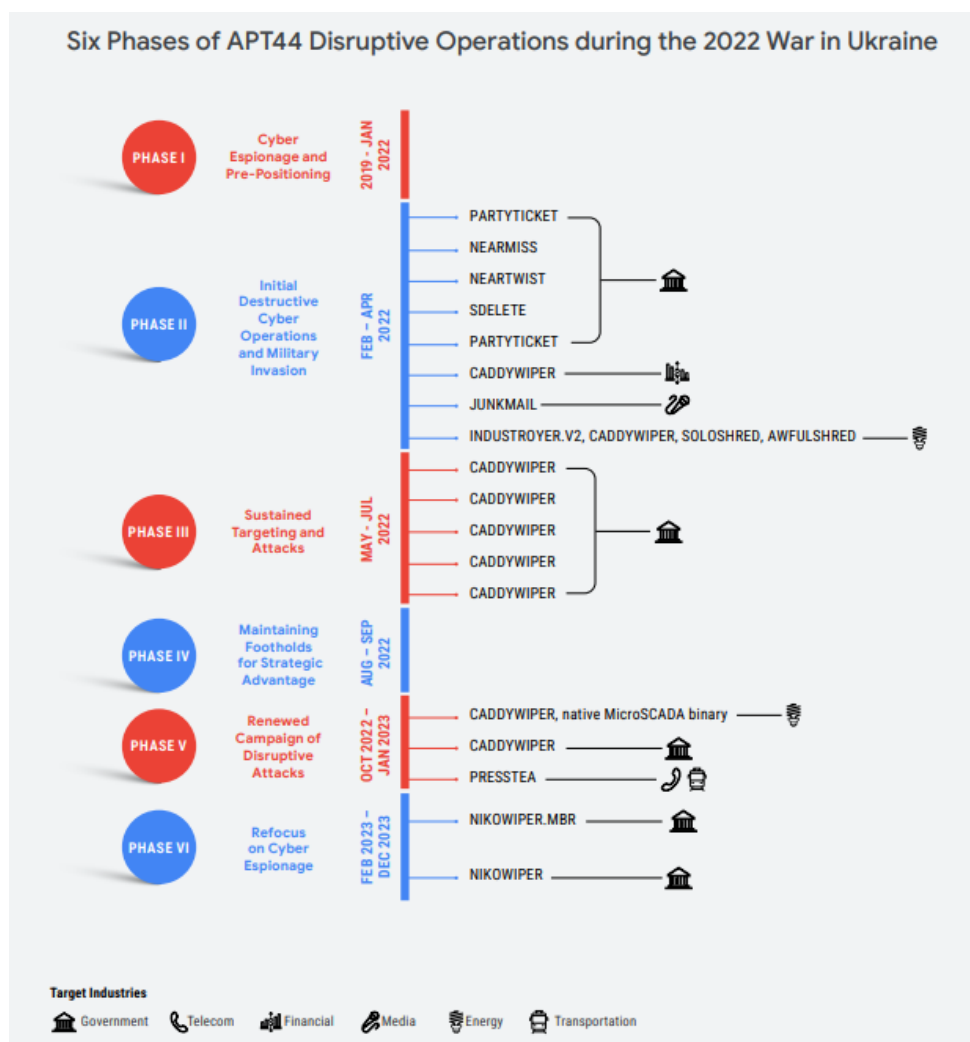


Рисунок 1.2 – Фази атак Sandworm [8]

У запропонованому інструменті цей кейс використано як аргумент для виділення окремого домену, пов'язаного з третіми сторонами, підрядниками та ланцюгом постачання. Якщо зовнішній постачальник або сервісна організація має доступ до критичних систем, то рівень кіберстійкості енергооб'єкта залежить не лише від внутрішніх політик, а й від правил перевірки, обмеження та моніторингу такого доступу.

1.1.4 Атака FrostyGoop (січень 2024)

Ще одним показовим інцидентом стала атака на теплопостачання у Львові в січні 2024 року. За даними Dragos, під час цього інциденту, ймовірно, використовувалося шкідливе програмне забезпечення FrostyGoop. За описом дослідників, інструмент не належить до технічно найскладніших, однак його небезпека полягає у здатності безпосередньо впливати на промислові пристрої, які взаємодіють із системами керування через протокол Modbus TCP [9].

Зловмисники могли проникнути в мережу ще у квітні 2023 року через вразливість у маршрутизаторі MikroTik, доступному з Інтернету. Подальшому розвитку атаки сприяли недостатня сегментація мережі, слабкий захист мережевої архітектури та неналежний контроль віддаленого доступу [10].

Для адаптованого профілю кіберстійкості цей інцидент показує значення базових, але критичних контролів: інвентаризації зовнішньо доступних пристроїв, перевірки паролів, обмеження доступу до промислових протоколів і контролю маршрутизаторів, які з'єднують технологічне середовище з іншими мережами. Саме тому в опитувальнику доцільно окремо перевіряти не лише наявність засобів захисту, а й фактичну керованість зовнішніх точок входу.

1.1.5 Атака із застосуванням PathWiper (червень 2025)

У червні 2025 року Cisco Talos повідомила про деструктивну атаку на український об'єкт критичної інфраструктури із застосуванням нового вайпера PathWiper [11]. За наявними даними, зловмисники, ймовірно, вже мали доступ до

консолі легітимного засобу адміністрування кінцевих вузлів і через неї розгорнули шкідливий код на підключені системи. На відміну від шпигунського програмного забезпечення, PathWiper був призначений саме для руйнування працездатності IT-середовища: він перезаписував критичні структури файлової системи та файли на диску [11].

Механізм атаки свідчить про попередню компрометацію адміністративного середовища підприємства. Небезпека такого сценарію полягає в тому, що зловмисники використовують наявні адміністративні можливості для масового розгортання вайпера. Характер ураження показує, що йшлося не про короткочасне порушення роботи, а про спробу знищити критично важливі дані та вивести IT-інфраструктуру з ладу.

Ці події підтверджують, що сучасне протистояння охоплює не лише фізичний, а й кіберпростір, де вплив на інформаційні та технологічні системи може мати прямі операційні наслідки. У контексті профілювання кіберстійкості PathWiper є показовим не лише як приклад деструктивного ШПЗ, а як сценарій зловживання вже наявним адміністративним середовищем. Тому оцінювання має включати питання щодо контролю привілейованих облікових записів, обмеження масового розгортання програмного забезпечення, ізоляції резервних копій і готовності до відновлення після втрати частини IT-інфраструктури.

1.2 Огляд атак на енергетичну інфраструктуру інших країн

1.2.1 Атака на Colonial Pipeline (США, травень 2021)

Одним із найбільш відомих міжнародних прикладів стала атака на Colonial Pipeline, компанію, що забезпечувала майже 45% потреб східного узбережжя США в паливі. У 2021 році зловмисники з угруповання DarkSide отримали доступ не через складну технічну експлуатацію, а через скомпрометовані облікові дані застарілого VPN-облікового запису, що належав колишньому працівнику. Оскільки в компанії не було налаштовано багатофакторну автентифікацію,

зловмисники використали цей доступ як легітимний вхід до корпоративної мережі [12].

Після отримання доступу було розгорнуто ransomware, який зашифрував дані бухгалтерських і білінгових систем. Хоча публічно не повідомлялося про пряме ураження технологічного контуру, компанія превентивно зупинила роботу трубопроводу, оскільки не могла виключити подальше поширення атаки. Інцидент спричинив дефіцит пального, черги на заправках і значний суспільний резонанс. Він також продемонстрував, що ураження корпоративних ІТ-систем може призвести до зупинки фізичних операцій через залежність виробничих процесів від інформаційних сервісів. Зрештою, компанія була змушена заплатити викуп, щоб отримати ключ для дешифрування [13].

Для цієї роботи цей інцидент є важливим, адже демонструє залежність фізичних операцій від корпоративних ІТ-сервісів. Навіть без прямого ураження ОТ-сегмента організація може зупинити фізичний процес через невпевненість у масштабі компрометації. Тому профілювання кіберстійкості має враховувати не лише стан технологічного середовища, а й готовність корпоративних сервісів, процедур ухвалення рішень і комунікації під час інциденту.

1.2.2 Інцидент із дамбою в Норвегії (квітень 2025)

У квітні 2025 року стався показовий інцидент на гідротехнічному об'єкті в Норвегії. Зловмисники отримали контроль над об'єктом на короткий термін, відкрили шлюз і протягом чотирьох годин здійснювали скид води, після чого атаку було зупинено. Влітку цей інцидент пов'язали із російськими хакерами, назвавши його прикладом нової активності проросійських кіберакторів проти критичної інфраструктури [14].

Випадок є особливо важливим тим, що фізичний ефект міг бути досягнутий без складної багаторівневої АРТ-операції та без використання спеціалізованого ШПЗ. Точкою входу міг бути зовнішньодоступний вебінтерфейс керування,

захищений слабким паролем [15]. Отже, ключова проблема полягала не у складному технічному обході захисту, а в недостатньому базовому контролі доступу до елементів операційного середовища.

У контексті профілювання кіберстійкості цей інцидент є показовим міжнародним прикладом, оскільки демонструє вплив базових недоліків контролю доступу на безпечність фізичних процесів. Він показує, що вплив на енергетичну або гідротехнічну інфраструктуру може бути досягнутий навіть через відносно просту помилку в захисті, якщо критичний елемент керування винесено назовні та недостатньо захищено. Для адаптованого інструмента цей приклад підтверджує, що низький рівень базового контролю доступу може створити фізичний ефект навіть без складної АРТ-операції. Тому питання фізичної та кіберфізичної безпеки не можна залишати поза межами оцінювання: вони мають бути включені до окремого домену разом із контролем доступу до критичних зон, зовнішніх інтерфейсів керування та процедур реагування на несанкціоновані дії.

1.3 Аналіз сучасних систем оцінки кіберстійкості

Огляд наведених інцидентів показує, що для об'єктів критичної інфраструктури важливо не лише описувати окремі загрози, а й мати можливість кількісно оцінювати здатність об'єкта підтримувати функціонування та відновлюватися після порушення. У цьому контексті доцільним є використання метрик кібервідмовостійкості, які дозволяють перейти від загального опису стану безпеки до вимірюваного профілю стійкості об'єкта [16].

Також розглянуті інциденти свідчать, що атаки на критичну інфраструктуру можуть відрізнятися за мотивами, тактикою та рівнем складності, однак у кожному випадку їхні наслідки пов'язані з порушенням критичних функцій, компрометацією середовища керування або зниженням доступності важливих сервісів.

Для таких об'єктів недостатньо лише констатувати наявність загроз або впроваджувати окремі технічні засоби захисту. Необхідний системний інструмент, який дає змогу оцінити слабкі місця, рівень підготовленості до інцидентів, спроможність до реагування та відновлення. Саме таку роль виконують фреймворки оцінювання кіберстійкості, які переводять загальні уявлення про захист у структуру доменів, критеріїв і показників.

Крім того, розглянуті приклади підтверджують важливість адаптивного реагування на порушення кіберстійкості. Для об'єктів критичної інфраструктури важливо не лише запобігати атакам, а й своєчасно змінювати режим функціонування, координувати дії відповідальних сторін, підтримувати критичні функції та відновлювати роботу після інциденту [17]. Саме тому профілювання кіберстійкості має враховувати не тільки поточний стан захисту, а й готовність об'єкта до реагування та відновлення.

1.3.1 Шотландський метод

Серед підходів до оцінювання кіберстійкості, орієнтованих на державні організації, виділяють Scottish Public Sector Cyber Resilience Framework (PSCRF), який у роботі розглядається як шотландський підхід до оцінювання кіберстійкості. Його використовують як основу для структурованого самооцінювання та перевірок, де увага приділяється не окремим технічним параметрам, а тому, наскільки в організації побудовано управління безпекою, контроль впроваджених заходів та готовність працювати під час інцидентів. Підхід дозволяє оцінювати ефективність управління ризиком, кіберконтролів і процесів управління, а результати обробляються спеціальним програмним застосунком [18].

Оцінка охоплює чотири домени: управління ризиками безпеки, захист від кібератак, виявлення кіберподій та мінімізація наслідків кіберінцидентів, у тому числі дії реагування і відновлення. Також PSCRF на практиці може інтегрувати вимоги інших стандартів і практик, що спрощує узгодження самооцінки з більш загальними вимогами до кібербезпеки в організації [19].

Якщо узагальнити, перевага шотландського підходу в тому, що він задає зрозумілу структуру оцінювання для державних організацій і допомагає фіксувати прогрес у часі в єдиному форматі, не зводячи все лише до технічних показників. Проте результати значною мірою залежать від суб'єктивності відповідей учасників опитування. Підхід є дещо спрощеним і може не враховувати специфічні технічні особливості складних індустріальних середовищ [19]. Тому в таких випадках метод доцільно використовувати як організаційно-процесну основу, а технічну частину доповнювати профільними настановами та стандартами.

1.3.2 Модель зрілості спроможностей кібербезпеки C2M2

Серед підходів до оцінювання кіберстійкості, які можна застосовувати до об'єктів енергетичної інфраструктури, доцільно виділити Cybersecurity Capability Maturity Model (C2M2), тобто Модель зрілості спроможностей кібербезпеки. Її розроблено за підтримки Міністерства енергетики США як безкоштовний інструмент самооцінювання, що допомагає організації оцінити власні кібербезпекові спроможності та обґрунтовано визначити напрями подальшого розвитку. Головна перевага C2M2 полягає в тому, що вона охоплює не лише класичні IT-системи, а й технологічні процеси (OT). І хоча розвиток C2M2 історично ініціювала саме енергетична галузь США, її можуть використовувати організації різного типу, масштабу та галузевої належності [20].

В основі C2M2 лежить ідея рівнів зрілості (MIL0–MIL3). Уся діяльність організації в межах моделі розділена на 10 доменів, які охоплюють повний цикл захисту: від управління активами та ризиками до реагування на інциденти та забезпечення безперервності роботи. Кожен наступний рівень зрілості передбачає не лише впровадження складніших практик, а й підтвердження того, що базові заходи вже документовані, регулярно виконуються та контролюються на управлінському рівні [21].

Процес оцінювання в межах C2M2 має характер структурованого самооцінювання, у якому аналізуються практики за доменами та рівнями зрілості

[21]. Оцінювання не обмежується заповненням анкети, а передбачає обговорення практик за участю технічних фахівців і представників управлінського рівня. Учасники спільно аналізують кожну практику та визначають, чи вона впроваджена, частково реалізована або потребує подальшого доопрацювання. Після завершення формується підсумковий звіт, який показує поточний стан реалізації практик і дає змогу виявити прогалини.

Модель створює можливість не лише зафіксувати поточний рівень, а й визначити напрями підвищення кіберстійкості. Водночас важливо розуміти, що C2M2 є гнучким інструментом і, оскільки результати значною мірою залежать від повноти, достовірності та обґрунтованості відповідей учасників самооцінювання, модель найкраще працює у поєднанні з національними стандартами та галузевими вимогами законодавства.

Для цієї роботи C2M2 обрано не як готовий шаблон для прямого перенесення, а як структурний каркас. Його домени використовуються для забезпечення повноти оцінювання, однак зміст питань і спосіб збору відповідей адаптовано під енергетичний об'єкт України. Зокрема, у запропонованому інструменті окремо враховано ролі респондентів, взаємодію ІТ- та ОТ-персоналу, зовнішніх підрядників, фізичну безпеку, резервування та готовність до ручного або ізольованого режиму роботи.

1.3.3 Методика NCSC Cyber Assessment Framework (CAF)

Серед підходів до оцінювання кіберстійкості, орієнтованих на організації, що забезпечують критично важливі функції, доцільно виділити Cyber Assessment Framework (CAF), розроблений Національним центром кібербезпеки Великої Британії (NCSC). Цей фреймворк призначений для системного оцінювання того, наскільки організація управляє кіберризиками, що можуть вплинути на виконання її критично важливих функцій. CAF побудований не як перелік формальних вимог, а як модель оцінювання очікуваних результатів у сфері кібербезпеки та кіберстійкості [22].

Структурно CAF базується на чотирьох високорівневих цілях: управління ризиками безпеки, захист від кібератак, виявлення кіберподій та мінімізація впливу кіберінцидентів. Ці цілі розбиті на 14 принципів, кожен з яких деталізується через конкретні очікувані результати. Для перевірки використовують «індикатори належної практики» (IGP). Це спеціальні таблиці, що допомагають визначити статус: «досягнуто», «частково досягнуто» або «не досягнуто» [23].

На практиці CAF використовується в секторах енергетики, охорони здоров'я, транспорту, цифрової інфраструктури та державного управління. NCSC прямо зазначає, що цей фреймворк застосовується майже всіма кіберрегуляторами Великої Британії та вже закріпився у державному секторі. Для визначення цільового рівня захисту в CAF використовується поняття CAF Profile. Існують Basic Profile і Enhanced Profile: перший задає базовий цільовий рівень кіберстійкості, а другий застосовується в умовах вищого рівня загроз і враховує складніші сценарії атак. Це дало змогу не просто зафіксувати поточний стан, а й сформувати очікуваний рівень кіберзахисту для конкретної організації або сектора [22].

Якщо узагальнити, перевага CAF полягає в тому, що він дає системну та достатньо гнучку структуру оцінювання кіберстійкості, орієнтовану саме на захист критично важливих функцій організації. Його сильною стороною є результативно-орієнтована логіка, можливість поєднувати самооцінювання із зовнішнім наглядом, а також здатність адаптувати спільне ядро моделі до потреб конкретного сектора. Проте, варто пам'ятати, що CAF потребує високої експертності від тих, хто проводить оцінювання, оскільки він базується на професійних судженнях, а не на простих тестах. Крім того, через досить загальний характер фреймворку його практичне застосування в індустріальних середовищах, зокрема в енергетиці, доцільно поєднувати з профільними технічними настановами та секторальними вимогами.

1.3.4 Методика CISA Cyber Resilience Review (CRR)

Ще одним практично орієнтованим підходом є Cyber Resilience Review (CRR), розроблений американським Агентством з кібербезпеки та захисту інфраструктури (CISA). Якщо частина інших фреймворків має переважно високорівневий характер, то CRR є більш прикладним інструментом оцінювання, побудованим у форматі структурованого інтерв'ю. У центрі уваги перебувають не лише технічні засоби захисту, а й організаційна стійкість установи, тобто її здатність підтримувати виконання критично важливих функцій навіть у разі порушення роботи окремих систем [24, 25].

Оцінювання охоплює десять ключових напрямів, серед яких управління вразливостями, конфігураціями, інцидентами, а також контроль залежностей від зовнішніх постачальників і партнерів [24]. На практиці CRR проводиться у формі сесії запитань і відповідей за участю оцінювачів та ключових представників організації [25]. Такий підхід дає змогу вийти за межі формальної перевірки документів і краще зрозуміти реальний стан кіберстійкості. Зокрема, він дозволяє визначити, чи пов'язані виявлені проблеми переважно з технічними недоліками, чи є наслідком недостатньо сформованих процедур, нечіткого розподілу відповідальності або управлінських рішень. Додатковою перевагою є те, що результати CRR можуть бути співвіднесені з NIST Cybersecurity Framework, що спрощує їх подальше використання в загальній системі управління кіберризиками [26].

Якщо узагальнити, основна цінність CRR полягає у його зрозумілій структурі та придатності для проведення внутрішніх оцінювань організаційної готовності до кіберінцидентів. Водночас, як і в інших підходах, що спираються на інтерв'ювання та самооцінювання, точність результатів значною мірою залежить від повноти наданої інформації, а також від рівня підготовки та обізнаності учасників оцінювання. Для енергетичного сектору цей інструмент може слугувати сильною організаційно-процесною основою, однак при практичному застосуванні його

доцільно доповнювати спеціалізованими технічними вимогами, що враховують особливості промислових систем керування та середовищ ОТ/ІКС.

1.4 Порівняльний аналіз фреймворків оцінювання кіберстійкості

Оскільки кожен із проаналізованих фреймворків має власні сильні та слабкі сторони, у роботі проведено їх порівняльний аналіз за низкою якісних показників. З цією метою фреймворки зіставлено за структурою, цільовим призначенням, способом проведення оцінювання, характером результатів і придатністю до практичного застосування в умовах української енергетичної інфраструктури. Розширену порівняльну характеристику розглянутих підходів узагальнено в таблиці 1.1.

Шотландський метод оцінки не призначений безпосередньо для енергетичних середовищ, а насамперед орієнтований на організації публічного сектору Шотландії, що обмежує його пряме застосування. Оцінювання в межах цього підходу відбувається за трьома рівнями: Baseline, Target та Advanced та охоплює чотири домени. Результати можуть бути відображені у вигляді відсоткового прогресу та розрахунково-аналітичної індикації. Відстеження досягнутого рівня та динаміки змін забезпечується завдяки використанню узагальненої матриці категорій, яка сформована на основі кількох стандартів і методологій [19]. Сильними сторонами цього підходу є простота самооцінювання, наочність подання результатів і зручність для використання на управлінському рівні.

Модель C2M2 охоплює 10 доменів, у межах яких практики згруповані за цілями й рівнями зрілості MIL0–MIL3. До цих доменів належать, зокрема, управління активами, загрозами та вразливостями, ризиками, доступом, ситуаційною обізнаністю, реагуванням і безперервністю, взаємодією з третіми сторонами, персоналом, архітектурою та управлінням програмою кібербезпеки [20]. Перевага цього підходу полягає в тому, що він забезпечує структурований механізм самооцінювання, має глибоку структуру та історично пов'язаний з

енергетичним сектором. Саме тому цей фреймворк є найбільш придатною основою для подальшої адаптації.

Фреймворк САФ побудований не як перелік контрольних заходів, а як результативно-орієнтована модель оцінювання кіберстійкості. Його мета полягає в системному оцінюванні того, наскільки організація управляє кіберризиками щодо своїх критично важливих функцій. САФ включає 4 високорівневі цілі та 14 принципів, а деталізація здійснюється через критерії якості. Додатковою перевагою цього підходу є можливість застосування як у форматі самооцінювання, так і в межах зовнішнього нагляду. Окреме значення мають профілі: Basic і Enhanced, які дозволяють визначати цільовий рівень стійкості залежно від рівня загроз [22]. У контексті адаптації до українських умов САФ є цінним насамперед як джерело логіки оцінювання станів і очікуваних результатів.

CRR є інтерв'ювальним інструментом оцінювання кіберстійкості. Його структура охоплює 10 доменів, серед яких управління активами, контролюми, конфігураціями і змінами, вразливостями, інцидентами, безперервністю сервісів, ризиками, зовнішніми залежностями, навчанням і обізнаністю, а також ситуаційною обізнаністю. Формат оцінювання передбачає використання набору питань із варіантами відповідей: Yes, No, Incomplete [25]. Це робить його придатним для збору якісної інформації про реальний стан процесів в організації та для виявлення слабких місць у її підготовленості до кіберінцидентів.

Окрім загальної характеристики фреймворків, у межах цього дослідження для їх порівняння було обрано також низку додаткових показників: релевантність для енергетичної інфраструктури, наявність готового механізму самооцінювання, глибину й структурованість оцінювання, зручність адаптації та придатність до візуалізації результатів. Релевантність для енергетичної інфраструктури відображає, наскільки підхід відповідає особливостям енергетичних об'єктів; наявність механізму самооцінювання показує, чи може фреймворк бути безпосередньо використаний як основа для практичного інструмента; глибина й

структурованість оцінювання характеризують детальність і комплексність аналізу; зручність адаптації визначає, наскільки легко локалізувати та пристосувати підхід до українського контексту; придатність до візуалізації результатів відображає можливість подання результатів у вигляді таблиць, діаграм і профілів оцінювання.

Таблиця 1.1 – Порівняльна характеристика фреймворків оцінювання

Критерій	Scottish method	C2M2	CAF	CRR
1	2	3	4	5
1. Первинна мета фреймворку	Поетапне підвищення кіберстійкості організацій публічного сектору	Оцінювання та розвиток кібербезпекових спроможностей організації	Оцінювання управління кіберризиками щодо критичних функцій	Оцінювання операційної стійкості та кібербезпекових практик організації
2. Цільова сфера застосування	Публічний сектор, державні та муніципальні організації	Передусім енергетичний сектор	Організації, що забезпечують критично важливі функції та сервіси	Організації різних типів
3. Структура фреймворку	Стадії Baseline / Target / Advanced, доменний підхід, прогрес за напрямками	10 доменів, цілі, практики, рівні зрілості MIL0–MIL3	4 високорівневі цілі, 14 принципів, Indicators of Good Practice	10 доменів, інтерв'ювальні питання, логіка gap analysis

Продовження таблиці 1.1

1	2	3	4	5
4. Наявність механізму самооцінювання	self-assessment tool	self-evaluation tool	self-assessment, але потребує більшої експертної інтерпретації	self-assessment kit та інтерв'ювальний формат
5. Формат результатів	Відсоток прогресу, RAG-індикація, стадійний профіль	Графічний і доменний профіль зрілості	Ступінь досягнення outcome-станів за принципами	Виявлення прогалин, якісна оцінка стану процесів
6. Релевантність для енергетичної інфраструктури	Низька–середня	Висока	Середня–висока	Середня
7. Охоплення IT/OT-середовища	Переважно IT-орієнтований підхід	Прямо охоплює IT та OT-середовища	Може застосовуватися до середовищ критичних функцій, але без такої ж прямої галузевої деталізації, як C2M2	Переважно організаційно-процесний підхід, без вираженої OT-спеціалізації

Кінець таблиці 1.1

1	2	3	4	5
8. Зручність адаптації до українського контексту	Середня	Висока	Висока	Середня–висока
9. Придатність як основа практичного інструмента профілювання кіберстійкості	Середня	Висока	Висока, але більше як логіка критеріїв та цільових станів	Середня–висока, особливо як база для опитувальних елементів

З таблиці видно, що жоден із розглянутих підходів окремо не покриває всі потреби цієї роботи. C2M2 є найсильнішим за структурою та галузевою релевантністю, але потребує доповнення інтерв'ювальним механізмом, шкалою станів і зручним управлінським поданням результатів.

Наступним кроком стало оцінювання придатності кожного фреймворку для адаптації до умов українського об'єкта енергетичної інфраструктури. Для забезпечення можливості кількісного порівняння якісні оцінки релевантності було переведено у бальну шкалу від 1 до 5, де 1 відповідає низькому рівню, а 5 – високому. Проміжні значення інтерпретуються як низький–середній, середній та середній–високий рівні релевантності. Отримані результати допомагають виділити найбільш придатний для адаптації фреймворк, для порівняння їх зображено на діаграмі (Рисунок 1.3).

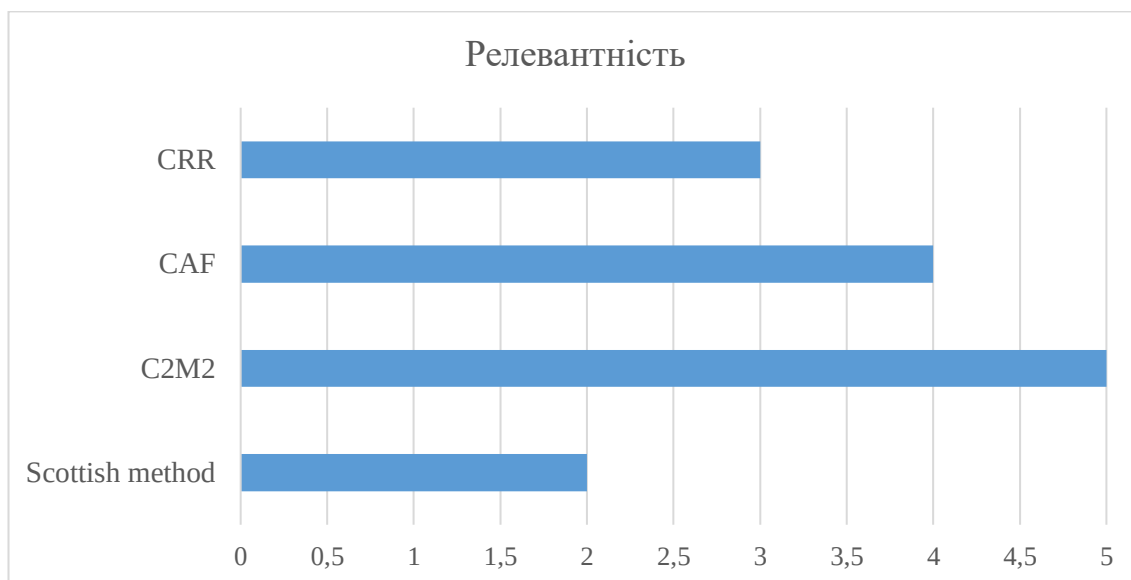


Рисунок 1.3 – Придатність фреймворку до адаптації

За результатами порівняння найбільш придатною основою для адаптації до українського об'єкта енергетичної інфраструктури визначено C2M2. Це зумовлено його початковою орієнтацією на енергетичний сектор, наявністю чіткої доменної структури, а також практичним механізмом самооцінювання.

CAF буде використано завдяки його підходу до оцінки станів: досягнуто, частково досягнуто, не досягнуто [23]. До адаптованої моделі також доцільно включити елементи опитувальника CRR як основу для побудови опитувальних компонентів [24, 25].

Висновки до розділу 1

У першому розділі здійснено комплексний аналітичний огляд сучасних кібератак на об'єкти критичної інфраструктури, зокрема її енергетичного сектору, та визначено їх деструктивні наслідки для безперервності технологічних процесів. Досліджені прецеденти в Україні та за кордоном засвідчили комбінований характер сучасних загроз, спрямованих як на операційні технології (ОТ-середовище), так і на корпоративну ІТ-інфраструктуру підприємств. Доведено, що критичними вразливостями виступають не лише спеціалізовані зразки шкідливого програмного забезпечення, а й базові організаційно-технічні прогалини: недостатня сегментація

мережевих контурів, зловживання легітимними правами доступу та слабкий контроль зовнішніх каналів підключення. Зазначене свідчить про недостатність стандартних захисних заходів і безпосередньо зумовлює доцільність проектування комплексного інформаційного забезпечення для профілювання та кількісного оцінювання кіберстійкості критичних об'єктів.

Також було розглянуто основні фреймворки оцінювання кіберстійкості, які можуть бути використані як основа для самооцінювання та подальшої адаптації до потреб організації. Порівняльний аналіз Scottish method, C2M2, CAF та CRR показав, що ці підходи мають різну спрямованість: шотландський метод є більш зручним для спрощеної організаційної самооцінки, CAF добре підходить для оцінювання стану критично важливих функцій, CRR є практичним інструментом інтерв'ювання та збору якісних даних про стан безпеки. Найбільш придатним методологічним підґрунтям для подальшої адаптації визначено модель C2M2, оскільки цей фреймворк максимально відповідає архітектурним особливостям енергетичної інфраструктури, інтегрує процеси IT/OT-середовищ, має розвинену доменну структуру та містить гнучкі інструменти самооцінювання.

Проте ізольоване використання жодного з чинних світових стандартів не є універсальним рішенням для вітчизняного безпекового контуру. Обмеженість наявних підходів зумовлює обґрунтовану необхідність проектування цілісної архітектури інформаційного забезпечення профілювання. Проектована система має інтегрувати взаємодоповнювальні компоненти міжнародних фреймворків, узгоджуючи їх із функціональними характеристиками української енергосистеми, актуальним ландшафтом воєнних загроз та потребами прикладного кількісного оцінювання кіберстійкості об'єктів критичної інфраструктури.

2 МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОФІЛЮВАННЯ КІБЕРСТІЙКОСТІ

Кожен підхід оцінювання кіберстійкості створювався з урахуванням конкретної галузі, нормативних вимог та організаційної структури. Тому пряме перенесення готової моделі є неефективним: без урахування локального контексту результати оцінювання будуть формальними й не відображатимуть реальних ризиків.

Для енергетичної інфраструктури така адаптація є особливо важливою. Ця галузь охоплює не лише інформаційні системи, а й технологічні процеси, мережеву інфраструктуру та засоби керування. Усі ці складові тісно пов'язані між собою, тому порушення в одному середовищі може позначитися на функціонуванні іншого [20]. За таких умов кіберстійкість слід розуміти ширше, ніж просто захищеність окремих систем. Вона передбачає спроможність організації підтримувати виконання критично важливих функцій під час інциденту, обмежувати його наслідки та відновлювати нормальну роботу. Отже, під час оцінювання необхідно враховувати не лише технічний захист, а й організаційні, операційні та управлінські аспекти. Для українського контексту це додатково ускладнюється постійними кіберзагрозами, атаками на критичну інфраструктуру та потребою пристосовувати міжнародні підходи до вітчизняних умов [8].

Інформаційне забезпечення профілювання має охоплювати управління ризиками, захист критичних активів, виявлення кіберподій, реагування на інциденти, відновлення після них, а також підтримання роботи ключових функцій у складних умовах. Таким чином, воно має бути комплексним і орієнтованим на реальний результат, а не лише на формальне виконання вимог [21–24]. Окрему увагу в межах такого підходу слід приділяти чутливим цифровим активам, тобто тим інформаційним, програмним, мережевим або керуючим компонентам, компрометація яких може безпосередньо вплинути на виконання критичних функцій об'єкта. Саме такі активи мають бути визначені як пріоритетні для

впровадження найважливіших заходів безпеки, оскільки їх ураження здатне спричинити найбільш суттєві операційні або технологічні наслідки.

Важливим аспектом є врахування ролей і відповідальності персоналу. Кіберстійкість залежить не лише від технічних рішень, а й від того, наскільки чітко в організації визначено, хто саме відповідає за управління ризиками, адміністрування систем, реагування на інциденти, підтримку технологічного середовища та взаємодію між різними рівнями управління. Тому адаптований підхід має враховувати організаційну структуру, посадові ролі та розподіл функцій між працівниками [24]. Схему утворення такого механізму наведено на рисунку 2.1.

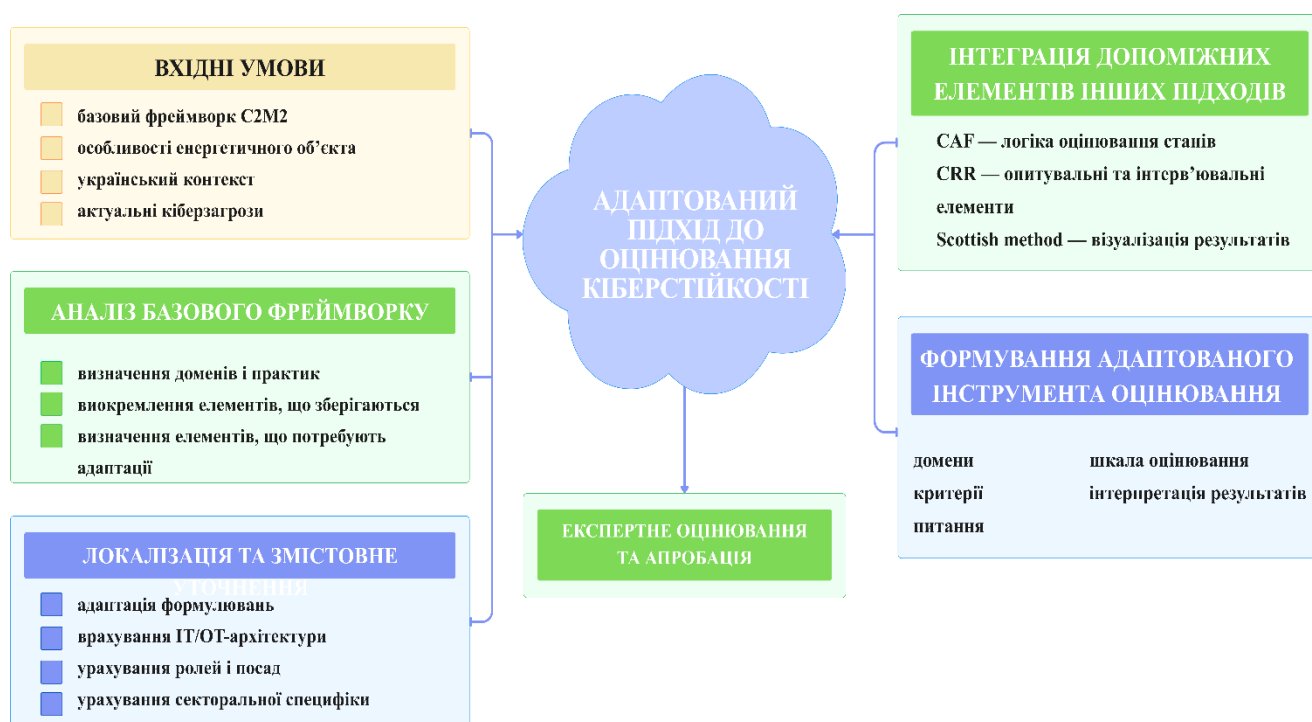


Рисунок 2.1 – Загальна схема процесу адаптації інструмента профілювання кіберстійкості

Методично процес адаптації інструмента профілювання кіберстійкості має ієрархічну структуру та реалізується послідовно. Спочатку потрібно визначити, які елементи базового фреймворку можна використати без суттєвих змін, а які потребують перегляду. Далі слід сформулювати вимоги до майбутнього інструмента профілювання кіберстійкості з урахуванням особливостей енергетичного об'єкта.

Після цього потрібно визначити, як саме будуть інтерпретуватися результати оцінювання і за якими критеріями визначатиметься рівень кіберстійкості. У підсумку, підхід має бути побудований так, щоб його можна було використовувати не лише для аналізу, а й як практичний інструмент самооцінювання та подальшого вдосконалення системи захисту. Саме такий комплексний підхід формує основу для отримання об'єктивної оцінки стійкості.

Далі у цьому розділі послідовно розглядаються: обґрунтування базового підходу для адаптації, роль допоміжних елементів інших фреймворків, формування вимог до структури адаптованого інструмента, концептуальна побудова майбутнього підходу та методичні засади використання експертних оцінок.

2.1 Обґрунтування базового підходу для подальшої адаптації

Основною причиною вибору C2M2 є його зв'язок з енергетичним сектором і придатність до оцінювання організацій, робота яких залежить від взаємодії інформаційних і технологічних систем. Для енергетичного об'єкта це має принципове значення, оскільки його кіберстійкість визначається не лише станом корпоративної IT-інфраструктури, а й захищеністю ОТ-компонентів, засобів керування, мережевої архітектури, процедур реагування та організаційної взаємодії. Саме тому базовий фреймворк має охоплювати як технічні, так і управлінські аспекти кібербезпеки [22, 23].

Важливою перевагою C2M2 є його чітка внутрішня структура. У версії 2.1 модель охоплює десять доменів, які разом формують цілісне бачення кіберстійкості організації: управління ризиками, активами, доступом, ситуаційною обізнаністю, реагуванням на інциденти, безперервністю діяльності, персоналом, третіми сторонами, архітектурою та програмою кібербезпеки. Така структура дає змогу не створювати модель оцінювання з нуля, а спиратися на вже систематизований набір напрямів.

Практичну цінність C2M2 підсилює використання рівнів MIL0–MIL3, які дозволяють оцінювати не лише факт наявності практики, а й ступінь її документування, регулярність застосування та керованість [21]. У цій роботі така логіка використовується для переходу від простого переліку питань до змістовної шкали оцінювання, що відображає реальний стан розвитку кіберстійкості за окремими напрямками.

Водночас C2M2 не може бути без змін перенесений на український об'єкт енергетичної інфраструктури. Модель сформована в іншому нормативному та організаційному середовищі, тому окремі її елементи потребують адаптації до локального контексту. Це стосується формулювання практик, способу збору відповідей, урахування посадових ролей, експертного оцінювання та узгодження моделі з реальною архітектурою українських об'єктів критичної інфраструктури.

Окремої адаптації потребує блок, пов'язаний із третіми сторонами. У загальному вигляді C2M2 враховує постачальників, партнерів і зовнішні залежності, однак для енергетичної інфраструктури України цього недостатньо. В адаптованому інструменті цей напрям конкретизований через питання щодо сервісних організацій, постачальників програмного забезпечення й обладнання, підрядників із віддаленим доступом, регламенту сторонніх підключень, перевірки постачальників та впливу зовнішніх організацій на безперервність критичних функцій [26].

Компрометація енергооб'єкта не завжди є наслідком складної цілеспрямованої атаки. Вона може виникати через слабке адміністрування доступу, помилки персоналу, неналежний контроль підрядників або порушення експлуатаційної дисципліни. Тому адаптований інструмент має оцінювати не лише технічні засоби захисту, а й організаційні умови, у яких ці засоби застосовуються.

Практики реагування та відновлення також потребують уточнення з урахуванням українського контексту. Для енергетичного об'єкта важливо оцінювати наявність сценаріїв реагування для різних типів інцидентів, визначення

пріоритетності відновлення критичних функцій, розподіл ролей між учасниками реагування, протоколи взаємодії з регуляторами, постачальниками, сервісними організаціями та CERT-структурами. В умовах воєнного стану особливого значення набуває здатність персоналу переходити до ізолюваного або ручного режиму керування у разі втрати зв'язку з централізованими системами [8, 11, 17, 23, 25].

Отже, C2M2 доцільно розглядати як базовий, але не єдиний фреймворк для побудови адаптованого інструмента. Він задає доменну структуру, логіку зрілості та основу для самооцінювання, однак для практичної реалізації цього недостатньо. Тому надалі його доцільно доповнити логікою оцінювання станів із CAF, інтерв'ювальним механізмом CRR та елементами наочного подання результатів, характерними для шотландського підходу.

2.2 Засади використання допоміжних елементів інших підходів

Попри релевантність C2M2 для вітчизняного енергетичного сектору, його ізолюване використання не дозволяє повною мірою вирішити поставлені у дослідженні завдання. Обмеженість будь-якого окремого фреймворку зумовлює необхідність інтеграції додаткових методологічних елементів для побудови цілісного інформаційного забезпечення профілювання кіберстійкості.

C2M2 забезпечує найбільш цілісну структурну базу, проте порівняльний аналіз показує, що ця модель менш деталізовано задає логіку оцінювання станів, не орієнтується на інтерв'ювальний спосіб збору інформації та не містить інструментів оперативного подання результатів для управлінського рівня [21–24]. Через це CAF, CRR та шотландський метод розглядаються не як альтернативи C2M2, а як комплементарні джерела компонентів, що інтегруються в єдину систему.

Таким чином, у роботі модель C2M2 виступає структурним каркасом профілювання, тоді як фреймворки CAF, CRR та запозичені елементи Scottish

method використовуються вибірково – у тих частинах, де вони дозволяють зробити розроблене інформаційне забезпечення більш змістовним, практичним та зручним для експериментальної апробації.

2.2.1 Використання допоміжних елементів CAF

Фреймворк CAF інтегровано як допоміжне джерело логіки оцінювання результативного стану кіберстійкості розробленого інформаційного забезпечення, а не як його окрему структурну основу. Головна перевага підходу полягає в орієнтації на фактичне досягнення організацією очікуваного стану захищеності критично важливих функцій, а не лише на формальну наявність засобів безпеки [22]. Це має визначальне значення для енергетичного сектору, де першочерговим завданням є підтримання безперервності технологічних процесів безпосередньо під час деструктивного кібервпливу.

Окрему практичну цінність для цієї роботи мають Indicators of Good Practice (IGP), які використовуються в CAF для деталізації очікуваних результатів [23]. Цей підхід використано в адаптованій моделі, оскільки він дозволяє описувати не лише сам критерій оцінювання, а й ознаки того, що відповідний стан дійсно досягнуто. Завдяки цьому оцінювання мінімізує суб'єктивізм експертних суджень, спираючись на специфічні операційні показники кіберфізичного середовища. Зокрема, у моделі враховується готовність персоналу до оперативного переходу в ручний режим керування, здатність підтримувати критичні функції за часткової недоступності цифрових систем та наявність узгоджених регламентів взаємодії між IT- і OT-підрозділами.

Ще одним важливим елементом Cyber Assessment Framework є використання CAF Profiles, зокрема Basic Profile і Enhanced Profile [22]. Для майбутньої адаптації ця логіка є корисною тим, що дає можливість встановлювати різні цільові стани кіберстійкості залежно від типу об'єкта, його функцій та рівня критичності. У контексті енергетичної інфраструктури це означає, що вимоги до кіберстійкості можуть бути не однаковими для всіх об'єктів. Для менш критичного елемента

інфраструктури може бути достатнім базовий профіль, тоді як для об'єкта з вищою критичністю доцільно орієнтуватися на посилений рівень очікуваних результатів.

У синтезі фреймворків практики C2M2 виступають об'єктом оцінювання, тоді як методологія CAF визначає критерії успішності через очікувані результати та індикатори належної практики. Це дозволяє оцінювати стан реалізації кожного елемента за трибальною якісною шкалою на основі конкретних перевірюваних ознак, що формує базу для математичного агрегування та кількісної інтерпретації профілю.

Взаємозв'язок між елементами C2M2 і CAF у межах проектного інформаційного забезпечення профілювання наочно представлено в таблиці 2.1.

Таблиця 2.1 – Розподіл ролей C2M2 та CAF в адаптованому інструменті оцінювання

Компонент адаптованої моделі	Джерело	Практична роль
Доменна структура	C2M2	Забезпечує повноту охоплення напрямів безпеки
Практики та напрями оцінювання	C2M2	Формують зміст і логіку побудови інструмента
Очікувані стани реалізації	CAF	Дозволяють визначати цільовий результат для кожної практики
Індикатори належної практики (IGP)	CAF	Мінімізація суб'єктивності експертних оцінок
Профілі оцінювання (Basic / Enhanced)	CAF	Адаптивність інструмента до об'єктів різної категорії критичності

Таблиця 2.1 показує, що CAF було використано не як базовий каркас моделі, а як методичний інструмент для формування критеріїв оцінювання, опису очікуваних станів і побудови диференційованих цільових профілів кіберстійкості.

Саме в такій ролі цей підхід найкраще доповнює C2M2 і підсилює майбутній адаптований інструмент.

2.2.2 Використання допоміжних елементів CRR

Фреймворк Cyber Resilience Review (CRR), розроблений CISA, використовується як джерело інтерв'ювального формату та логіки збору якісних даних. Ключова перевага цього підходу полягає у фокусі на фактичній операційній готовності установи, а не лише на формальному аудиті документів.

На відміну від автоматизованого анкетування, використання структурованого інтерв'ю з представниками різних підрозділів та наявність детального методичного супроводу мінімізує ризики суб'єктивного чи помилкового трактування запитань. [24]. У межах адаптованого інструмента це корисно, оскільки в практичній частині оцінювання залучено експертні судження, а також ураховано посади, ролі й сфери відповідальності різних категорій персоналу. У такому разі частина питань орієнтована на керівництво, частина – на ІТ-фахівців, частина – на ОТ/АСУТП-персонал або експлуатаційні служби.

Методична цінність CRR підсилюється наявністю матеріалів, що дозволяють співвідносити результати оцінювання із NIST Cybersecurity Framework. Використання офіційних матриць відповідності (crosswalks) дає змогу узгодити результати інтерв'ювання з вимогами NIST CSF. Це підсилює методичну обґрунтованість дослідження, оскільки адаптований інструментарій ґрунтується не лише на практичному досвіді CISA, а й на загальновизнаних світових стандартах управління кіберризиками [27].

Важливою діагностичною рисою CRR є аналіз внутрішніх організаційних суперечностей для виявлення прихованих прогалин у процесах. Відсутність єдиної узгодженої позиції між підрозділами або труднощі під час інтерпретації практик безпосередньо свідчать про недостатню зрілість відповідного процесу. Такий підхід дозволяє зафіксувати не лише номінальний стан захисту, а й реальний рівень

координації між службами під час реагування на інциденти. Для збереження простоти первинного збору даних якісні відповіді респондентів фіксуються у трирівневому форматі «Yes / No / Incomplete» [25], що створює передумови для подальшого переведення лінгвістичних оцінок у числові еквіваленти.

Логіку інтеграції цього фреймворку у загальну структуру інформаційного забезпечення унаочнено на рисунку 2.2. На відміну від моделі C2M2, яка формує базовий архітектурний каркас і доменну структуру, інструменти CRR застосовуються безпосередньо як прикладний механізм верифікації експертних даних та експрес-діагностики організаційних розривів.

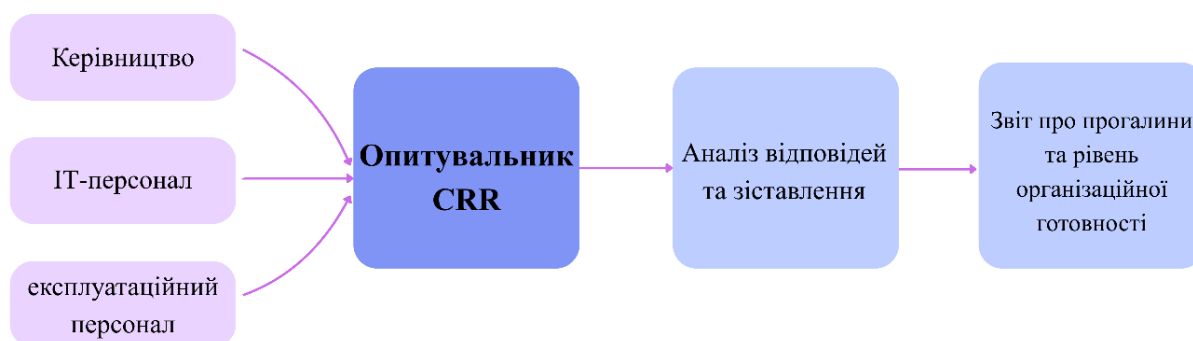


Рисунок 2.2 – Логіка використання опитувальника CRR в експертному оцінюванні

Представлена на рисунку 2.2 логіка фреймворку CRR дозволяє організувати системний збір даних від персоналу та сформувані об’єктивне уявлення про рівень організаційної готовності підприємства. Таке рішення забезпечує валідацію експертних оцінок через призму посадових ролей та реального стану внутрішніх процесів об’єкта.

Для енергетичної інфраструктури це має визначальне значення, оскільки її кіберстійкість прямо залежить від чіткої координації між технічним, експлуатаційним і управлінським рівнями. Тому компоненти CRR використано для побудови контуру експертного оцінювання, де відповіді респондентів допомагають перевірити не формальну наявність регламентів, а їхню практичну зрозумілість, узгодженість та дієвість в умовах кризових ситуацій. Насамперед це стосується

практик реагування, управління залежностями, розподілу відповідальності та підтримання безперервності функціонування активів.

Інтеграція інтерв'ювального формату, методичного супроводу до запитань, алгоритмів виявлення організаційних розривів та прив'язка критеріїв до посадових функцій роблять розроблене інформаційне забезпечення не лише чітко структурованим, а й придатним для збору реальних даних під час експериментальної апробації.

2.2.3 Використання окремих елементів шотландського підходу

Scottish method не є найбільш придатною основою для профілювання кіберстійкості енергетичної інфраструктури, оскільки цей підхід орієнтований насамперед на організації публічного сектору [18, 19]. Водночас він містить корисні елементи, які доцільно використати для узагальнення, візуалізації та подання результатів оцінювання на управлінському рівні.

Передусім ідеться про поетапний підхід, побудований на рівнях Baseline, Target і Advanced [19]. Така трирівнева логіка є зручною для узагальнення результатів оцінювання, оскільки дозволяє представити складніші показники та рівні зрілості у спрощеному вигляді. У межах адаптованого інструмента це використано для формування зрозумілих орієнтирів розвитку кіберстійкості, які полегшують визначення пріоритетних напрямів удосконалення.

Окрему увагу доцільно приділити способам візуалізації результатів. Шотландський підхід передбачає використання наочних графічних форм подання, зокрема радарних діаграм, які дозволяють на одній площині зіставити фактичний стан за різними доменами з цільовим профілем. Для енергетичного об'єкта, де в оцінюванні задіяні різні служби та напрями діяльності, такий формат є корисним для швидкого виявлення найбільш слабких місць і представлення загальної картини кіберстійкості.

Не менш важливим є і управлінський аспект цього підходу. Scottish method підтримує подання результатів оцінювання у формі, зрозумілій не лише технічним фахівцям, а й керівництву. Це дає змогу пов'язати технічні результати оцінювання з ризиками, пріоритетами вдосконалення та потребами розвитку організації, що підвищує практичну цінність підсумкового звіту.

Таким чином, Scottish method доцільно розглядати як допоміжне джерело інструментів для візуалізації, узагальнення та інтерпретації результатів на управлінському рівні. У межах адаптованого підходу такі елементи можуть використовуватися на завершальному етапі представлення результатів – після структурного оцінювання за C2M2, уточнення критеріїв через CAF і збору експертних відповідей за логікою CRR.

2.2.4 Узагальнення ролі допоміжних підходів

Для узагальнення ролі допоміжних елементів інших підходів доцільно подати їх у вигляді порівняльної таблиці, яка відображає, що саме запозичується з кожного фреймворку, яку практичну роль це відіграє в адаптованому інструменті та як такі елементи поєднуються з базовою логікою C2M2.

Елементи інших підходів не замінюють C2M2 як базову основу адаптації, а підсилюють окремі складові майбутнього інструмента профілювання. C2M2 визначає, що саме має оцінюватися, тобто задає домени, напрями та загальну логіку зрілості практик. CAF уточнює, як інтерпретувати стан реалізації цих практик через логіку “досягнуто / частково досягнуто / не досягнуто” та критерії належної практики. CRR забезпечує інтерв'ювальний і рольовий механізм збору даних, що дозволяє врахувати експертні відповіді різних категорій персоналу та виявити організаційні прогалини. Scottish method використовується для узагальнення й наочного представлення результатів, зокрема у формі профілю, зрозумілого для управлінського рівня.

Таблиця 2.2 – Допоміжні елементи інших підходів, що використовуються в адаптованому інструменті

Підхід	Що запозичується	Практична роль	Зв'язок із С2М2
1	2	3	4
CAF	Очікувані стани реалізації; Indicators of Good Practice (IGP); профілі Basic / Enhanced	Формування критеріїв успішності, зменшення суб'єктивності оцінювання, встановлення різних цільових рівнів для об'єктів різної критичності	Доменна структура і практики беруться з С2М2, а логіка оцінювання станів реалізації – з CAF
CRR	Інтерв'ювальний формат; структуровані запитання; методичний супровід до запитань; виявлення прогалин через відповіді; прив'язка до ролей	Побудова опитувального та експертного компонента, збір даних від різних категорій персоналу, перевірка узгодженості процесів	Практики С2М2 оцінюються через запитання й експертні відповіді, організовані за логікою CRR

Кінець таблиці 2.2

1	2	3	4
Scottish method	Поетапний підхід; спрощене профілювання результатів; наочне подання; орієнтація на управлінський рівень	Узагальнення результатів, візуалізація профілю кіберстійкості та підготовка матеріалів для управлінського рівня	Результати оцінювання, отримані на основі C2M2, можуть бути подані у спрощеній поетапній формі для управлінської інтерпретації

2.3 Формування вимог до адаптованого інструмента профілювання кіберстійкості

Наступним логічним кроком після обґрунтування базового фреймворку та визначення ролі допоміжних елементів інших підходів є формування вимог до адаптованого інструмента профілювання кіберстійкості, який має бути придатним до використання на об'єкті енергетичної інфраструктури України та узгодженим із практичними потребами оцінювання.

Загальна мета оцінної діяльності полягає у формуванні обґрунтованого рівня обізнаності про стан певного об'єкта. У багатьох випадках цей стан співвідноситься з очікуваннями щодо відповідності стандарту, профілю, нормативно-правовому акту або визначеним внутрішнім вимогам. Для цього оцінювач застосовує одну чи кілька методик, які дозволяють визначити, описати або підтвердити фактичний стан об'єкта за встановленими критеріями.

Під час проектування критеріїв, запитань і цільових орієнтирів розробленого інформаційного забезпечення використано логіку SMART як допоміжний метод формування практичних вимог. Відповідно до цього підходу, елементи оцінювання

мають бути конкретними, вимірюваними, досяжними з погляду практичного впровадження, релевантними до критичних функцій об'єкта та чітко прив'язаними до операційних чи часових меж використання [28].

Таке моделювання дозволяє уникнути абстрактних формулювань, роблячи систему придатною для верифікованого самооцінювання та подальшої якісної інтерпретації результатів. Кожен критерій формулюється так, щоб респондент міг надати однозначну перевірювану відповідь, що мінімізує суб'єктивізм експертних суджень і покращує придатність первинних даних до подальшої математичної обробки.

Необхідність формування таких вимог зумовлена тим, що об'єкти енергетичної інфраструктури функціонують у складному середовищі, де поєднуються інформаційні системи, технологічні процеси, засоби диспетчерського та локального керування, мережеві сервіси, віддалений доступ, зовнішні підрядники та різні рівні відповідальності персоналу. За таких умов інструмент профілювання кіберстійкості не може бути зведений лише до перевірки наявності технічних засобів захисту. Він повинен враховувати як ІТ-, так і ОТ-компоненти, здатність організації підтримувати виконання критичних функцій, готовність до реагування на інциденти, а також організаційні механізми координації та управління [20–25].

З методичного погляду сформовані вимоги розподілено на п'ять взаємопов'язаних груп: структурні, функціональні, галузеві, організаційні та аналітичні. Така класифікація дозволяє всебічно охопити як внутрішню архітектуру інформаційного забезпечення, так і умови його практичного застосування, логіку збору даних, особливості інтерпретації результатів і загальну придатність моделі до використання в умовах українського енергетичного сектору.

2.3.1 Структурні вимоги

Структурні вимоги регламентують архітектуру інформаційного забезпечення на основі його послідовного поділу. Система складається з окремих доменів, які відображають ключові складові кіберстійкості об'єкта. Побудова за принципом «від загального до конкретного» передбачає деталізацію кожного напрямку через систему критеріїв та цільових запитань, що забезпечує повноту дослідження без пропуску важливих елементів.

Супутньою умовою є можливість ізольованого аналізу кожного домену. Це дозволяє уникнути усереднення розрахункових даних, яке часто приховує специфічні вразливості, та дає змогу оцінювати реальний стан окремих процесів. У контексті енергооб'єктів такий аналіз є життєво необхідним, оскільки критичні ризики зазвичай локалізуються у вузьких сферах (як-от сторонній доступ підрядників чи аварійне реагування) і не мають нівелюватися за рахунок високих балів у інших, більш розвинених областях безпеки.

2.3.2 Функціональні вимоги

Інструмент повинен бути придатним до практичного самооцінювання та застосування на реальному об'єкті. Це означає, що його побудова має бути достатньо зрозумілою для користувачів, а формулювання критеріїв і запитань – однозначними та придатними до інтерпретації різними категоріями учасників оцінювання. Інструмент не повинен вимагати надмірно складної підготовки для використання, але водночас має забезпечувати достатню глибину отриманих результатів.

Крім того, функціонально важливою є можливість збору інформації з різних джерел. Частина даних може надходити від технічного персоналу, частина – від фахівців із кібербезпеки, частина – від управлінського або експлуатаційного рівня. Отже, інструмент має підтримувати багаторівневий збір інформації, поєднувати

елементи самооцінювання та експертного опитування, а також бути придатним до використання в умовах обмеженого часу й ресурсів.

Окремою функціональною вимогою є наявність чіткого методичного алгоритму обчислення результатів. Це означає, що інструмент повинен містити зрозумілий порядок переходу від окремих відповідей або оцінок до підсумкових значень за критеріями, доменами та загальним профілем кіберстійкості. У межах адаптованого підходу така логіка може бути реалізована через адитивну модель із числовим представленням відповідей та ваговими коефіцієнтами для окремих доменів. Така вимога є принциповою для забезпечення відтворюваності оцінювання, оскільки результати мають бути однаково інтерпретовані незалежно від того, хто саме проводить самооцінювання.

2.3.3 Галузеві вимоги

Наступними йдуть вимоги, які впливають безпосередньо зі специфіки енергетичної інфраструктури. Адаптований інструмент повинен враховувати взаємозв'язок між ІТ- та ОТ-середовищами, оскільки для енергооб'єкта критично важливими є не лише корпоративні сервіси, а й технологічні системи керування, диспетчеризації, зв'язку та моніторингу. У зв'язку з цим оцінювання має охоплювати не лише традиційні кіберзахисні заходи, а й стани, які безпосередньо впливають на безперервність фізичних процесів.

До галузевих вимог також належить обов'язкове врахування критичних функцій об'єкта. Інструмент має дозволяти співвідносити результати оцінювання не просто з окремими технічними практиками, а з тими функціями, від яких залежить стабільна робота енергетичного об'єкта. Це означає, що в ньому повинні бути відображені питання резервування, безперервності функціонування, захисту віддаленого доступу, сегментації мереж, взаємодії із зовнішніми підрядниками та постачальниками [26].

Окремо слід підкреслити, що для енергетичної інфраструктури важливою є вимога врахування кіберфізичної стійкості об'єкта. Йдеться про спроможність підтримувати безпечне та контрольоване функціонування технологічних процесів навіть за часткової недоступності систем. Саме тому адаптований інструмент має охоплювати не лише цифрові аспекти захисту, а й можливість переходу до резервного, ізольованого або ручного режиму керування, готовність персоналу діяти в таких умовах та перевіряти наявність процедур, що забезпечують безперервність фізичних процесів у разі кіберінциденту. З огляду на це адаптивність реагування є важливою характеристикою майбутнього інструмента, оскільки профіль кіберстійкості має відображати не лише поточний стан захисту, а й готовність об'єкта до зміни режиму функціонування під час інциденту [17].

Для українського контексту особливо важливо врахувати також вплив воєнних загроз, можливість комбінованих атак, обмеженість ресурсів для відновлення, необхідність швидкої локалізації порушень та підтримання роботи критичних функцій навіть у нестабільних умовах. Таким чином, галузеві вимоги мають забезпечити не абстрактний характер оцінювання, а його реальну прив'язку до умов функціонування вітчизняного енергооб'єкта.

2.3.4 Організаційні вимоги

Оскільки кіберстійкість формується не лише через технічні рішення, інструмент повинен враховувати організаційну структуру, розподіл ролей і відповідальності, порядок взаємодії між підрозділами та участь різних категорій персоналу в забезпеченні стійкості. Це означає, що адаптований підхід має бути придатним до застосування за участю керівництва, фахівців з кібербезпеки, ІТ-персоналу, ОТ/АСУТП-фахівців, експлуатаційних служб та, за потреби, представників підрядних організацій.

Організаційно важливою вимогою є також можливість залучення експертних оцінок. Частина характеристик кіберстійкості не може бути визначена виключно шляхом формальної перевірки, тому інструмент повинен допускати використання

професійного судження та зіставлення відповідей різних учасників оцінювання. Це дозволяє не лише зафіксувати наявність або відсутність певної практики, а й перевірити її реальну зрозумілість, узгодженість та придатність до використання в умовах інциденту.

2.3.5 Аналітичні вимоги

Адаптований інструмент має забезпечувати не просто накопичення відповідей, а можливість подальшої інтерпретації результатів. Це означає, що його побудова повинна дозволяти визначати рівень реалізації окремих практик, оцінювати стани за доменами, виявляти найбільш проблемні напрями та формувати узагальнений профіль кіберстійкості. Результати повинні бути придатними як для детального технічного аналізу, так і для стислого представлення на управлінському рівні.

Під час інтерпретації результатів важливо враховувати, що одна й та сама вразливість може впливати одночасно на кілька систем або процесів організації, однак рівень ризику та пріоритет реагування для них можуть істотно відрізнятися. Саме тому оцінювання не повинно обмежуватися лише фіксацією факту наявності проблеми, а має враховувати її реальний вплив на конкретні критичні функції. Іншим важливим аспектом аналізу є виявлення глибинної причини проблеми. Неспроможність визначити й усунути таку причину може призвести до повторного виникнення цієї самої або подібних вразливостей у майбутньому.

Важливою аналітичною вимогою є також можливість візуалізації результатів. Оскільки в адаптованому підході передбачено використання елементів шотландського підходу для узагальнення та представлення профілю, то інструмент повинен підтримувати таку форму вихідних даних, яка створює можливість для побудови діаграми, профілі та зведені таблиці. Це підвищує наочність результатів і полегшує визначення пріоритетів подальшого вдосконалення.

Для узагальнення сформованих вимог доцільно подати їх у вигляді таблиці, яка відображає основні групи вимог, їх зміст та практичне значення для побудови адаптованого інструмента профілювання кіберстійкості.

Таблиця 2.3 – Вимоги до адаптованого інструмента профілювання кіберстійкості

Група вимог	Зміст вимоги	Практичне значення
1	2	3
Структурні	Поділ на домени; ієрархія критеріїв; можливість окремого оцінювання напрямів	Забезпечує повноту охоплення та логічність побудови інструмента
Функціональні	Придатність до самооцінювання; зручність використання на реальному об'єкті; можливість збору даних від різних ролей; чіткий алгоритм обчислення результатів	Дозволяє застосовувати інструмент у практичному середовищі та забезпечує відтворюваність оцінки
Галузеві	Урахування ІТ/ОТ, критичних функцій, сегментації, віддаленого доступу, резервування, підрядників, реагування та відновлення, переходу до ручного або ізольованого режиму	Забезпечує відповідність специфіці енергетичної інфраструктури та вимогам кіберфізичної стійкості

Кінець таблиці 2.3

1	2	3
Організаційні	Урахування посад, відповідальності, експертних оцінок, багаторівневої участі персоналу	Дозволяє поєднати технічну та управлінську складові кіберстійкості
Аналітичні	Інтерпретація результатів, візуалізація, виявлення пріоритетних слабких місць	Перетворює результати оцінювання на основу для подальших управлінських і технічних рішень

Таблиця 2.3 узагальнює сформовані вимоги до адаптованого інструмента профілювання кіберстійкості. Вони показують, що майбутній підхід має бути одночасно структурованим, придатним до практичного використання, враховувати специфіку енергетичної інфраструктури, спиратися на багаторівневу участь персоналу, забезпечувати відтворюваність результатів і підтримувати можливість змістовної інтерпретації отриманих оцінок. Саме така багаторівнева система вимог дає змогу перейти від загальної методології до побудови цілісної моделі оцінювання.

2.4 Концептуальна побудова адаптованого підходу

Архітектура розробленого інформаційного забезпечення визначає склад його структурних компонентів, логіку їхньої взаємодії та механізми трансформації вихідних даних у підсумкові показники кіберстійкості. Проєктована система поєднує базову доменну структуру, локалізовані критерії оцінювання, експертно-опитувальний контур, логіку визначення станів реалізації практик, алгоритми

агрегування результатів та інструменти формування підсумкового профілю стійкості енергооб'єкта.

Структурний каркас моделі формує доменна архітектура, яка задає основні напрями аналізу. У межах дослідження вона спирається на функціональні домени фреймворку C2M2 [22, 23], що слугують основою для диференціації процесів безпеки за окремими областями.

Змістовне наповнення доменів конкретизує базові напрями з урахуванням специфіки вітчизняного енергетичного сектору. До контуру оцінювання інтегровано критерії, пов'язані з безпекою технологічних мереж (ОТ-середовища), сегментацією ІТ/ОТ-контурів, захистом віддаленого доступу, управлінням ланцюгами постачання та підтриманням критичних функцій під час інцидентів. Це дозволяє пов'язати концептуальну логіку з реальними вимогами кіберфізичної безпеки підприємства.

Оцінювання стану реалізації практик здійснюється на основі трирівневої якісної шкали («досягнуто / частково досягнуто / не досягнуто») [22, 23], яка доповнюється індикаторами належної практики. Таке рішення забезпечує перехід від простого переліку вимог до об'єктивного аналізу фактичного стану кіберстійкості системи.

Первинний збір даних реалізовано через експертно-опитувальний інструментарій, призначений для отримання структурованих відповідей від різних категорій респондентів: керівництва, фахівців з кібербезпеки, ІТ- та ОТ-персоналу, а також операційних служб [24, 25]. Цей механізм забезпечує багаторольову крос-верифікацію даних, сприяючи виявленню прихованих організаційних розривів та слабких місць у взаємодії підрозділів.

Математична обробка та агрегування зібраних відповідей трансформують локальні оцінки запитань в інтегральні показники критеріїв і доменів. Впровадження адитивної моделі та системи вагових коефіцієнтів дозволяє

врахувати різну значущість окремих процесів для безперервності виробничого циклу енергооб'єкта, гарантуючи відтворюваність та об'єктивність результатів.

Підсумковим етапом є побудова результуючого профілю кіберстійкості та інтерпретація отриманих індексів. Результати відображаються у формі, придатній як для поглибленого технічного аналізу, так і для прийняття управлінських рішень, а цільові орієнтири моделі узгоджуються з категоріями критичності об'єктів інфраструктури [19, 22]. Повну структуру формування підходу показано на схемі 2.3.

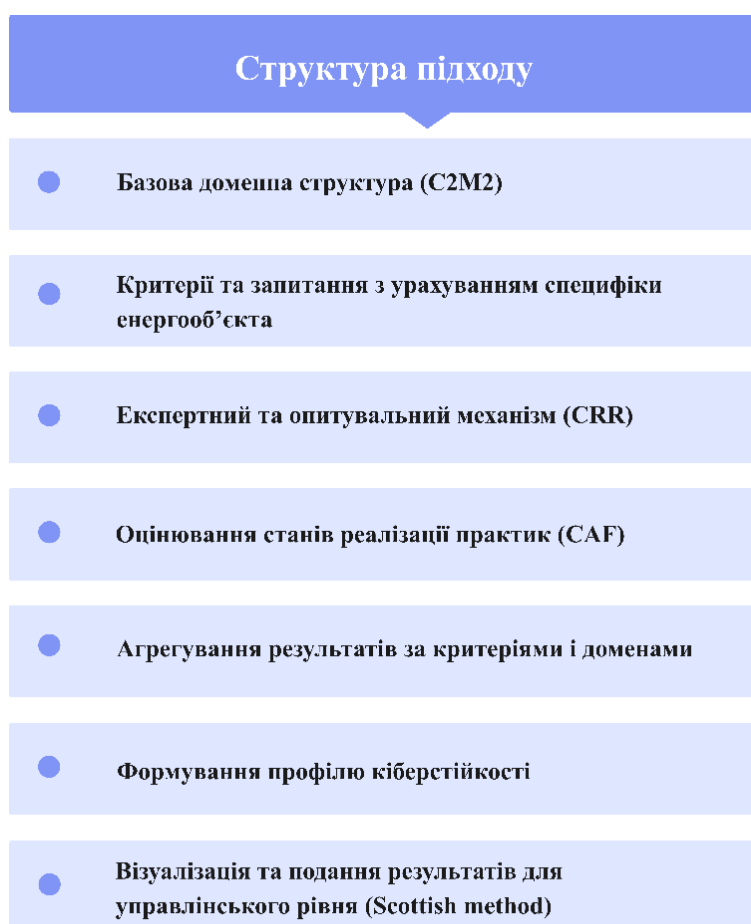


Рисунок 2.3 – Концептуальна структура адаптованого підходу оцінювання кіберстійкості

Як показано на рисунку 2.3, адаптований підхід формується як багаторівнева система, у якій кожен етап виконує окрему функцію: C2M2 задає структурну основу, CAF визначає логіку оцінювання станів, CRR забезпечує механізм збору

експертних даних, а *Scottish method* використовується для узагальнення та представлення результатів. Така модель показує місце кожного структурного компонента та створює основу для наступного етапу – обґрунтування використання експертних оцінок.

2.5 Методичне обґрунтування використання експертних оцінок

Методологічна доцільність залучення експертних оцінок обумовлена неможливістю визначення повного рівня кіберстійкості енергооб'єкта суто технічними засобами без урахування його організаційного, операційного та кіберфізичного контексту. Для підприємств енергетичної інфраструктури визначальну роль відіграють не лише номінально впроваджені інструменти захисту, а й якість взаємодії між ІТ- та ОТ-персоналом, готовність до переходу в ізольований або ручний режим керування, чіткість розподілу обов'язків, а також практична придатність регламентів реагування та відновлення під час реальних інцидентів [20–24]. Через це експертні судження розглядаються у дослідженні як необхідне джерело відомостей про фактичний стан захищеності критичних процесів.

Для уникнення суб'єктивізму та перетворення експертного оцінювання на хаотичне анкетування впроваджено три обмежувальні механізми. По-перше, усі запитання жорстко розподілені за доменами та конкретними практиками безпеки. По-друге, опитування має диференційований характер: респонденти надають відповіді лише на ті питання, які входять до їхньої безпосередньої зони компетенції. По-третє, система передбачає порівняльний аналіз результатів різних категорій опитуваних, що дозволяє виявляти не поодинокі слабкі місця, а системні організаційні розриви у розумінні процесів безпеки між підрозділами.

Питання побудови метрик кібервідмовостійкості є важливим для переходу від якісного опису стану об'єкта до кількісної інтерпретації результатів. У дослідженнях, присвячених метрикам оцінки кібервідмовостійкості, підкреслюється необхідність використання показників, які дозволяють не лише

фіксувати наявність окремих заходів безпеки, а й оцінювати здатність системи підтримувати функціонування та відновлюватися після порушень [16]. Це узгоджується з логікою цієї роботи, де експертні відповіді переводяться у числові значення та агрегуються в доменні й інтегральні показники кіберстійкості.

Методична побудова цього контуру спирається на інструменти фреймворку CRR, орієнтованого на проведення структурованих інтерв'ю для збору якісних даних. У межах розробленого інформаційного забезпечення профілювання це передбачає залучення широкого кола стейкхолдерів: вищого керівництва, фахівців з інформаційної безпеки, системних адміністраторів, інженерів АСУТП та експлуатаційних служб. Безпосередньо список ролей, щодо яких проводиться опитування, наведено в таблиці 2.4.

Таблиця 2.4 – Рольова структура респондентів під час апробації

Код	Роль	Кількість респондентів
R1	Вище керівництво	3
R2	Фахівці з кібербезпеки	5
R3	ІТ-персонал	5
R4	ОТ / експлуатація та обслуговування	10
R5	Фізична безпека	6
R6	Підрядники / постачальники	3

Такий багаторівневий збір інформації дозволяє всебічно охопити архітектурні й операційні особливості об'єкта та мінімізувати ризик упередженого чи однобічного трактування його стану.

Важливим аналітичним інструментом експертного оцінювання є механізм крос-верифікації. Зіставлення відповідей різних посадових груп допомагає виявити неузгодженості або лакуни в управлінні процесами [24, 25]. Наприклад, якщо

управлінський апарат вважає інструкцію з реагування на інциденти повністю відпрацьованою, а технічний персонал зазначає відсутність практичних навичок її виконання, така суперечність безпосередньо вказує на недостатню зрілість процесу. У структурою розробленого інформаційного забезпечення експертні оцінки виконують не лише описативну, а й діагностичну функцію. У разі виявлення суттєвих розбіжностей між відповідями респондентів відповідна практика не отримує максимальний бал; така аномалія автоматично знижує підсумковий показник домену або ініціює додаткову технічну перевірку.

Для формалізації експертних суджень і забезпечення можливості математичного аналізу доцільно застосовувати адитивну модель оцінювання. У межах дослідження цей процес базується на синтезі двох підходів: збір первинних даних здійснюється в інтерв'юальному форматі за методикою CRR, а їх подальша інтерпретація – за трибальною шкалою, адаптованою відповідно до логіки CAF.

Практична реалізація передбачає трансформацію відповідей респондентів типу «Yes / No / Incomplete» у числові значення: 1 – «досягнуто», 0,5 – «частково досягнуто» та 0 – «не досягнуто». Відповідність балів та їхніх значень наведено в таблиці 2.5.

Таблиця 2.5 – Шкала оцінювання відповідей

Бал	Стан	Інтерпретація
1	Досягнуто	Практика формалізована, застосовується та підтверджується доказами.
0,5	Частково досягнуто	Практика існує частково, застосовується нерегулярно або підтверджується не всіма ролями.
0	Не досягнуто	Практика відсутня або немає відомостей про її фактичне застосування.

Такий механізм дозволяє конвертувати суб'єктивні описові характеристики у математично агреговані дані, що забезпечує об'єктивність та відтворюваність підсумкових результатів оцінювання. Для кожного питання респондент обирає один із запропонованих варіантів відповіді, який автоматично трансформується у відповідне числове значення для подальшої обробки.

Для наочнішого представлення місця експертних оцінок у межах адаптованого підходу доцільно узагальнити їх роль у формуванні підсумкових результатів у вигляді таблиці 2.6.

Таблиця 2.6 – Роль експертних оцінок у формуванні результатів адаптованого інструмента

Етап	Зміст	Практична роль
1	2	3
Збір відповідей	Отримання оцінок від представників різних ролей	Формує первинні дані про стан практик і процесів
Крос-верифікація	Порівняння відповідей між різними респондентами	Дозволяє виявити суперечності та прогалини
Формалізація	Переведення якісних відповідей у числові значення	Забезпечує перехід від лінгвістичних оцінок до числових значень
Агрегування	Узагальнення оцінок за критеріями, доменами та профілем	Формує підсумкову оцінку кіберстійкості

Кінець таблиці 2.6

1	2	3
Інтерпретація	Визначення сильних і слабких сторін об'єкта	Створює основу для подальших рішень та вдосконалення

Таблиця 2.6 показує, що експертні оцінки виконують не лише функцію збору первинної інформації, а й виступають основою для подальшої формалізації, агрегування та інтерпретації результатів оцінювання.

На концептуальному рівні підсумковий показник окремого домену (D) визначається як зважена сума оцінок станів реалізації практик, що входять до його складу:

$$D = \sum_{i=1}^n (w_i * p_i), \quad (2.1)$$

де D – підсумковий показник домену, w_i – ваговий коефіцієнт i -тої практики у межах домену, а p_i – числове значення оцінки стану її реалізації, n – кількість практик у домені. Сума вагових коефіцієнтів у межах одного домену повинна дорівнювати одиниці. Вагові коефіцієнти w_i визначаються на основі експертного ранжування значущості окремих практик для забезпечення безперервності критичних функцій об'єкта. Це дозволяє зробити модель менш довільною та прив'язати підсумкову оцінку до реальної важливості окремих елементів кіберстійкості.

Подальше агрегування доцільно здійснювати послідовно: спочатку на рівні окремих критеріїв або практик, далі – на рівні доменів, а потім – у межах загального профілю кіберстійкості об'єкта [22, 23]. Для врахування різної значущості окремих напрямів можуть застосовуватися вагові коефіцієнти, приклад розподілу наведено у таблиці 2.7.

Таблиця 2.7 – Розподіл ваг за доменами адаптованого інструмента

Домен		Ваги доменів
D ₁	Управління, стратегія та ризики	0,12
D ₂	Критичні функції, цифрові активи та дані	0,13
D ₃	Архітектура, сегментація, доступ і технічна гігієна	0,14
D ₄	Експлуатація, технічне обслуговування та управління змінами	0,1
D ₅	Треті сторони, підрядники та ланцюг постачання	0,1
D ₆	Фізична та кіберфізична безпека	0,11
D ₇	Виявлення, моніторинг і реагування	0,14
D ₈	Обізнаність, навчання та людський фактор	0,1
D ₉	Безперервність, резервування та відновлення	0,16

Це особливо важливо для енергетичної інфраструктури, де окремі домени, наприклад реагування та відновлення, безпека технологічних мереж, сегментація або управління зовнішніми залежностями, можуть мати більший вплив на загальну стійкість об'єкта, ніж інші складові [21, 23, 26]. У такому разі підсумкова оцінка формується не як просте середнє всіх показників, а як зважене узагальнення з урахуванням критичності доменів.

Методична доцільність такого підходу полягає в тому, що він поєднує переваги якісного й кількісного оцінювання. З одного боку, дані збираються у формі експертних відповідей, що дає змогу врахувати специфіку реального функціонування об'єкта [24, 25]. З іншого боку, ці відповіді переводяться в числову форму й обробляються за єдиним алгоритмом, що забезпечує відтворюваність,

порівнюваність і прозорість результатів. Таким чином, експертні оцінки не суперечать вимозі кількісної обробки результатів, а навпаки, виступають джерелом вихідних даних для подальшого обчислення показників кіберстійкості.

Окрему увагу слід приділити надійності експертних оцінок. Для зменшення суб'єктивності доцільно дотримуватися кількох методичних принципів: використовувати єдину шкалу оцінювання для всіх респондентів, формулювати запитання максимально однозначно, супроводжувати критерії короткими поясненнями або індикаторами належної практики, а також залучати до оцінювання представників різних ролей [23, 24]. За можливості результати окремих оцінок доцільно порівнювати між собою та аналізувати на предмет істотних розбіжностей. Такий підхід підвищує достовірність підсумкового профілю й робить оцінювання більш стійким до індивідуальних упереджень окремих учасників.

У межах практичної реалізації адаптованого підходу експертні оцінки доцільно розглядати як основне джерело даних для заповнення інструмента. Саме вони забезпечуватимуть первинну інформацію про стан окремих практик, критеріїв і процесів, після чого ця інформація буде узагальнюватися відповідно до обраного алгоритму. Таким чином, експертний компонент не є допоміжним елементом, а виступає центральною частиною практичної апробації інструмента профілювання кіберстійкості.

Отже, методичне використання експертних оцінок у цій роботі є виправданим з огляду на складність енергетичної інфраструктури, необхідність врахування організаційних і кіберфізичних аспектів, а також потребу в отриманні даних, які не можуть бути повністю описані лише формальними показниками. Поєднання експертного збору інформації з її подальшою формалізацією через адитивну модель і вагові коефіцієнти дозволяє побудувати інструмент, який одночасно зберігає практичну гнучкість, забезпечує відтворюваність оцінювання та створює основу для кількісної інтерпретації рівня кіберстійкості об'єкта.

Висновки до розділу 2

У другому розділі сформовано методологічні засади інформаційного забезпечення профілювання кіберстійкості об'єктів енергетичної інфраструктури України. На основі порівняльного аналізу обґрунтовано вибір моделі C2M2 як базового структурного каркаса розробки, що зумовлено її галузевою релевантністю, всебічним охопленням ІТ- та ОТ-середовищ, а також використанням рівнів зрілості (MIL) для оцінювання не лише наявності практик, а й ступеня їхньої керованості й сталості.

Визначено роль комплементарних елементів інших міжнародних фреймворків у межах проектованої гібридної архітектури. Логіку моделі CAF залучено для формування критеріїв оцінювання станів реалізації практик та побудови цільових профілів. Методологію CRR покладено в основу структурованого інтерв'ювального контуру та механізму багаторольової крос-верифікації відповідей персоналу. Для підвищення наочності й управлінського подання результатів адаптовано інструменти візуалізації шотландського методу (Scottish Framework). У результаті сформовано цілісну методичну схему, де кожен запозичений компонент виконує чітко визначену аналітичну функцію.

Систематизовано комплекс структурних, функціональних, галузевих, організаційних та аналітичних вимог до розробленого інформаційного забезпечення. Особливу увагу приділено специфіці енергетичного сектору, зокрема забезпеченню кіберфізичної стійкості – здатності об'єкта підтримувати безпечне виконання критичних процесів в ізольованому або ручному режимі керування в умовах воєнних загроз.

Обґрунтовано концептуальну архітектуру інформаційного забезпечення як багаторівневої системи, що трансформує первинні лінгвістичні експертні судження у підсумковий кількісний профіль кіберстійкості. Математичний апарат спирається на адитивну модель агрегування з використанням системи вагових коефіцієнтів, що дозволяє врахувати диференційовану значущість окремих доменів для

безперервності виробничого циклу підприємства та гарантує відтворюваність результатів.

Оскільки профілювання фіксує дискретний стан об'єкта в часі, розроблену модель визначено як інструмент періодичного контролю, який у подальшому має доповнюватися безперервним моніторингом, інструментальними перевірками та динамічним оновленням профілю відповідно до змін у ландшафті загроз.

Сформована методологічна база чітко регламентує параметри практичної реалізації програмного прототипу (застосування доменно-рольової структури, трирівневої шкали оцінювання « 1 / 0,5 / 0 » та алгоритмів зваженого узагальнення) і є безпосереднім підґрунтям для його подальшої експериментальної апробації на тестовому профілі об'єкта критичної інфраструктури.

3 РОЗРОБКА ТА ЗАСТОСУВАННЯ ПРАКТИЧНОГО АПАРАТУ

У цьому розділі методологічні положення, сформовані в попередніх розділах, реалізовано у вигляді інформаційного забезпечення для профілювання кіберстійкості енергетичного об'єкта. Практична частина дослідження охоплює формування доменно-рольового опитувальника, структури збереження даних, алгоритмів обробки відповідей, візуалізації результатів, аналізу чутливості та програмної реалізації прототипу ПКППР.

Розроблений інструмент поєднує доменну структуру C2M2, результативно-орієнтовану логіку CAF, інтерв'ювальний формат CRR та елементи наочного подання результатів, характерні для управлінських моделей самооцінювання. У практичній реалізації ці складові трансформовано в опитувальник, базу респондентів, механізм збереження відповідей, алгоритм розрахунку показників та експортований профіль оцінювання.

3.1 Постановка практичного завдання та логіка реалізації

Метою практичної частини є розробка та апробація автоматизованого інструмента профілювання кіберстійкості, який враховує специфіку енергетичного об'єкта, взаємодію ІТ- та ОТ-середовищ, роль персоналу, зовнішні залежності, критичні функції, а також потребу в кількісній інтерпретації результатів. На відміну від загального аудиту безпеки, запропонований інструмент орієнтований на оцінювання спроможності об'єкта підтримувати безперервність функціонування, виявляти інциденти, реагувати на них і відновлювати критичні процеси після порушення.

Практичне завдання передбачало виконання таких етапів: формування адаптованого опитувальника; визначення ролей респондентів; побудову структури збереження відповідей; реалізацію програмного застосунку; проведення тестового опитування; обчислення результатів за доменами, ролями та критеріями;

формування профілю кіберстійкості; визначення пріоритетних напрямів удосконалення.

Загальна логіка практичної реалізації має послідовний характер: методична основа перетворюється на банк питань, який використовується для збору відповідей від різних ролей; далі відповіді переводяться у числові значення, після чого система обчислює доменні, рольові та загальні показники. Такий підхід забезпечує простежуваність результату від конкретної відповіді респондента до підсумкового профілю кіберстійкості.

3.2 Структура інформаційного забезпечення та формування опитувальника

Опитувальник побудовано як доменно-рольову структуру. Домен визначає напрям оцінювання, критерій уточнює зміст перевірки, а роль респондента визначає категорію персоналу, компетентну для надання відповіді. Фрагмент конфігурації опитування наведено в додатку В.1. Застосовано диференційований підхід до формування опитувальних листів залежно від зони відповідальності респондентів. Це дозволяє уникнути ситуації, коли всі питання ставляться одній особі незалежно від її повноважень: стратегічні та ресурсні питання спрямовані на управлінський рівень, питання базової технічної безпеки – на ІТ-персонал, питання технологічного керування – на ОТ- та експлуатаційних фахівців, а питання фізичного доступу – на службу фізичної безпеки.

Принцип побудови інтерфейсу користувача в частині рольової сегрегації запитань представлено на рисунках 3.1 та 3.2. Механізм рольової фільтрації забезпечує цільове відображення елементів оцінювання відповідно до попередньо визначеної матриці компетенцій конкретного стейкхолдера. Специфікація форми унеможливорює виведення надлишкових для обраної посади запитань, що оптимізує процес експертного опитування. Практичне виконання цієї логіки продемонстровано у додатку В.2 та на прикладі взаємовиключних профілів: фахівець з інформаційних технологій (ІТ) не залучається до оцінювання

специфічних параметрів фізичного контуру (запитання №4, №8), які делегуються експлуатаційним службам та фахівцям з фізичної безпеки.

Профіль Респонденти **Опитування** Відповіді Розрахунки Візуалізація Експорт

Опитування

Респондент

№12 — IT-персонал 4 — IT-персонал

☐ Показати питання для всіх ролей

Фільтр за доменом

Усі

Питань для заповнення: 34

- > Q9 | D2. Критичні функції, цифрові активи та дані | Існує актуальний реєстр цифрових активів
- > Q12 | D2. Критичні функції, цифрові активи та дані | Обмежено доступ працівників до спільних папок

Рисунок 3.1 – Відображення релевантних питань відповідно до ролі респондента №12

Опитування

Респондент

№29 — Фізична безпека 6 — Фізична безпека

☐ Показати питання для всіх ролей

Фільтр за доменом

Усі

Питань для заповнення: 21

- > Q4 | D1. Управління, стратегія та ризики | Визначено персональну відповідальність за кібербезпеку для
- > Q8 | D1. Управління, стратегія та ризики | Використовуються визнані стандарти або настанови для
- > Q19 | D3. Архітектура, сегментація, доступ і технічна гігієна | Дотримуються вимоги щодо структури паролів і
- > Q37 | D6. Фізична та кібер-фізична безпека | Спрацьовує система фізичного захисту
- > Q38 | D6. Фізична та кібер-фізична безпека | Дотримуються встановлений рівень допуску для працівників

Рисунок 3.2 – Відображення релевантних питань відповідно до ролі респондента №29

Під час формування питань використано логіку SMART як допоміжний принцип побудови практичного інструмента [28]. Під час апробації питання мають бути конкретними, вимірюваними, практично досяжними для відповіді, релевантними до критичних функцій об'єкта та придатними до подальшої інтерпретації. Завдяки цьому формулювання питання не обмежується загальним твердженням про “наявність безпеки”, а вимагає перевірюваної відповіді, яку

можна підтвердити документом, журналом, процедурою або експертним поясненням.

У практичній версії інструмента сформовано 9 доменів оцінювання та 64 питання. Розподіл питань за доменами наведено в таблиці 3.1, їх повний перелік наведено в додатку А.

Таблиця 3.1 – Розподіл питань за доменами адаптованого інструмента

Домен		Кількість питань
D ₁	Управління, стратегія та ризики	8
D ₂	Критичні функції, цифрові активи та дані	7
D ₃	Архітектура, сегментація, доступ і технічна гігієна	8
D ₄	Експлуатація, технічне обслуговування та управління змінами	7
D ₅	Треті сторони, підрядники та ланцюг постачання	6
D ₆	Фізична та кіберфізична безпека	7
D ₇	Виявлення, моніторинг і реагування	7
D ₈	Обізнаність, навчання та людський фактор	7
D ₉	Безперервність, резервування та відновлення	7

Ролі респондентів визначено так, щоб охопити управлінський, технічний, експлуатаційний, фізичний та зовнішній контури оцінювання. Такий розподіл відповідає інтерв'ювальній логіці CRR, оскільки реальний стан практики може бути коректно оцінений лише за участі тих осіб, які відповідають за її виконання або безпосередньо з нею працюють.

3.3 Програмна реалізація інструмента профілювання

Для практичної реалізації інструмента розроблено прототип програмного комплексу підтримки прийняття рішень мовою Python. Як середовище побудови інтерфейсу використано Streamlit [29]. Такий вибір обґрунтовано потребою швидкого створення локального інтерактивного прототипу. Для локального збереження даних – SQLite [30], для табличної обробки та експорту результатів використано pandas [31], а для формування експортованого звіту – засоби запису даних у формат Excel. Практична реалізація можливості формування звіту наведена у додатку В.3. Такий стек обрано через його придатність до швидкої реалізації прототипу, можливість локального запуску без розгортання складної серверної інфраструктури та зручність подальшої обробки результатів.

Повний архітектурний перелік компонентів системи, опис призначення ключових модулів, а також інтерактивне посилання на віддалений репозиторій із сирцевим кодом розробленого програмного комплексу наведено у додатку Б.

Розроблений ПКППР складається з кількох функціональних вкладок: профіль оцінювання, респонденти, опитування, відповіді, розрахунки, візуалізація та експорт. Відповідні функціональні вкладки наведено на рисунку 3.3.

Профіль Респонденти Опитування Відповіді Розрахунки Візуалізація Експорт

Рисунок 3.3 – Функціональні вкладки програмного застосунку

У профілі задаються відомості про об'єкт і сесію оцінювання (див. рис. 3.4).

Назва об'єкта
Тестовий енергооб'єкт

Тип об'єкта
Підстанція / диспетчерський центр

Категорія критичності
I

Рисунок 3.4 – Вікно внесення даних про об'єкт оцінювання

У вкладці респондентів створюються записи учасників оцінювання із зазначенням ролі, це продемонстровано на рисунку 3.5. У вкладці опитування система відображає питання відповідно до ролі респондента (рисунки 3.1 та 3.2), а у вкладках розрахунків і візуалізації формуються підсумкові показники.

respondent_no	respondent_name	role_code	role	department
1	Вище керівництво 1	R1	Вище керівництво	Керівництво
2	Вище керівництво 2	R1	Вище керівництво	Керівництво
3	Вище керівництво 3	R1	Вище керівництво	Керівництво
4	Фахівець з кібербезпеки 1	R2	Фахівці з кібербезпеки	Служба кібербезпеки
5	Фахівець з кібербезпеки 2	R2	Фахівці з кібербезпеки	Служба кібербезпеки
6	Фахівець з кібербезпеки 3	R2	Фахівці з кібербезпеки	Служба кібербезпеки
7	Фахівець з кібербезпеки 4	R2	Фахівці з кібербезпеки	Служба кібербезпеки
8	Фахівець з кібербезпеки 5	R2	Фахівці з кібербезпеки	Служба кібербезпеки
9	ІТ-персонал 1	R3	ІТ-персонал	ІТ
10	ІТ-персонал 2	R3	ІТ-персонал	ІТ

Рисунок 3.5 – Сформований реєстр експертної групи в базі даних інформаційного забезпечення

Програма також передбачає роботу з базою даних, що складається з таблиць. Їхній вміст наведено в таблиці 3.2.

Таблиця 3.2 – Структура бази даних програмного застосунку

Таблиця	Призначення
1	2
assessments	Зберігає профіль сесії оцінювання: назву об'єкта, тип, категорію критичності, дату та опис.
respondents	Містить перелік респондентів із кодом, роллю, підрозділом і прив'язкою до сесії оцінювання.
questions	Містить банк питань із кодом питання, доменом, критерієм, цільовими ролями, текстом питання та джерелом логіки.
responses	Зберігає відповіді респондентів, числовий бал, коментар, джерело підтвердження та час заповнення.

Кінець таблиці 3.2

1	2
domain_weights	Містить вагові коефіцієнти доменів, що використовуються для підсумкового розрахунку.
quantitative_metrics	Містить додаткові кількісні показники для розширення підсумкового звіту.

Важливою вимогою до реалізації була простежуваність кожного запису. Для цього відповідь зберігається не ізольовано, а разом із кодом сесії оцінювання, кодом респондента та кодом питання. Така структура дозволяє простежити, хто саме надав відповідь, до якого домену вона належить, який бал було присвоєно та які пояснення або підтвердження були додані.

3.4 Алгоритм збору, обробки та інтерпретації даних

Збір даних відбувається за уніфікованою шкалою оцінювання. Для кожного питання респондент обирає один із трьох варіантів, наведених у таблиці 2.5. Додатково передбачено поля для коментаря та підтвердження, що дає змогу не обмежуватися лише числовою оцінкою. Це ілюструє рисунок 3.6.

Відповідь

☒ 1 — досягнуто / так / реалізовано

☐ 0.5 — частково досягнуто / частково реалізовано

☐ 0 — не досягнуто / ні / відсутнє

Коментар

Практика формалізована та фактично застосовується; під час тестового заповнення вважається реалізованою.

Джерело підтвердження / доказ

Внутрішні політики, журнали, регламенти, звіти перевірок для Q55

Зберегти відповідь

Рисунок 3.6 – Екранна форма експертного оцінювання практики із блоками текстового обґрунтування та аудиторських доказів

Після збереження відповідей програма виконує кілька рівнів обробки. Спочатку формується оцінка окремого питання або критерію. Значення p_i визначається як середнє арифметичне оцінок усіх респондентів, до компетенції яких входить відповідне питання:

$$p_i = \frac{1}{k} \sum_{r=1}^k s_{ir}, \quad (3.1)$$

де s_{ir} – оцінка, надана r -м респондентом за i -м питанням; k – кількість респондентів, які відповідали на це питання.

Далі обчислюється показник домену. У загальному вигляді він може бути поданий так:

$$D_j = \frac{\sum_{i=1}^n w_i \cdot p_i}{\sum_{i=1}^n w_i}, \quad (3.2)$$

де D_j – оцінка j -го домену; p_i – числове значення відповіді або оцінки практики; w_i – ваговий коефіцієнт практики в межах домену. У тестовій реалізації ваги окремих питань у межах домену встановлено однаковими, а відмінність значущості враховано на рівні доменів. Фрагмент реалізації обчислення доменних оцінок наведено в додатку В.4.

Загальний показник кіберстійкості розраховується як зважена сума доменних оцінок:

$$R = \frac{\sum_{j=1}^n w_j \cdot D_j}{\sum_{j=1}^n w_j}, \quad (3.3)$$

де R – загальний показник кіберстійкості; w_j – вага j -го домену; D_j – оцінка відповідного домену.

Вагові коефіцієнти доменів визначено експертно з урахуванням впливу кожного напрямку на безперервність критичних функцій енергетичного об'єкта. Найбільшу вагу надано домену D9 “Безперервність, резервування та відновлення”, оскільки саме він безпосередньо відображає здатність об'єкта підтримувати роботу

та повертатися до прийнятного стану після інциденту. Підвищені ваги також отримали D3 “Архітектура, сегментація, доступ і технічна гігієна” та D7 “Виявлення, моніторинг і реагування”, оскільки ці напрями впливають на обмеження поширення атаки, своєчасність її виявлення та швидкість реагування. Менші ваги не означають другорядності інших доменів, а лише відображають їх відносний вплив у межах тестового профілю. Перелік та визначення ваг доменів було наведено в таблиці 2.7. Сума вагових коефіцієнтів дорівнює 1, що забезпечує коректність зваженого агрегування доменних оцінок.

Використання кількісних показників у межах такого підходу відповідає загальній логіці метрик кібервідмовостійкості, де оцінювання має відображати не лише факт наявності контролів, а й здатність об’єкта підтримувати роботу критичних функцій за умов порушення та відновлюватися після інциденту [16].

Для інтерпретації інтегрального індексу кіберстійкості використано чотирирівневу шкалу. Її побудовано з урахуванням базової трибальної логіки оцінювання відповідей. Практична реалізація розрахунку наведена в додатку В.5. Проте значення інтегрального індексу не слід трактувати як абсолютний показник безпеки, а як узагальнену міру реалізації сукупності практик у межах доменів оцінювання.

Значення від 0 до 0,39 відповідає низькому рівню кіберстійкості, оскільки більшість практик не реалізована або має фрагментарний характер. Інтервал від 0,40 до 0,59 характеризує середній рівень, за якого частина практик уже впроваджена, однак залишаються суттєві прогалини. Значення від 0,60 до 0,79 відповідає достатньому рівню, коли основні практики реалізовані, але окремі напрями потребують посилення. Інтервал від 0,80 до 1,00 інтерпретується як високий рівень кіберстійкості, за якого більшість практик досягнута, однак локальні критичні прогалини все ще можуть створювати ризики для окремих функцій об’єкта. Фрагмент коду, що відповідає за формування короткого підсумку наведено в додатку В.6.

Така градація дає змогу уникнути спрощеної інтерпретації результату. Наприклад, високий інтегральний індекс не означає повної відсутності ризиків, оскільки окремі питання або домени можуть мати нульові чи часткові оцінки. Саме тому подальший аналіз має враховувати не лише загальний індекс, а й доменні оцінки, рольові розбіжності, часткові реалізації та питання з нульовими значеннями.

3.5 Проведення апробації інструмента профілювання

Апробацію проведено на профілі енергетичного об'єкта “Тестовий енергооб'єкт”. Тип об'єкта у профілі визначено як “Підстанція / диспетчерський центр”, категорію критичності – “Г”. Отримані результати мають апробаційний характер і використовуються для перевірки працездатності інструмента, логіки збереження даних, коректності розрахунків і придатності підсумкових звітів для подальшого аналізу.

У межах апробації було залучено 32 респонденти. Банк питань містив 64 питання, розподілені між 9 доменами. Загальна кількість збережених відповідей становила 1082. Кількість відповідей є меншою за добуток загальної кількості респондентів і питань, оскільки опитувальник має рольову структуру. Кожен респондент отримував не весь банк питань, а лише ті питання, що відповідали його зоні відповідальності. Завдяки цьому оцінювання не дублювало некомпетентні відповіді й краще відображало реальний розподіл функцій між учасниками. Розподіл відповідей за шкалою наведено в таблиці 3.3.

Таблиця 3.3 – Розподіл відповідей за шкалою оцінювання

Бал	Стан	Кількість відповідей	Частка
1,0	Досягнуто	777	71,8%
0,5	Частково досягнуто	277	25,6%
0,0	Не досягнуто	28	2,6%

3.6 Результати профілювання за доменами, ролями та критеріями

За результатами апробації загальна зважена оцінка кіберстійкості становила 0,863. Відповідно до прийнятої шкали це відповідає високому рівню. Проте така оцінка не означає повної відсутності проблем: доменний, рольовий і критеріальний аналіз показує наявність окремих напрямів, які потребують першочергової уваги.

Графічне подання доменних оцінок наведено на рисунку 3.7. Це дає змогу швидко визначити напрями, які мають найнижчі значення і потребують першочергової уваги.

Також у таблиці 3.4 наведено результати оцінювання саме за ролями респондентів. Окремо виділено кількість часткових відповідей, що демонструє певні прогалини у дотриманні вимог або реалізації відповідних практик захисту об'єкту.

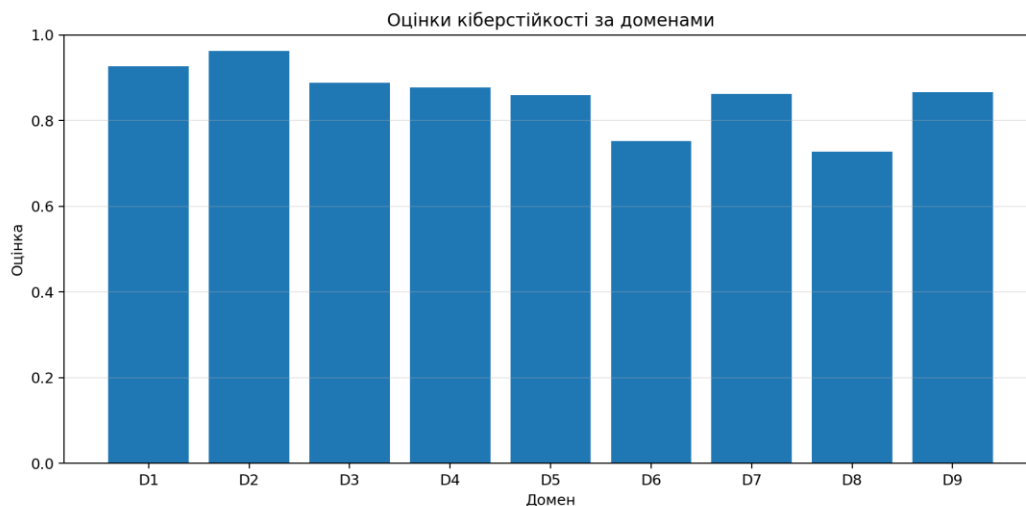


Рисунок 3.7 – Оцінки кіберстійкості за доменами

Для комплексного огляду результатів також побудовано радарний профіль кіберстійкості (рисунок 3.8). Така форма подання є зручною для управлінської інтерпретації, оскільки показує не лише загальний бал, а й нерівномірність розвитку окремих напрямів. Порівняння оцінок за ролями респондентів наведено на рисунку 3.9.

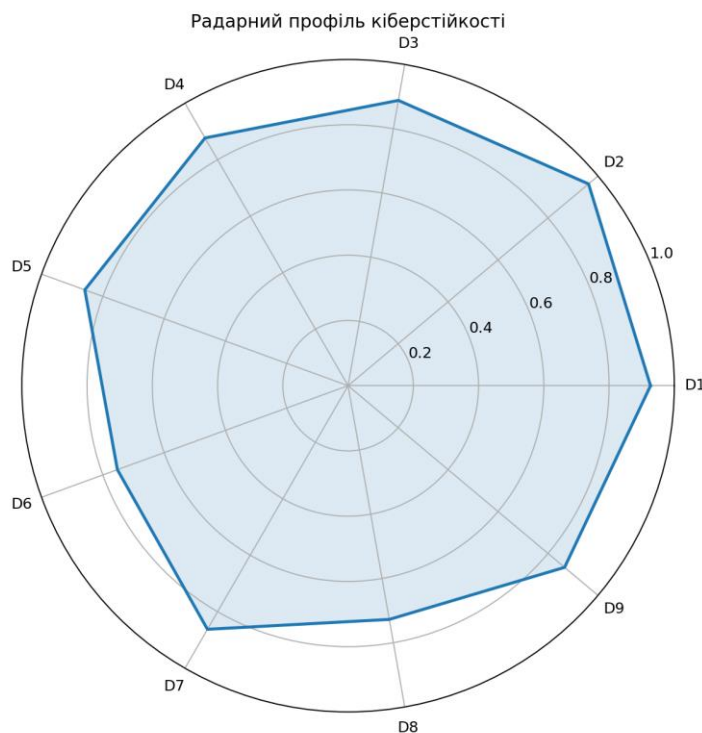


Рисунок 3.8 – Радарний профіль кіберстійкості апробаційного об’єкта

Таблиця 3.4 – Результати оцінювання за ролями респондентів

Код	Роль	Середня оцінка	К-сть відповідей	0	0,5	Рівень
R1	Вище керівництво	0,781	96	6	30	Достатній рівень
R2	Фахівці з кібербезпеки	0,869	295	5	67	Високий рівень
R3	ІТ-персонал	0,841	170	5	44	Високий рівень
R4	ОТ / експлуатація та обслуговування	0,874	350	0	88	Високий рівень
R5	Фізична безпека	0,778	126	12	32	Достатній рівень
R6	Підрядники / постачальники	0,822	45	0	16	Високий рівень

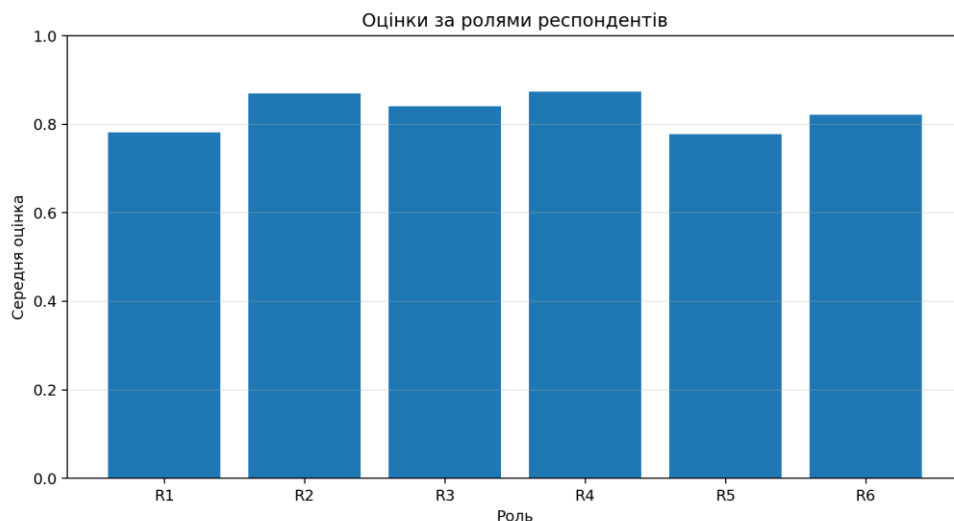


Рисунок 3.9 – Порівняння оцінок за ролями респондентів

Аналіз за ролями показує, що найнижчі середні значення отримали групи фізичної безпеки та вищого керівництва. Це не свідчить безпосередньо про низьку якість роботи цих груп, однак вказує на те, що відповідні напрями містять більше часткових або нереалізованих практик, які мають бути деталізовані під час подальшого аналізу.

Таблиця 3.5 – Найслабші практики за результатами апробації

Код	Домен	Питання	Середня оцінка	К-сть відповідей	0	0,5
1	2	3	4	5	6	7
Q41	D6	Чи застосовуються додаткові механізми перевірки особи, наприклад біометрія або двофакторний фізичний доступ, для критичних зон?	0,000	9	9	0

Продовження таблиці 3.5

1	2	3	4	5	6	7
Q57	D8	Чи відстежуються ризики внутрішнього порушника, зокрема несанкціоноване використання ресурсів, майнінг або передавання службових файлів стороннім особам?	0,000	19	19	0
Q5	D1	Чи виділено достатній бюджет і ресурси для підтримки програми кібербезпеки відповідно до оцінених ризиків?	0,625	8	0	6
Q7	D1	Чи включені вимірювані показники кібербезпеки до KPI організації або управлінської звітності?	0,625	8	0	6
Q27	D4	Чи є процес повідомлення про вразливості, їх відстеження та контроль усунення?	0,625	20	0	15
Q43	D6	Чи проводяться спільні навчання з реагування на комбіновані кіберфізичні атаки та активні дії внутрішнього порушника?	0,625	24	0	18
Q46	D7	Чи брали ключові ролі участь у навчаннях з реагування на кіберінцидент протягом останніх 12 місяців?	0,625	24	0	18

Кінець таблиці 3.5

1	2	3	4	5	6	7
Q52	D8	Чи перевіряється здатність працівників ідентифікувати, зупинити й повідомити про соціальну інженерію або фішинг?	0,625	32	0	24
Q53	D8	Чи дотримуються працівники процедур повідомлення після виявлення імітованої або реальної фішингової атаки?	0,625	32	0	24
Q56	D8	Чи повідомляють працівники про потенційні питання кібербезпеки та звертаються по рекомендації у сумнівних ситуаціях?	0,625	32	0	24

Таблиця 3.5 показує, що головний аналітичний результат інструмента полягає не в самому інтегральному індексі, а у виявленні конкретних практик, які знижують стійкість профілю. Нульові значення за Q41 і Q57 є більш значущими для планування покращень, ніж загальна висока оцінка, оскільки саме вони вказують на локальні критичні прогалини.

3.7 Перевірка чутливості результатів оцінювання

Зважаючи на пряму залежність інтегрального індексу кіберстійкості від конфігурації вагових коефіцієнтів та суб'єктивізму експертних суджень, у роботі реалізовано процедуру валідації розрахункових параметрів. У межах дослідження чутливість аналізується як амплітуда варіативності підсумкового показника за

умов контрольованої зміни вхідних даних. Цей етап дозволяє верифікувати математичну стійкість проектного інформаційного забезпечення та довести, що помірні коливання експертних оцінок чи ваг не призведуть до викривлення фінального якісного рівня кіберстійкості підприємства.

Перевірку надійності розрахунків виконано за двома аналітичними векторами. Перший вектор передбачає оцінювання стійкості системи до зсуву пріоритетів безпеки. Для цього вагові коефіцієнти доменів, що мають визначальний вплив на безперервність критичних процесів енергооб'єкта, послідовно змінювалися на $\pm 10\%$ із наступною ренормалізацією їхньої суми до одиниці та повторним розрахунком цільового індексу.

Другий вектор спрямований на компенсацію можливих похибок та суб'єктивності експертів у випадках, коли вони дають неоднозначні відповіді. З цією метою базове значення часткової оцінки (0,5) протестовано у двох сценаріях: песимістичному (де рівень реалізації практики знижувався до 0,4) та оптимістичному (із підвищенням показника до 0,6). Реалізація аналізу чутливості наведена в додатках В.7 та В.8.

Збереження інтегрального індексу в межах початкового інтервалу інтерпретації свідчить про високу інваріантність математичного апарату до експертного шуму. Результати сценарного моделювання чутливості для тестового профілю об'єкта енергетичної інфраструктури систематизовано в таблиці 3.6.

Обчислені дані підтверджують високу надійність впровадженої інтервальної градації. В усіх аналізованих випадках підсумковий показник зберіг позицію в межах високого рівня кіберстійкості (діапазон коливань від 0,849 до 0,877 за базового значення 0,863). Це доводить стійкість інформаційного забезпечення до невизначеності експертних суджень. Водночас системна стабільність індексу не скасовує критичності локальних прогалів, виявлених у доменах D6 та D8, які потребують першочергової технічної й організаційної корекції.

Таблиця 3.6 – Результати перевірки чутливості інтегрального показника

Сценарій	Умова перерахунку	Інтегральний індекс	Рівень
Базовий	Початкові ваги та оцінки	0,863	Високий
Зміна ваг -10%	Зменшення ваг критичних доменів із нормалізацією	0,865	Високий
Зміна ваг +10%	Збільшення ваг критичних доменів із нормалізацією	0,861	Високий
Песимістичний	Часткові оцінки в критичних доменах зменшено з 0,5 до 0,4	0,849	Високий
Оптимістичний	Часткові оцінки в критичних доменах збільшено з 0,5 до 0,6	0,877	Високий

Задля поглибленої імовірнісної валідації математичної моделі додатково застосовано стохастичне моделювання за методом Монте-Карло. На відміну від детермінованого сценарного підходу, цей інструмент дозволяє згенерувати щільну множину випадкових комбінацій вхідних змінних, забезпечуючи комплексне оцінювання закону розподілу ймовірностей підсумкового показника.

Під час проведення ітерацій випадкове обурення параметрів охоплювало як вагові коефіцієнти (інтервал коливань $\pm 10\%$ із процедурою нормалізації), так і значення часткових відповідей респондентів (рівномірний розподіл у діапазоні $[0,4; 0,6]$). Повні (1) та нульові (0) оцінки станів практик розглядалися як фіксовані константи, оскільки вони відображають повністю верифіковані стани. Фрагмент моделювання невизначеності методом Монте-Карло наведено в додатку В.9. Ітераційний перерахунок інтегрального індексу методом Монте-Карло та його реалізація наведена в додатку В.10.

Розрахункові параметри за результатами 10 000 ітерацій моделювання зведено в таблиці 3.7.

Таблиця 3.7 – Результати перевірки чутливості методом Монте-Карло

Показник	Значення
Базовий індекс	0,863
Кількість ітерацій	10 000
Середнє значення	0,863
Медіана	0,863
Стандартне відхилення	0,0015
5-й перцентиль	0,86
95-й перцентиль	0,865
Ймовірність високого рівня	99,0%

Статистичні метрики стохастичного аналізу свідчать про екстремальну концентрацію змодельованих значень навколо математичного очікування (середнє значення та медіана повністю збігаються з базовим індексом і становлять 0,863). Мінімальне стандартне відхилення (0,0015), а також вузький перцентильний коридор (0,860–0,865) підтверджують, що з ймовірністю 99% підсумковий рівень кіберстійкості об'єкта залишається інваріантним до випадкових коливань параметрів.

Для унаочнення отриманих результатів імовірнісного моделювання побудовано гістограму щільності підсумкового показника, представлену на рисунку 3.10.

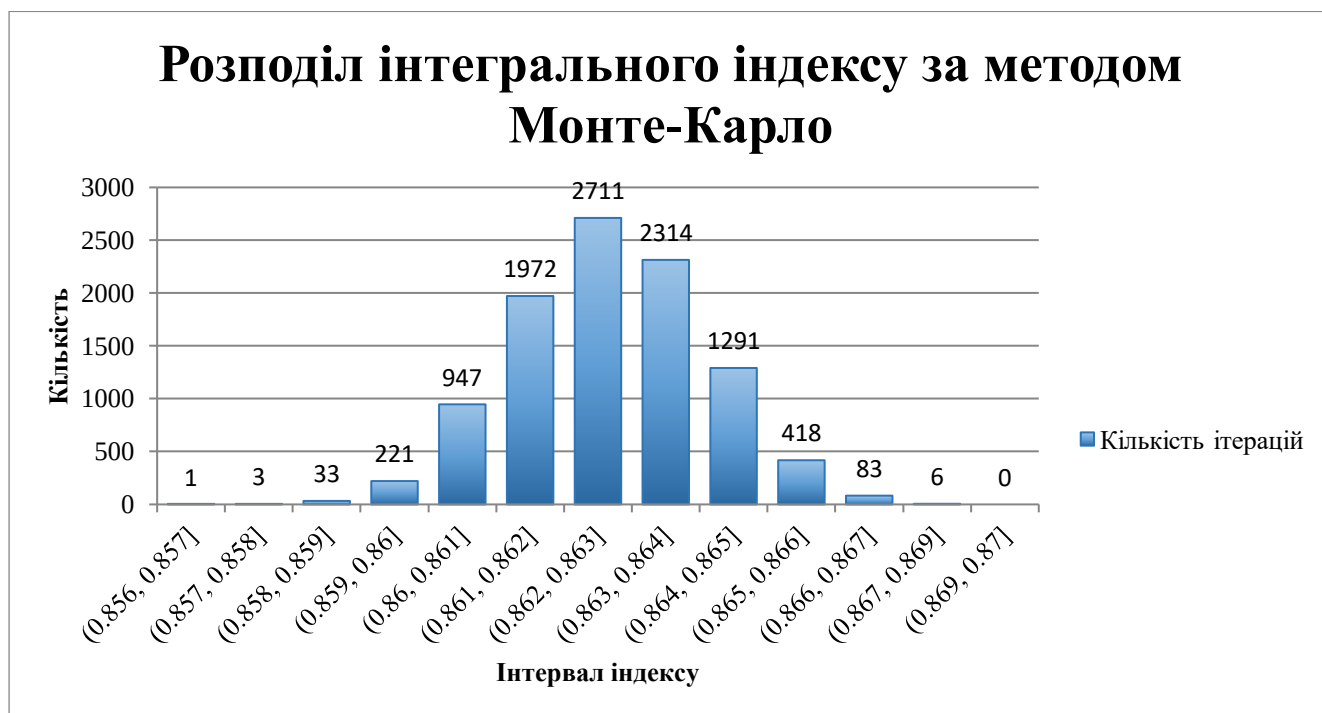


Рисунок 3.10 – Розподіл інтегрального індексу кіберстійкості за методом Монте-Карло

Графічний розподіл доводить, що основна маса змодельованих значень зосереджена у безпосередній близькості до базової оцінки. Отримані дані підтверджують коректність математичної логіки розробленого інформаційного забезпечення. Проте, аналогічно до попередніх висновків, висока агрегована стабільність індексу не свідчить про повну відсутність безпекових ризиків. Нульові та часткові оцінки за конкретними індикаторами (зокрема, критичні прогалини у точках Q41 та Q57) вимагають цільового операційного реагування незалежно від загального стабільно високого інтегрального фону системи.

3.8 Інтерпретація профілю кіберстійкості та напрями вдосконалення

Отриманий загальний результат свідчить про високий рівень сформованості більшості практик у межах апробаційного профілю. Найсильнішими напрямами виявилися домени, пов'язані з управлінням, критичними активами та базовою технічною гігієною. Це означає, що в межах тестових даних добре представлені

практики інвентаризації активів, зв'язку активів із критичними функціями, управління ризиками та базового технічного контролю.

Водночас найнижчі доменні значення отримали напрями D8 “Обізнаність, навчання та людський фактор” і D6 “Фізична та кіберфізична безпека”. За прийнятою шкалою вони формально відповідають достатньому рівню, однак саме ці домени є критичними зонами уваги через наявність нульових оцінок за окремими питаннями. Це є методично важливим результатом, оскільки саме ці напрями часто складно оцінити лише технічними засобами. Їх виявлення підтверджує доцільність використання експертно-опитувального механізму, а не лише автоматизованих технічних перевірок.

Нульові оцінки за питаннями Q41 і Q57 свідчать про наявність критичних прогалин у тестовому профілі. Перша стосується додаткових механізмів перевірки особи для критичних зон, друга – контролю ризиків внутрішнього порушника. Обидві практики мають безпосередній зв'язок із кіберфізичною безпекою, людським фактором та можливістю несанкціонованого впливу на критичні процеси. У межах інтерпретації такі прогалини доцільно розглядати як потенційні єдині точки відмови, оскільки навіть за високого інтегрального показника вони можуть нівелювати загальний рівень стійкості в разі реалізації відповідного сценарію загрози.

Часткові оцінки за питаннями щодо фішингових перевірок, повідомлення про підозрілі події, участі ключових ролей у навчаннях, управління підрядниками та практичного відновлення з резервних копій вказують на напрями, де практика вже існує, але не має достатньої регулярності, повноти або підтвердження з боку всіх відповідальних ролей. Запропоновані напрями вдосконалення мають розглядатися не як статичний перелік заходів, а як основа для адаптивного реагування на порушення кіберстійкості. Це означає, що об'єкт повинен мати можливість змінювати пріоритети дій залежно від типу інциденту, уражених функцій, доступності ресурсів і рівня впливу на критичні процеси [17].

Таблиця 3.8 – Пріоритетні напрями вдосконалення за результатами апробації

Пріоритет	Напрям	Рекомендована дія
1	Контроль внутрішнього порушника	Визначити ознаки потенційно небезпечної поведінки, запровадити моніторинг несанкціонованого використання ресурсів і передавання службових файлів.
2	Фізичний доступ до критичних зон	Посилити механізми перевірки особи для критичних зон, розглянути додаткову автентифікацію або двоетапний контроль доступу.
3	Навчання та фішинг-перевірки	Проводити регулярні фішинг-тести, навчання за ролями та контроль дотримання процедури повідомлення.
4	Підрядники та ланцюг постачання	Уточнити вимоги до стороннього доступу, перевірки постачальників і повторного оцінювання виявлених проблем.
5	Відновлення та резервування	Регулярно перевіряти практичне відновлення з резервних копій, ізоляцію копій і готовність до ручного або резервного режиму.

Отже, розроблений інструмент дозволяє не лише отримати інтегральний бал, а й пояснити, які саме практики знижують підсумковий профіль. Це є основною перевагою запропонованої реалізації: результат не обмежується одним числом, а перетворюється на основу для планування покращень, пріоритезації заходів захисту та виявлення прихованих організаційних розривів між різними групами респондентів.

3.9 Обмеження апробації та можливості подальшого розвитку

Проведена апробація має тестовий характер, тому її результати не слід трактувати як остаточну оцінку реального енергетичного об'єкта. Частина відповідей була сформована для перевірки роботи інструмента, а не в межах повноцінного незалежного аудиту. Відповідно, аналітичне значення мають передусім структура інструмента, логіка розрахунку, можливість виявлення прогалин, крос-верифікація відповідей і зручність формування підсумкового профілю.

Окремим обмеженням є залежність результатів від прийнятої шкали інтерпретації відповідей і вагової моделі. Хоча виконана перевірка чутливості дає змогу оцінити стійкість інтегрального індексу до помірних змін параметрів, вона не усуває потреби в подальшому уточненні ваг для конкретних типів енергетичних об'єктів.

У подальшому вагові коефіцієнти доцільно уточнювати шляхом експертного ранжування залежно від конкретних критичних функцій об'єкта. Крім того, доцільним є розширення блоку кількісних метрик, автоматичне виявлення суперечностей між відповідями різних ролей, формування рекомендацій на основі типу прогалини та додавання окремого модуля для порівняння результатів кількох сесій оцінювання в динаміці.

Перспективним напрямом розвитку є також інтеграція інструмента з реальними джерелами даних: системами управління вразливостями, журналами моніторингу, SIEM, системами управління змінами та платформами навчання персоналу. Це дозволило б поєднати експертну оцінку з фактичними операційними показниками та підвищити достовірність профілю кіберстійкості.

Висновки до розділу 3

У третьому розділі розроблено та апробовано прототип програмного комплексу підтримки прийняття рішень для профілювання кіберстійкості об'єкта енергетичної інфраструктури. ПКППР реалізовано мовою Python із використанням Streamlit для інтерфейсу, SQLite для збереження результатів, pandas для табличної обробки даних та механізму експорту результатів у формат Excel.

На основі методологічних положень попереднього розділу сформовано доменно-рольову структуру опитувальника: 64 адаптовані питання розподілено за 9 доменами оцінювання та 6 групами респондентів. Такий підхід забезпечив диференційований збір даних залежно від зон відповідальності зацікавлених сторін і створив основу для крос-верифікації відповідей між управлінським, технічним, експлуатаційним, фізичним та зовнішнім контурами оцінювання.

У межах тестової апробації було залучено 32 респонденти, отримано 1082 відповіді, з яких 777 відповідей (71,8%) відповідали стану “досягнуто”, 277 відповідей (25,6%) – стану “частково досягнуто”, а 28 відповідей (2,6%) – стану “не досягнуто”. Для інтерпретації інтегрального індексу використано чотирирівневу шкалу: низький, середній, достатній і високий рівні кіберстійкості. Розрахований індекс становив 0,863, що відповідає високому рівню за прийнятою шкалою, однак деталізований аналіз виявив критичні зауваження щодо доменів D6 “Фізична та кіберфізична безпека” (0,752) та D8 “Обізнаність, навчання та людський фактор” (0,727).

Додатково уточнено шкалу інтерпретації оцінок і виконано перевірку чутливості отриманих результатів. Аналіз чутливості виконано у два етапи: спочатку через сценарний перерахунок зі зміною ваг критичних доменів і числової інтерпретації часткових відповідей, а потім за допомогою методу Монте-Карло. Такий підхід дозволив оцінити стійкість інтегрального індексу не лише за окремими контрольними сценаріями, а й за великої кількості випадкових комбінацій вхідних параметрів.

За результатами методу Монте-Карло при 10 000 ітерацій середнє значення інтегрального індексу становило 0,863, медіана – 0,863, стандартне відхилення – 0,0015, а 5-й і 95-й перцентилі перебували в межах 0,860–0,865. Ймовірність збереження високого рівня становила 99%, що підтверджує стійкість отриманого результату до помірної невизначеності часткових експертних оцінок і вагових коефіцієнтів.

Апробація підтвердила працездатність запропонованого інструмента не лише для розрахунку інтегрального показника, а й для виявлення прихованих організаційних розривів. Зокрема, за окремими питаннями було виявлено розбіжності між управлінським і технічним персоналом щодо готовності до ручного або резервного керування, що підтверджує практичну значущість механізму крос-верифікації. Виявлені нульові оцінки за Q41 і Q57 дали змогу визначити потенційні єдині точки відмови, пов'язані з фізичним доступом до критичних зон та ризиком внутрішнього порушника. Отже, інструмент дозволяє пріоритезувати заходи з модернізації захисту, зокрема посилення контролю внутрішніх порушників, удосконалення фізичного доступу, проведення рольових навчань і регулярну перевірку процедур відновлення.

ВИСНОВКИ

У дипломній роботі розроблено інформаційне забезпечення для профілювання кіберстійкості енергетичного об'єкта, реалізовано його програмний прототип та апробовано на тестовому профілі енергооб'єкта. Запропоноване інформаційне забезпечення поєднує доменну структуру C2M2, логіку оцінювання станів CAF, інтерв'ювальний і рольовий механізм CRR, окремі елементи управлінського подання результатів шотландського підходу, адитивну модель агрегування оцінок та перевірку чутливості отриманих результатів.

У результаті аналізу сучасних кібератак на критичну та енергетичну інфраструктуру встановлено, що актуальні загрози мають комплексний кіберфізичний характер і можуть впливати як на ОТ-середовище, так і на корпоративну IT-інфраструктуру. Розглянуті інциденти Industroyer2, атаки Sandworm, FrostyGoop, PathWiper, Colonial Pipeline та інцидент із дамбою в Норвегії показали, що критичними слабкими місцями залишаються не лише спеціалізовані зразки шкідливого програмного забезпечення, а й базові організаційно-технічні прогалини: недостатня сегментація IT/ОТ-середовищ, слабкий контроль доступу, неналежний контроль підрядників, недостатня готовність до реагування та відновлення. Це обґрунтувало потребу в інструменті, який оцінює не лише наявність засобів захисту, а й здатність енергетичного об'єкта підтримувати критичні функції під час інциденту.

У результаті дослідження фреймворків оцінювання кіберстійкості визначено елементи, придатні для побудови інформаційного забезпечення профілювання. Порівняльний аналіз C2M2, CAF, CRR та Scottish Framework показав, що жоден із цих підходів окремо не покриває всі потреби роботи. C2M2 обґрунтовано як базовий структурний каркас завдяки його енергетичній спрямованості, охопленню IT/ОТ-середовищ і розвиненій доменній структурі. CAF використано для логіки оцінювання станів “досягнуто / частково досягнуто / не досягнуто” та критеріїв належної практики, CRR – для інтерв'ювального збору даних і крос-верифікації

відповідей, а *Scottish method* – для наочного подання результатів на управлінському рівні. У результаті сформовано функціонально розподілену методичну схему.

Сформовано структуру інформаційного забезпечення профілювання кіберстійкості енергетичного об'єкта. Вона включає 9 доменів оцінювання, рольову модель респондентів, перелік питань, трирівневу шкалу відповідей, механізм переведення якісних експертних суджень у числові значення та адитивну модель агрегування результатів. У межах структури враховано 6 груп респондентів: вище керівництво, фахівців з кібербезпеки, ІТ-персонал, ОТ/експлуатацію та обслуговування, фізичну безпеку, підрядників і постачальників. Такий розподіл забезпечує диференційований збір даних за зонами відповідальності та дозволяє виявляти не лише технічні, а й організаційні прогалини.

У третьому розділі розроблено прототип програмного комплексу підтримки прийняття рішень для профілювання кіберстійкості. Прототип реалізовано мовою Python із використанням Streamlit для побудови інтерфейсу, SQLite для локального збереження результатів, pandas для табличної обробки даних та механізму експорту результатів у формат Excel. Розроблений ПКППР підтримує створення сесії оцінювання, внесення профілю об'єкта, реєстрацію респондентів, рольову фільтрацію питань, збереження відповідей, розрахунок показників за доменами, ролями та критеріями, побудову графіків, формування профілю кіберстійкості та експорт результатів для подальшого аналізу.

Проведено апробацію розробленого інформаційного забезпечення на тестовому профілі енергетичного об'єкта та отримано кількісні результати профілювання. У межах апробації використано 64 адаптовані питання, розподілені за 9 доменами та 6 групами респондентів. Було залучено 32 респонденти й отримано 1082 відповіді, з яких 777 відповідей, тобто 71,8%, відповідали стану “досягнуто”, 277 відповідей, або 25,6%, – стану “частково досягнуто”, а 28 відповідей, або 2,6%, – стану “не досягнуто”. Інтегральний індекс кіберстійкості

становив 0,863, що відповідає високому рівню за прийнятою шкалою. Водночас деталізований аналіз показав, що високий загальний індекс не усуває локальних критичних прогалин: найнижчі значення отримали домени D6 “Фізична та кіберфізична безпека” – 0,752 та D8 “Обізнаність, навчання та людський фактор” – 0,727. Нульові оцінки за питаннями Q41 і Q57 вказали на потенційні єдині точки відмови, пов’язані з додатковою перевіркою особи для критичних зон і контролем ризиків внутрішнього порушника. Також виконано перевірку чутливості отриманих результатів, що підтвердила стійкість підсумкового індексу до помірної невизначеності вхідних параметрів. Сценарний аналіз показав, що за зміни ваг критичних доменів на $\pm 10\%$ та зміни інтерпретації часткових відповідей інтегральний індекс залишався в межах високого рівня: від 0,849 до 0,877 за базового значення 0,863. Додаткове моделювання методом Монте-Карло на 10 000 ітерацій показало середнє значення 0,863, медіану 0,863, стандартне відхилення 0,0015, а 5-й і 95-й перцентилі перебували в межах 0,860–0,865. Ймовірність збереження високого рівня становила 99,0%, що підтверджує відносну стійкість результату до зміни часткових експертних оцінок і вагових коефіцієнтів.

Отже, поставлені задачі в межах даної роботи виконано. Зокрема, розроблено інформаційне забезпечення для профілювання кіберстійкості енергетичного об’єкта, сформовано його методологічну основу, реалізовано програмний прототип, проведено тестову апробацію, отримано кількісний профіль кіберстійкості та визначено пріоритетні напрями вдосконалення. Практична цінність результатів полягає в тому, що запропонований інструмент дозволяє не лише розрахувати інтегральний індекс, а й виявити слабкі місця за доменами, ролями та окремими практиками. Це створює основу для пріоритезації заходів безпеки, зокрема посилення контролю внутрішніх порушників, удосконалення фізичного доступу до критичних зон, проведення рольових навчань, регулярних фішингових перевірок, перевірки процедур відновлення та підвищення якості взаємодії між управлінським, технічним і експлуатаційним рівнями.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Reuters. Ukraine says it thwarted Russian cyberattack on electricity grid [Електронний ресурс]. – 12.04.2022. – URL: <https://www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12/>
2. ESET Research. Industroyer2: Industroyer reloaded [Електронний ресурс]. – 12.04.2022. – URL: <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>
3. Mandiant. INDUSTROYER.V2: Old Malware Learns New Tricks [Електронний ресурс]. – 25.04.2022. – URL: <https://cloud.google.com/blog/topics/threat-intelligence/industroyer-v2-old-malware-new-tricks>
4. Mandiant. Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology [Електронний ресурс]. – 09.11.2023. – URL: <https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/>
5. MITRE ATT&CK. 2022 Ukraine Electric Power Attack, Campaign C0034 [Електронний ресурс]. – 10.04.2024. – URL: <https://attack.mitre.org/campaigns/C0034/>
6. Industrial Cyber. Ukrainian CERT details malicious plan by Sandworm group to disrupt critical infrastructure facilities [Електронний ресурс]. – 23.04.2024. – URL: <https://industrialcyber.co/critical-infrastructure/ukrainian-cert-details-malicious-plan-by-sandworm-group-to-disrupt-critical-infrastructure-facilities/>
7. BleepingComputer. Russian Sandworm hackers targeted 20 critical orgs in Ukraine [Електронний ресурс]. – 22.04.2024. – URL: <https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-targeted-20-critical-orgs-in-ukraine/>

8. Mandiant. APT44: Unearthing Sandworm [Электронный ресурс]. – 2024. – URL: <https://nsarchive.gwu.edu/sites/default/files/documents/semon9-ryglx/2024-04-17-Mandiant-APT44-Unearthing-Sandworm.pdf>
9. BleepingComputer. FrostyGoop malware attack cut off heat in Ukraine during winter [Электронный ресурс]. – 23.07.2024. – URL: <https://www.bleepingcomputer.com/news/security/frostygoop-malware-attack-cut-off-heat-in-ukraine-during-winter/>
10. CyberScoop. Simple ‘FrostyGoop’ malware responsible for turning off Ukrainians’ heat in January attack [Электронный ресурс]. – 23.07.2024. – URL: <https://cyberscoop.com/frostygoop-ics-malware-dragos-ukraine/>
11. Cisco Talos. Newly identified wiper malware “PathWiper” targets critical infrastructure in Ukraine [Электронный ресурс]. – 05.06.2025. – URL: <https://blog.talosintelligence.com/pathwiper-targets-ukraine/>
12. Reuters. U.S. seizes \$2.3 mln in bitcoin paid to Colonial Pipeline hackers [Электронный ресурс]. – 08.06.2021. – URL: <https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/>
13. U.S. Department of Justice. Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside [Электронный ресурс]. – 2021. – URL: <https://www.justice.gov/archives/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>
14. Reuters. Norway spy chief blames Russian hackers for dam sabotage in April [Электронный ресурс]. – 13.08.2025. – URL: <https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/>
15. Claroty. Cyberattack on Norwegian Dam Highlights Password Exposure Risks [Электронный ресурс]. – 26.06.2025. – URL:

<https://claroty.com/blog/cyberattack-on-norwegian-dam-highlights-password-exposure-risks>

16. Гальчинський, Л., & Личик, В. (2023). Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство, (2 (8), С. 27-33. URL: <https://doi.org/10.32689/maup.it.2023.2.3>

17. Личик, В. В. (2025). Адаптивний підхід до реагування на порушення кіберстійкості об'єктів критичної інфраструктури. Комп'ютерно-інтегровані технології: освіта, наука, виробництво, (59), С. 16-28. URL: <https://doi.org/10.36910/6775-2524-0560-2025-59-02>

18. CyberScotland. Cyber Resilience Framework [Електронний ресурс]. – URL: <https://www.cyberscotland.com/advice-and-guidance/cyber-resilience-framework/>

19. Scottish Government. Scottish public sector cyber resilience framework v2.0 [Електронний ресурс]. – 2024. – URL: <https://www.gov.scot/publications/scottish-public-sector-cyber-resilience-framework-v2-0/>

20. U.S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2) [Електронний ресурс]. – URL: <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>

21. U.S. Department of Energy. Cybersecurity Capability Maturity Model, Version 2.1 [Електронний ресурс]. – 2022. – URL: <https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf>

22. National Cyber Security Centre. Introduction to the Cyber Assessment Framework [Електронний ресурс]. – URL: <https://www.ncsc.gov.uk/collection/cyber-assessment-framework/introduction-to-caf>

23. National Cyber Security Centre. Cyber Assessment Framework 4.0 [Электронный ресурс]. – URL: <https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf>
24. CISA. CRR: Method Description and Self-Assessment User Guide [Электронный ресурс]. – URL: https://www.cisa.gov/sites/default/files/publications/2_CRR%25204.0_Self-Assessment_User_Guide_April_2020.pdf
25. CISA. Cyber Resilience Review (CRR) [Электронный ресурс]. – URL: <https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr>
26. NIST. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Special Publication 800-161 Rev. 1 Update 1 [Электронный ресурс]. – 2024. – URL: <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>
27. CISA. CRR: NIST Cybersecurity Framework Crosswalks [Электронный ресурс]. – URL: <https://www.cisa.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf>
28. Doran, G. T. There's a S.M.A.R.T. way to write management's goals and objectives. Management Review. 1981. Vol. 70, No. 11. P. 35–36.
29. Streamlit. Streamlit documentation [Электронный ресурс]. – URL: <https://docs.streamlit.io/>
30. SQLite. About SQLite [Электронный ресурс]. – URL: <https://www.sqlite.org/about.html>
31. pandas. pandas.DataFrame.to_excel [Электронный ресурс]. – URL: https://pandas.pydata.org/docs/reference/api/pandas.DataFrame.to_excel.html

ДОДАТОК А

ПЕРЕЛІК ІНДИКАТОРІВ ОЦІНЮВАННЯ

Таблиця А.1 – Структурована матриця запитань за тематичними доменами інструменту профілювання

Домен	Код	Питання	Ролі	Підтвердження
D1	Q1	Чи отримує вище керівництво регулярні оцінки поточного стану кіберзагроз і їхнього можливого впливу на критичні функції об'єкта?	R1; R2	Звіти про загрози, бюлетені, протоколи нарад.
	Q2	Чи має організація затверджену стратегію кіберзахисту, що узгоджена з цілями діяльності, ризиками та особливостями ОТ-середовища?	R1; R2; R4	Стратегія, політика, план розвитку програми.
	Q3	Чи включена кібербезпека до загальної системи управління ризиками організації?	R1; R2	Реєстр ризиків, методика оцінювання, рішення керівництва.
	Q4	Чи визначено персональну відповідальність за кібербезпеку для керівництва, ІТ, ОТ, фізичної безпеки та експлуатаційних служб?	R1; R2; R4; R5	RACI, посадові інструкції, накази.
	Q5	Чи виділено достатній бюджет і ресурси для підтримки програми кібербезпеки відповідно до оцінених ризиків?	R1; R2	Бюджет, штат, договори, закупівлі.

Продовження таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D1	Q6	Чи проводить вище керівництво щонайменше щорічний огляд програми кібербезпеки та результатів останньої оцінки?	R1; R2	Протоколи огляду, звіти оцінювання.
	Q7	Чи включені вимірювані показники кібербезпеки до KPI організації або управлінської звітності?	R1; R2	KPI, дашборди, звіти.
	Q8	Чи використовуються визнані стандарти або настанови для побудови програми кібербезпеки ІТ та ОТ?	R1; R2; R5	Посилання на стандарти, політики, внутрішні вимоги.
D2	Q9	Чи існує актуальний реєстр цифрових активів, мереж, цифрових компонентів і систем, що підтримують критичні функції?	R2; R3; R4	CMDB, інвентаризація, мережеві схеми.
	Q10	Чи визначено перелік чутливих цифрових активів, компрометація яких може вплинути на безпеку або безперервність технологічного процесу?	R2; R4	Класифікація активів, перелік критичних компонентів.
	Q11	Чи пов'язано критичні активи з конкретними критичними функціями об'єкта?	R1; R2; R4	Мапа актив-функція, BIA.

Продовження таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D2	Q12	Чи обмежено доступ працівників до спільних папок, архівів і чутливих файлів відповідно до службової необхідності?	R2; R3	ACL, групи доступу, журналювання доступу.
	Q13	Чи захищено архівні файли та критичні дані від несанкціонованої зміни за допомогою підпису, хешування, часових міток або журналювання?	R2; R3	Хеші, ЕЦП, журнали, контроль цілісності.
	Q14	Чи визначено правила зберігання, передавання та знищення чутливих даних?	R2; R3; R4	Політика даних, акти знищення, інструкції.
	Q15	Чи відстежуються випадки несанкціонованого винесення, передавання або публікації внутрішніх файлів?	R2; R3; R1	DLP, журнали, розслідування, дисциплінарні записи.
D3	Q16	Чи відокремлені ІТ- та ОТ-середовища технічно й організаційно, а обмін між ними контролюється?	R2; R3; R4	Сегментація, firewall rules, DMZ.
	Q17	Чи застосовується принцип глибоко ешелонованого захисту для цифрових активів і технологічних систем?		Рівні контролів, схеми захисту.

Продовження таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D3	Q18	Чи регламентовано віддалений доступ до IT/OT-середовища, зокрема MFA, часові обмеження, jump host, VPN і журналювання?	R2; R3; R6	Політика доступу, журнали VPN, MFA.
	Q19	Чи дотримуються вимоги щодо структури паролів і своєчасної зміни облікових даних?	усі ролі	Політика паролів, результати перевірок.
	Q20	Чи підтримуються цифрові пристрої в актуальному стані згідно з політикою оновлень?	R3; R2	Звіти патч-менеджменту.
	Q21	Чи забезпечується регулярне оновлення антивірусних/EDR-засобів і контроль їх працездатності?	R3; R2	Консолі AV/EDR, звіти.
	Q22	Чи аналізуються ризики, пов'язані з виходом в інтернет, електронною поштою, завантаженими файлами та використаними програмами?	R2; R3	Proxy logs, email security, sandboxing.
	Q23	Чи виявляються й усуваються корінні причини повторюваних вразливостей, а не лише окремі симптоми?	R2; R3	Problem management, RCA-звіти.
	Q24	Чи враховують процеси планування, експлуатації та технічного обслуговування вимоги кібербезпеки?	R4; R2	Плани робіт, чек-листи.
D4				

Продовження таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D4	Q25	Чи проходить заміна цифрового компонента перевірку на відповідність вимогам кібербезпеки перед введенням у роботу?	R4; R2; R3	Форми change request, акти приймання.
	Q26	Чи використовується система управління змінами для цифрової інфраструктури й технологічних систем?	R2; R3; R4	Change log, approvals.
	Q27	Чи є процес повідомлення про вразливості, їх відстеження та контроль усунення?	R2; R4; R3	Тікети, реєстр вразливостей.
	Q28	Чи керується використання портативних носіїв і мобільних пристроїв у технологічному середовищі?	R4; R2; R3	Політика USB, whitelist, журнали.
	Q29	Чи мають працівники експлуатації та обслуговування достатню підготовку для роботи з чутливими цифровими активами?	R4; R2	Сертифікати навчання, допуски.
	Q30	Чи є регулярна взаємодія між кібербезпекою, ІТ та експлуатацією щодо змін, ризиків і проблем у цифрових системах?	R2; R3; R4	Протоколи зустрічей, спільні заявки.

Продовження таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D5	Q31	Чи ведеться перелік постачальників, підрядників і сервісних організацій, від яких залежать критичні функції?	R1; R2; R6	Реєстр постачальників, класифікація.
	Q32	Чи оцінюється кібербезпека ланцюга постачання цифрових компонентів і супутніх послуг до підключення або закупівлі?	R1; R2; R6	Оцінка постачальника, вимоги договору.
	Q33	Чи перевіряються права стороннього доступу, технічного обслуговування та повноваження підрядників?	R2; R3; R6	Списки доступу, журнали сесій.
	Q34	Чи мають продавці й підрядники достатній рівень обізнаності про кібербезпеку та вимоги об'єкта?	R6; R4; R2	Інструктажі, договори, підписані вимоги.
	Q35	Чи враховано, що інцидент може виникнути не лише через злий умисел, а й через помилки персоналу або підрядника?	R1; R2; R4; R6	Ризик-сценарії, навчання, процедури контролю.
	Q36	Чи періодично переоцінюються раніше виявлені проблеми в роботі постачальників або підрядників?	R2; R1; R6	Плани коригувальних дій, повторна оцінка.

Продовження таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D6	Q37	Чи спрацює система фізичного захисту відповідно до встановлених сценаріїв і чи перевіряється це тестуванням?	R5; R2; R4	Журнали тестів, акти перевірки.
	Q38	Чи дотримується встановлений рівень допуску для працівників, відвідувачів і сторонніх осіб?	R5; R1	Пропускний режим, журнали входу.
	Q39	Чи визначено правила зберігання відеозаписів, доступу до них, строків зберігання та захисту від зміни або видалення?	R5; R2; R3	Політика відеоспостереження, журнали доступу.
	Q40	Чи дотримується частота патрулювання території та чи відповідає фактичний процес затвердженому протоколу?	R5	Маршрути, журнали патрулювання.
	Q41	Чи застосовуються додаткові механізми перевірки особи, наприклад біометрія або двофакторний фізичний доступ, для критичних зон?	R5; R1	Система контролю доступу, регламент.
	Q42	Чи перевіряються сторонні предмети, носії та обладнання при вході/виході з критичних зон відповідно до процедури?	R5; R4	Процедури огляду, журнали.

Продовження таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D6	Q43	Чи відпрацьовуються сценарії кіберфізичних атак та дій внутрішнього порушника?	R5; R2; R4; R1	Плани навчань, звіти, сценарії.
	Q44	Чи існує процес оповіщення групи кібербезпеки та керівників про потенційні кіберінциденти або аномалії?	R4; R2; R3; R5	Процедури, контакти, журнали повідомлень.
	Q45	Чи визначено сценарії реагування на інциденти, що одночасно впливають на ІТ, ОТ і фізичну безпеку?	R2; R4; R5; R1	IR playbooks, сценарії tabletop.
D7	Q46	Чи брали ключові ролі участь у навчаннях з реагування на кіберінцидент протягом останніх 12 місяців?	R1; R2; R4; R5	Журнали навчань, учасники.
	Q47	Чи визначено порядок комунікації із зовнішніми суб'єктами: CERT, регуляторами, постачальниками, підрядниками та правоохоронними органами?	R1; R2; R6	Контакт-лист, MoU, процедури.
	Q48	Чи дозволяють журнали, моніторинг і процеси аналізу підтвердити фактичний перебіг інциденту?	R2; R3; R4	SIEM, журнали, кореляційні правила.
	Q49	Чи фіксуються та відстежуються проблемні питання й недоліки з кібербезпеки в офіційній системі управління інформацією?	R2; R1	Тікети, реєстр проблем, статуси.

Продовження таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D7	Q50	Чи проводиться періодичне переоцінювання сфер, де були виявлені проблеми, для перевірки ефективності усунення?	R2; R1; R5	Повторні оцінки, corrective action plan.
	Q51	Чи проходять працівники навчання з кібербезпеки відповідно до своєї ролі та рівня доступу?	Усі ролі	Списки навчання, відсоток проходження.
D8	Q52	Чи перевіряється здатність працівників ідентифікувати, зупинити й повідомити про соціальну інженерію або фішинг?	Усі ролі;	Фішинг-тести, результати.
	Q53	Чи дотримуються працівники процедур повідомлення після виявлення імітованої або реальної фішингової атаки?	Усі ролі;	Звіти навчань, helpdesk-заявки.
	Q54	Чи демонструють працівники розуміння безпекової політики, процесів і норм?	Усі ролі	Тестування, опитування, аудит.
	Q55	Чи дотримуються працівники правил захисту робочого місця перед залишенням робочої зони?	Усі ролі;	Огляд робочих місць, clean desk checks.
	Q56	Чи повідомляють працівники про потенційні питання кібербезпеки та звертаються по рекомендації у сумнівних ситуаціях?	Усі ролі;	Канали повідомлення, кількість звернень.

Кінець таблиці А.1

Домен	Код	Питання	Ролі	Підтвердження
D8	Q57	Чи відстежуються зловживання ресурсами, майнінг, витік файлів?	R1; R2; R3; R5	Моніторинг, HR/security processes.
	Q58	Чи визначено пріоритетність відновлення критичних функцій і систем, від яких вони залежать?	R1; R2; R4	BCP/DRP, BIA, пріоритети.
D9	Q59	Чи дотримується періодичність створення резервних копій відповідно до політики організації?	R3; R2	Backup reports, журнали.
	Q60	Чи використовуються різні варіанти збереження резервних копій, зокрема ізоляція або офлайн-копії?	R3; R2	Схема резервування, перевірка копій.
	Q61	Чи захищені резервні копії від несанкціонованого видалення, зміни або шифрування під час інциденту?	R3; R2	Immutable backups, RBAC, журнали.
	Q62	Чи перевіряється можливість відновлення з резервних копій на практиці, а не лише факт їх створення?	R3; R2; R4	Звіти тестового відновлення.
	Q63	Чи забезпечено безпечний перехід на резервний, ізольований або ручний режим керування?	R4; R1; R2	Процедури ручного режиму, навчання.
	Q64	Чи забезпечено резервне живлення (ДБЖ) для критичних мережевих компонентів?	R3; R4	Схеми живлення, UPS tests.

ДОДАТОК Б

СТРУКТУРА РЕПОЗИТОРІЮ ПРОГРАМНОГО ЗАСТОСУНКУ

Програмна реалізація інформаційного забезпечення профілювання кіберстійкості об'єктів критичної інфраструктури розміщена у відкритому віддаленому репозиторії на платформі GitHub.

Повне посилання на сирцевий код проєкту: <https://github.com/slbdn/cyber-resilience-profiler>

Нижче представлено архітектурну структуру директорій та файлів розробленого програмного комплексу.

cyber-resilience-profiler /

— README.md	- інструкція з розгортання проєкту
— app.py	- головний виконуваний модуль графічного вебінтерфейсу користувача (Streamlit)
— config_assessment.py	- модуль конфігурації доменів кіберстійкості та логіки рольової фільтрації
— cyber_resilience_assessment.db	- локальна реляційна база даних результатів опитування експертів (SQLite)
— profil_kiberstiikosti_1.xlsx	- звітний файл експорту підсумкового профілю кіберстійкості енергооб'єкта
— requirements.txt	- специфікація залежностей та зовнішніх бібліотек програмного середовища
— sensitivity_analysis_combined.py	- аналітичний модуль оцінювання чутливості та моделювання Монте-Карло
— sensitivity_results.xlsx	- файл фіксації розрахункових масивів стохастичного аналізу чутливості

ДОДАТОК В

КЛЮЧОВІ ФРАГМЕНТИ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ МЕТОДИКИ

У додатку наведено скорочені фрагменти програмної реалізації, які безпосередньо відповідають методичній частині дипломної роботи. Повний код програмного засобу подано в репозиторії, зазначеному в додатку Б.

В.1 Конфігурація ролей, шкали відповідей і ваг доменів

```

12 ANSWER_OPTIONS = {
13     "1 – досягнуто / так / реалізовано": 1.0,
14     "0.5 – частково досягнуто / частково реалізовано": 0.5,
15     "0 – не досягнуто / ні / відсутнє": 0.0,
16 }
17
18 ROLE_DEFINITIONS = {
19     "R1": "Вище керівництво",
20     "R2": "Фахівці з кібербезпеки",
21     "R3": "ІТ-персонал",
22     "R4": "ОТ / експлуатація та обслуговування",
23     "R5": "Фізична безпека",
24     "R6": "Підрядники / постачальники",
25 }
26
27 DOMAIN_WEIGHTS = dict([('D1. Управління, стратегія та ризики', 0.12),
28 ('D2. Критичні функції, цифрові активи та дані', 0.13),
29 ('D3. Архітектура, сегментація, доступ і технічна гігієна', 0.14),
30 ('D4. Експлуатація, технічне обслуговування та управління змінами', 0.1),
31 ('D5. Треті сторони, підрядники та ланцюг постачання', 0.1),
32 ('D6. Фізична та кібер-фізична безпека', 0.11),
33 ('D7. Виявлення, моніторинг і реагування', 0.14),
34 ('D8. Обізнаність, навчання та людський фактор', 0.1),
35 ('D9. Безперервність, резервування та відновлення', 0.16)])

```

Рисунок В.1 – Фрагмент коду конфігурації

В.2 Відбір питань відповідно до ролі респондента

```

230 def role_matches(role_code: str, target_roles: str) -> bool:
231     normalized = (target_roles or "").lower()
232     if "uci poli" in normalized:
233         return True
234     targets = [part.strip() for part in str(target_roles).split(";") if part.strip()]
235     return role_code in targets
236
237
238 def get_questions_for_role(role_code=None) -> pd.DataFrame:
239     df = read_sql("SELECT * FROM questions")
240     df["sort_key"] = df["question_id"].apply(question_sort_key)
241     if role_code:
242         df = df[df["target_roles"].apply(lambda value: role_matches(role_code, value))]
243     return df.sort_values(["domain", "sort_key"]).drop(columns=["sort_key"])

```

Рисунок В.2 – Фрагмент коду реалізації рольового відбору питань

В.3 Формування звіту формату Excel

```

324 def export_excel(assessment_id):
325     profile = read_sql("SELECT * FROM assessments WHERE assessment_id = ?", [assessment_id])
326     respondents = read_sql(
327         "SELECT respondent_no, respondent_name, role_code, role, department FROM respondents WHERE assessment_id = ? ORDER BY respondent_no",
328         [assessment_id],
329     )
330     questions = get_questions_for_role(None)
331     metrics = read_sql("SELECT * FROM quantitative_metrics ORDER BY metric_id")
332     responses, domain, criteria, roles, gaps = calculate_results(assessment_id)
333
334     if not domain.empty:
335         overall = domain["weighted_score"].sum() / domain["weight"].sum() if domain["weight"].sum() else domain["domain_score"].mean()
336     else:
337         overall = None

```

Рисунок В.3 – Фрагмент реалізації можливості формування звіту формату Excel

В.4 Розрахунок доменних оцінок

```

281 def calculate_results(assessment_id):
282     df = get_all_data(assessment_id)
283     weights = read_sql("SELECT * FROM domain_weights")
284     if df.empty:
285         return df, pd.DataFrame(), pd.DataFrame(), pd.DataFrame(), pd.DataFrame()
286
287     domain = (
288         df.groupby("domain")
289         .apply(lambda g: (g["score"] * g["question_weight"]).sum() / g["question_weight"].sum(), include_groups=False)
290         .reset_index(name="domain_score")
291     )
292     domain = domain.merge(weights, on="domain", how="left")
293     domain["weight"] = domain["weight"].fillna(0)
294     domain["weighted_score"] = domain["domain_score"] * domain["weight"]
295     domain["level"] = domain["domain_score"].apply(classify_score)

```

Рисунок В.4 – Фрагмент обчислення доменних оцінок на основі відповідей респондентів

В.5 Розрахунок інтегрального індексу кіберстійкості

```

194 def calculate_overall_index(domain_scores: pd.DataFrame) -> float:
195     if domain_scores.empty:
196         return float("nan")
197     return weighted_average(domain_scores["domain_score"], domain_scores["weight"])

```

Рисунок В.5 – Фрагмент коду розрахунку інтегрального індексу кіберстійкості

В.6 Короткий підсумок проведеного опитування

```

339 summary = pd.DataFrame([
340     {"Показник": "Загальна оцінка кіберстійкості", "Значення": None if overall is None else round(overall, 3)},
341     {"Показник": "Рівень", "Значення": classify_score(overall) if overall is not None else "Немає даних"},
342     {"Показник": "Кількість відповідей", "Значення": len(responses)},
343     {"Показник": "Кількість прогалин", "Значення": len(gaps)},
344 ])

```

Рисунок В.6 – Фрагмент коду формування підсумкових показників опитування

В.7 Модифікація ваг і часткових оцінок у сценарному аналізі

```

200 def change_critical_weights(weights: pd.DataFrame, delta: float) -> pd.DataFrame:
201     modified = weights.copy()
202     critical = modified["domain"].apply(is_critical_domain)
203     modified.loc[critical, "weight"] = modified.loc[critical, "weight"] * (1 + delta)
204     return normalize_weights(modified)
205
206
207 def change_partial_scores(responses: pd.DataFrame, value: float, only_critical_domains: bool = True) -> pd.DataFrame:
208     modified = responses.copy()
209     mask = modified["score"].eq(0.5)
210     if only_critical_domains:
211         mask = mask & modified["domain"].apply(is_critical_domain)
212     modified.loc[mask, "score"] = value
213     return modified

```

Рисунок В.7 – Фрагмент налаштування сценарного аналізу

В.8 Формування сценаріїв аналізу чутливості

```

265 def run_scenario_analysis(
266     assessment_id: str,
267     aggregation: str = DEFAULT_AGGREGATION,
268 ) -> tuple[pd.DataFrame, pd.DataFrame, pd.DataFrame]:
269     responses = load_responses(assessment_id)
270     weights = load_domain_weights()
271
272     scenarios = [
273         ("Базовий", "Початкові ваги та оцінки", responses, weights),
274         ("Ваги -10%", "Зменшення ваг критичних доменів із нормалізацією", responses, change_critical_weights(weights, -0.10)),
275         ("Ваги +10%", "Збільшення ваг критичних доменів із нормалізацією", responses, change_critical_weights(weights, 0.10)),
276         ("Песимістичний", "Часткові оцінки 0.5 у критичних доменах інтерпретовано як 0.4", change_partial_scores(responses, 0.4, weights),
277         ("Оптимістичний", "Часткові оцінки 0.5 у критичних доменах інтерпретовано як 0.6", change_partial_scores(responses, 0.6, weights),
278     ]
279
280     summary_rows: list[dict] = []
281     domain_tables: list[pd.DataFrame] = []
282     base_index: float | None = None
283
284     for name, condition, data, scenario_weights in scenarios:
285         domain_scores = calculate_domain_scores(data, scenario_weights, aggregation)
286         index = calculate_overall_index(domain_scores)
287         if name == "Базовий":
288             base_index = index
289
290         summary_rows.append(
291             {
292                 "Сценарій": name,
293                 "Умова перерахунку": condition,
294                 "Інтегральний індекс": round(index, 3),
295                 "Відхилення від базового значення": None if base_index is None else round(index - base_index, 3),
296                 "Рівень": classify_score(index),
297             }
298         )

```

Рисунок В.8 – Фрагмент формування аналізу чутливості

В.9 Моделювання невизначеності методом Монте-Карло

```

310 def randomize_partial_scores(responses: pd.DataFrame, rng: np.random.Generator, score_delta: float) -> pd.DataFrame:
311     modified = responses.copy()
312     partial = modified["score"].eq(0.5)
313     if partial.any():
314         low = max(0.0, 0.5 - score_delta)
315         high = min(1.0, 0.5 + score_delta)
316         modified.loc[partial, "score"] = rng.uniform(low, high, size=int(partial.sum()))
317     return modified
318
319
320 def randomize_weights(weights: pd.DataFrame, rng: np.random.Generator, weight_delta: float) -> pd.DataFrame:
321     modified = weights.copy()
322     multipliers = rng.uniform(1 - weight_delta, 1 + weight_delta, size=len(modified))
323     modified["weight"] = modified["weight"].to_numpy(dtype=float) * multipliers
324     return normalize_weights(modified)

```

Рисунок В.9 – Фрагмент налаштування параметрів моделювання методом Монте-Карло

В.10 Ітераційний перерахунок інтегрального індексу

```

348     rng = np.random.default_rng(seed)
349     indexes: list[float] = []
350     levels: list[str] = []
351     domain_rows: list[pd.DataFrame] = []
352
353     for iteration in range(1, iterations + 1):
354         sim_responses = randomize_partial_scores(responses, rng, score_delta)
355         sim_weights = randomize_weights(weights, rng, weight_delta)
356         sim_domains = calculate_domain_scores(sim_responses, sim_weights, aggregation)
357         sim_index = calculate_overall_index(sim_domains)
358
359         indexes.append(sim_index)

```

Рисунок В.10 – Фрагмент коду ітераційного перерахунку інтегрального індексу методом Монте-Карло

Наведені фрагменти демонструють ключові можливості програмної реалізації запропонованої методики. Інструмент автоматично відбирає питання відповідно до ролі респондента, зберігає відповіді у структурованій базі даних, перетворює якісні відповіді у числові значення та розраховує доменні оцінки з урахуванням вагових коефіцієнтів. Окремою перевагою реалізації є формування інтегрального індексу кіберстійкості. Також у програмному коді реалізовано аналіз чутливості результатів. Сценарний перерахунок і моделювання методом Монте-Карло дають змогу перевірити, наскільки стабільним залишається інтегральний індекс за зміни ваг доменів і часткових експертних оцінок.