МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИКА ОЦІНЮВАННЯ ЗРІЛОСТІ СИСТЕМ КІБЕРЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ІЗ ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Олексій КЛІМЧЕНКО

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБДМ-61
Олексій КЛІМЧЕНКО

Керівник:
к.т.н., доцент Юрій ЩАВІНСЬКИЙ
Ім’я, ПРІЗВИЩЕ

Рецензент:
к.т.н., доцент Юрій ПЕПА
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Клімченку Олексію Романовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Методика оцінювання зрілості систем кіберзахисту об'єктів критичної інформаційної інфраструктури із застосуванням штучного інтелекту"

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н., доцент.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи "11" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи:. сучасні підходи та моделі зрілості в кібербезпеці (CMMI, C2M2, NIST CSF тощо), нормативно-правові документи оцінювання зрілості.
4. Перелік питань, які потрібно розробити:
   1. Дослідити теоретичні та методологічні засади оцінювання зрілості систем кіберзахисту.
   2. Проаналізувати сучасні підходи до застосування штучного інтелекту в оцінюванні та управлінні кіберзахистом.
   3. Розробити методику оцінювання зрілості систем кіберзахисту із застосуванням штучного інтелекту
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідження теоретичних та методологічних засад оцінювання зрілості систем кіберзахисту.	27.10.2025	
4.	Аналіз сучасних підходів до застосування штучного інтелекту в оцінюванні та управлінні кіберзахистом.	10.11.2025	
5.	Розробка методики оцінювання зрілості систем кіберзахисту із застосуванням штучного інтелекту.	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Олексій КЛІМЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Клімченко О.Р. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
на тему: "Методика оцінювання зрілості систем кіберзахисту об'єктів критичної інформаційної інфраструктури із застосуванням штучного інтелекту"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **КЛІМЧЕНКО Олексій** у кваліфікаційній роботі дослідив теоретичні та методологічні засади оцінювання зрілості систем кіберзахисту, проаналізував сучасні підходи до застосування штучного інтелекту в оцінюванні та управлінні кіберзахистом, а також розробив методику оцінювання зрілості систем кіберзахисту із застосуванням штучного інтелекту.

КЛІМЧЕНКО Олексій показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **КЛІМЧЕНКА Олексія** на оцінку "добре" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Клімченко О.Р. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Клімченка Олексія Романовича
на тему “ Методика оцінювання зрілості систем кіберзахисту об’єктів критичної інформаційної інфраструктури із застосуванням штучного інтелекту ”

Актуальність Актуальність теми дипломної роботи зумовлена зростанням кількості та складності кіберзагроз щодо об’єктів критичної інформаційної інфраструктури, порушення функціонування яких може мати суттєві соціально-економічні та безпекові наслідки. В умовах цифровізації державних і корпоративних систем особливого значення набуває не лише впровадження засобів кіберзахисту, а й об’єктивне оцінювання рівня їх зрілості. Традиційні експертні підходи часто є статичними та суб’єктивними, що обмежує їх ефективність у динамічному кіберсередовищі. У цьому контексті застосування методів штучного інтелекту для оцінювання зрілості систем кіберзахисту є своєчасним та науково обґрунтованим напрямом дослідження.

Позитивні сторони

У дипломній роботі послідовно та логічно вирішено поставлені завдання. Автором ґрунтовно досліджено теоретичні та методологічні засади оцінювання зрілості систем кіберзахисту, проаналізовано сучасні підходи до використання штучного інтелекту в процесах оцінювання та управління кібербезпекою. Особливу наукову та практичну цінність має розроблена методика оцінювання зрілості систем кіберзахисту із застосуванням інтелектуальних моделей, яка дозволяє підвищити об’єктивність, адаптивність та аналітичну глибину оцінювання. Робота характеризується достатнім рівнем наукової новизни, коректним використанням термінології та логічною структурою викладу матеріалу.

Недоліки

Разом з тим, у роботі доцільно було б більш детально обґрунтувати вибір конкретних моделей штучного інтелекту та розширити експериментальну частину шляхом апробації методики на більшій кількості реальних об’єктів критичної інформаційної інфраструктури. Також корисним було б доповнення методики рекомендаціями щодо її інтеграції у практичну діяльність центрів кіберзахисту або SOC. Зазначені зауваження не знижують загальної позитивної оцінки роботи, мають рекомендаційний характер і не впливають на досягнення поставленої мети.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Клімченко Олексій Романович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною та кіернетичною безпекою”.

Рецензент:
професор кафедри
Технічних систем кіберзахисту
к.т.н, доцент _____ Юрій ПЕПА
підпис *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 90 стор., 18 рис., 10 табл., 62 джерелf.

Метою роботи є розробка та обґрунтування методики оцінювання зрілості систем кіберзахисту об'єктів критичної інформаційної інфраструктури з використанням технологій штучного інтелекту для підвищення ефективності управління кібербезпекою.

Об'єктом дослідження є системи кіберзахисту об'єктів критичної інформаційної інфраструктури.

Предмет дослідження – методичні підходи, моделі та інструменти оцінювання зрілості систем кіберзахисту із застосуванням штучного інтелекту.

Методи дослідження. : аналіз і синтез наукових джерел, систематизація підходів до оцінювання зрілості, порівняльний аналіз міжнародних стандартів, аналіз кейсів кіберінцидентів та існуючих практик оцінювання зрілості, методи штучного інтелекту (машинне навчання, кластеризація, класифікація, виявлення аномалій), моделювання процесів кіберзахисту, побудова моделей, схем, діаграм та матриць зрілості.

Короткий зміст роботи. Як результат у роботі досліджено теоретичні та методологічні засади оцінювання зрілості систем кіберзахисту, проаналізовано сучасні підходи до застосування штучного інтелекту в оцінюванні та управлінні кіберзахистом, а також розроблено методику оцінювання зрілості систем кіберзахисту із застосуванням штучного інтелекту

Галузь застосування. Розроблені підходи можуть бути використані під час планування та впровадження систем кіберзахисту об'єктів критичної інформаційної інфраструктури, зокрема для оцінювання рівня їх зрілості та підвищення ефективності протидії сучасним кіберзагрозам із застосуванням методів штучного інтелекту.

КЛЮЧОВІ СЛОВА : КІБЕРЗАХИСТ, КРИТИЧНА ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА, ЗРІЛІСТЬ СИСТЕМ КІБЕРЗАХИСТУ, ОЦІНЮВАННЯ ЗРІЛОСТІ, ШТУЧНИЙ ІНТЕЛЕКТ, УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 90 pages, 18 figures, 10 tables, 62 sources.

The purpose of the work is to develop and justify a methodology for assessing the maturity of cyber protection systems for critical information infrastructure objects using artificial intelligence technologies to improve the effectiveness of cybersecurity management.

Object of research is cyber protection systems for critical information infrastructure objects.

Subject ***of research*** is methodological approaches, models, and tools for assessing the maturity of cyber protection systems using artificial intelligence.

Research methods Theoretical, empirical, applied and visualisation methods are used to analyse and develop a methodology for assessing the maturity of cyber protection systems for critical information infrastructure using artificial intelligence.

Brief content of research. As a result, the work examines the theoretical and methodological foundations of assessing the maturity of cyber defence systems, analyses modern approaches to the application of artificial intelligence in assessing and managing cyber defence, and develops a methodology for assessing the maturity of cyber defence systems using artificial intelligence.

Field of research. The developed approaches can be used in the planning and implementation of cyber protection systems for critical information infrastructure, in particular for assessing their maturity level and improving the effectiveness of countering modern cyber threats using artificial intelligence methods.

KEYWORDS: CYBER DEFENCE, CRITICAL INFORMATION INFRASTRUCTURE, MATURITY OF CYBER DEFENCE SYSTEMS, MATURITY ASSESSMENT, ARTIFICIAL INTELLIGENCE, CYBER SECURITY MANAGEMENT.

ЗМІСТ

ВСТУП

Актуальність теми. Об’єкти критичної інформаційної інфраструктури держави, підприємств та установ відіграють ключову роль у забезпеченні національної безпеки, стабільності економіки та безперервності життєво важливих процесів. З огляду на зростання кількості, складності та цілеспрямованості кіберзагроз, питання забезпечення належного рівня кіберзахисту таких об’єктів набуває особливої актуальності. Водночас ефективність кіберзахисту значною мірою залежить від рівня зрілості відповідних систем, що зумовлює необхідність розроблення обґрунтованих методик їх оцінювання.

Сучасні технології штучного інтелекту відкривають нові можливості для автоматизації процесів аналізу, моніторингу та оцінювання стану кіберзахисту, дозволяючи обробляти великі обсяги даних, виявляти приховані закономірності та підвищувати об’єктивність прийняття управлінських рішень. Разом із тим, застосування штучного інтелекту в процесах оцінювання зрілості систем кіберзахисту потребує науково обґрунтованих підходів, які враховують специфіку критичної інформаційної інфраструктури, вимоги нормативно-правових документів та сучасні моделі управління кібербезпекою.

У зв’язку з цим, розроблення методики оцінювання зрілості систем кіберзахисту об’єктів критичної інформаційної інфраструктури із застосуванням штучного інтелекту є актуальним науково-практичним завданням, вирішення якого сприятиме підвищенню ефективності управління кібербезпекою, своєчасному виявленню вразливостей та обґрунтуванню напрямів подальшого розвитку систем кіберзахисту.

Мета роботи полягає у розробці та обґрунтуванні методики оцінювання зрілості систем кіберзахисту об’єктів критичної інформаційної інфраструктури з використанням технологій штучного інтелекту для підвищення ефективності управління кібербезпекою.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити теоретичні та методологічні засади оцінювання зрілості систем кіберзахисту.

2. Проаналізувати сучасні підходи до застосування штучного інтелекту в оцінюванні та управлінні кіберзахистом.

3. Розробити методику оцінювання зрілості систем кіберзахисту із застосуванням штучного інтелекту

Об'єкт дослідження **–** системи кіберзахисту об'єктів критичної інформаційної інфраструктури.

Предмет дослідження – методичні підходи, моделі та інструменти оцінювання зрілості систем кіберзахисту із застосуванням штучного інтелекту.

Методи дослідження. Аналіз і синтез – для опрацювання наукових публікацій, міжнародних і національних стандартів та рекомендацій (ISO/IEC, NIST, ENISA та інших профільних організацій) у сфері кіберзахисту та оцінювання зрілості систем безпеки, а також для формування цілісного уявлення про можливості застосування штучного інтелекту в цих процесах.

Системний та структурно-функціональний аналіз – для дослідження систем кіберзахисту об'єктів критичної інформаційної інфраструктури як складних соціотехнічних систем, визначення взаємозв'язків між організаційними, технічними та процесними компонентами, а також ролі штучного інтелекту в забезпеченні їх зрілості.

Порівняльний аналіз – для зіставлення існуючих моделей і фреймворків оцінювання зрілості кібербезпеки (CMMI, NIST CSF, ISO/IEC 27001/27002, SOC-CMM тощо), а також визначення можливостей їх удосконалення шляхом інтеграції методів штучного інтелекту.

Метод експертних оцінок – для визначення вагових коефіцієнтів критеріїв і показників зрілості систем кіберзахисту об'єктів критичної інформаційної інфраструктури, а також для оцінювання практичної доцільності застосування інтелектуальних методів у процесі прийняття управлінських рішень.

Моделювання – для розроблення методики оцінювання зрілості систем кіберзахисту із застосуванням штучного інтелекту, з урахуванням етапів збору

та обробки даних, аналізу стану захищеності, формування інтегральних показників та вироблення рекомендацій щодо підвищення рівня кіберзахисту.

Наукова новизна роботи полягає в тому, що запропоновано методику оцінювання зрілості систем кіберзахисту об'єктів критичної інформаційної інфраструктури із застосуванням технологій штучного інтелекту, розроблено модель інтеграції алгоритмів AI у процес оцінювання зрілості систем кіберзахисту, удосконалено підхід до формування критеріїв зрілості, що враховують не лише організаційно-правові й технічні аспекти, а й інтелектуальну підтримку прийняття рішень.

Практичне значення одержаних результатів. Застосування розробленої методики оцінювання зрілості систем кіберзахисту об'єктів критичної інформаційної інфраструктури із використанням технологій штучного інтелекту дозволяє організаціям здійснювати обґрунтоване оцінювання поточного стану кібербезпеки, визначати пріоритетні напрями її вдосконалення та підвищувати ефективність управління ризиками.

Отримані результати можуть бути використані під час планування та модернізації систем кіберзахисту, зокрема для автоматизованого аналізу інцидентів, виявлення вразливостей, прогнозування розвитку кіберзагроз і формування рекомендацій щодо підвищення рівня зрілості процесів безпеки. Запропонована методика також може бути інтегрована в діяльність центрів моніторингу безпеки (SOC) та систем управління інформаційною і кібербезпекою. Крім того, результати дослідження сприятимуть розробленню та актуалізації політик і процедур кібербезпеки відповідно до вимог міжнародних стандартів і нормативних документів, а також забезпечать практичну основу для прийняття управлінських рішень щодо розвитку систем кіберзахисту об'єктів критичної інформаційної інфраструктури з урахуванням специфіки їх функціонування та наявних ресурсів.

Апробація результатів кваліфікаційної роботи відбулася на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ОЦІНЮВАННЯ ЗРІЛОСТІ СИСТЕМ КІБЕРЗАХИСТУ

Питання забезпечення належного рівня кіберзахисту об’єктів критичної інформаційної інфраструктури набуває особливої актуальності. Ефективне функціонування таких систем визначається не лише наявністю технічних засобів, але й ступенем їх зрілості, що відображає комплексну спроможність протидіяти кіберзагрозам, адаптуватися до нових викликів та забезпечувати безперервність операцій. Формування об’єктивної методики оцінювання зрілості систем кіберзахисту передбачає врахування як нормативно-методичних засад, так і сучасних підходів, серед яких особливе місце займають технології штучного інтелекту. Їх використання дозволяє підвищити точність аналізу, автоматизувати процеси прийняття рішень і сформувати більш гнучкі та адаптивні моделі оцінювання.

1.1. Сутність і значення систем кіберзахисту для об’єктів критичної інформаційної інфраструктури

Системи кіберзахисту об’єктів критичної інформаційної інфраструктури (КІІ) становлять комплекс організаційних, технічних, програмних і процедурних заходів, спрямованих на забезпечення стійкості, безперервності та надійності функціонування інформаційно-телекомунікаційних систем, від яких залежить стабільність державних, економічних і соціальних процесів (рис. 1.1). КІІ охоплює енергетичні, транспортні, фінансові, телекомунікаційні, оборонні, медичні та інші системи, порушення роботи яких може спричинити масштабні негативні наслідки як на регіональному, так і на національному рівнях [1]. У зв’язку з цим питання побудови ефективних систем кіберзахисту набуває ключового стратегічного значення.

Сутність систем кіберзахисту полягає у створенні багаторівневої моделі захисту, яка забезпечує конфіденційність, цілісність, доступність та спостережуваність інформаційних ресурсів. Сучасні системи орієнтовані не лише на реагування на інциденти, але й на їхнє раннє виявлення, попередження, адаптацію до нових типів загроз, синхронізацію дій між зацікавленими суб'єктами безпеки [2]. Це зумовлено постійним зростанням складності кібератак, зокрема розвитком цілеспрямованих атак (APT), технологій соціальної інженерії, автоматизованих інструментів злому, використанням штучного інтелекту зловмисниками. Тому системи кіберзахисту КІІ мають забезпечувати не лише статичні механізми безпеки, а й динамічні функції адаптивної протидії загрозам.

Рис. 1.1 Багаторівнева модель системи кіберзахисту КІІ

Важливе значення для систем кіберзахисту має інтеграція ризик-орієнтованих підходів. В основі сучасних методологій лежить аналіз ризиків, який дозволяє оцінити ймовірність реалізації кіберзагроз, ступінь потенційних збитків, визначити пріоритети щодо впровадження заходів безпеки [3]. У контексті КІІ це особливо актуально, оскільки критичні системи мають складну архітектуру, взаємопов'язані з великою кількістю зовнішніх і внутрішніх

компонентів та характеризуються низькою толерантністю до збоїв. Це потребує системного підходу до моделювання загроз і побудови адекватних механізмів захисту.

Системи кіберзахисту виконують низку ключових функцій [4]:

- управління ідентифікацією та доступом (IAM);
- захист комунікацій та мережевої інфраструктури;
- моніторинг і виявлення аномалій, включно з використанням систем SIEM, SOC та інтелектуальних аналітичних платформ;
- захист кінцевих точок та серверної інфраструктури;
- забезпечення криптографічного захисту;
- управління інцидентами та безперервністю бізнес-процесів;
- аудит і тестування безпеки, включно з пентестом і Red/Blue Team практиками.

Опис цих функцій вказано у табл. 1.1

Таблиця 1.1

Основні функції систем кіберзахисту КІ

Функція	Зміст
Управління доступом	Контроль ідентифікації, авторизації та розмежування прав
Захист мережі	Міжмережеві екрани, сегментація, фільтрація трафіку
Виявлення загроз	SIEM, SOC, аналіз аномалій, автоматизоване реагування
Захист кінцевих точок	Антивірусні системи, EDR/XDR
Криптографічний захист	Шифрування, PKI, управління ключами
Управління інцидентами	Аналіз, реагування, відновлення
Аудит безпеки	Тестування, оцінювання відповідності, пентест

Особливість систем кіберзахисту для КІІ полягає у тому, що вони повинні забезпечувати як технічну, так і організаційну безпеку, включаючи виконання норм законодавства, стандартів, політик і процедур. Наявність відповідних нормативних вимог (наприклад, стандартів ISO/IEC 27000, NIST CSF, рекомендацій ЄС щодо кіберстійкості критичних секторів) формує основу для забезпечення системного та комплексного захисту [5]. У контексті управління зрілістю такі стандарти виступають фундаментом для побудови моделей оцінювання, що дозволяють визначити рівень розвитку системи, ступінь її відповідності найкращим практикам та пріоритетні напрями вдосконалення.

Значення систем кіберзахисту для КІІ підсилюється необхідністю протистояння кібератакам, які можуть мати наслідки національного масштабу. Порушення роботи електроенергетичних, газотранспортних, банківських або урядових систем може призвести до соціально-економічної нестабільності, зупинки критично важливих процесів, втрати конфіденційних даних, зниження довіри громадян до державних інституцій. Саме тому системи кіберзахисту повинні бути здатні до забезпечення кіберстійкості, тобто здатності не лише запобігати атакам, а й швидко відновлюватися після інцидентів (табл. 1.2).

Таблиця 1.2

Вплив порушення роботи КІІ на сферу діяльності

Сектор	**Наслідки кіберінциденту**
Енергетика	Знеструмлення, дестабілізація регіонів
Транспорт	Зупинка руху, затримки, аварії
Фінанси	Блокування транзакцій, фінансові втрати
Охорона здоров’я	Неможливість надання медичних послуг
Державне управління	Порушення роботи служб, витік даних

Нині суттєво зростає значення застосування штучного інтелекту в системах кіберзахисту КІІ [6]. Алгоритми машинного навчання та

інтелектуальної аналітики дозволяють автоматизувати процеси виявлення аномалій, прогнозування потенційних атак, класифікації інцидентів, оптимізації заходів реагування. Завдяки цьому підвищується якість аналізу даних, зменшується навантаження на аналітиків безпеки, забезпечується швидше прийняття рішень. Штучний інтелект стає ключовим елементом еволюції систем кіберзахисту та важливим інструментом у формуванні моделей оцінювання їхньої зрілості.

Системи кіберзахисту для об’єктів критичної інформаційної інфраструктури мають стратегічне значення для національної безпеки, соціальної стабільності та економічного розвитку [7]. Їх ефективність визначається здатністю забезпечити багаторівневий, адаптивний та інтегрований захист, що враховує специфіку критичних процесів, сучасний ландшафт загроз та розвиток інтелектуальних технологій. У цьому контексті оцінювання зрілості систем кіберзахисту набуває особливої важливості як інструмент об’єктивного аналізу та подальшого вдосконалення механізмів забезпечення кібербезпеки.

1.2. Підходи та моделі зрілості в кібербезпеці

Оцінювання зрілості систем кіберзахисту є одним із ключових інструментів управління інформаційною безпекою, що дозволяє визначити рівень сформованості процесів, відповідність найкращим практикам та готовність організації реагувати на сучасні кіберзагрози. Концепція зрілості походить із теорії процесного управління і з часом була адаптована до галузі кібербезпеки [8]. На відміну від традиційних методів аудиту, моделі зрілості надають можливість оцінити не лише факт наявності певних механізмів захисту, а насамперед їхню ефективність, системність, інтегрованість та здатність до розвитку (рис. 1.2).

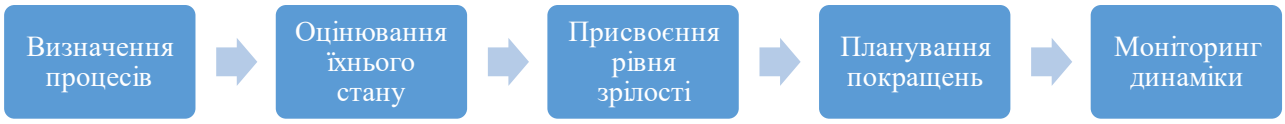

Рис.1.2 Загальна логіка моделей зрілості

Моделі зрілості забезпечують структурований підхід до аналізу, що включає визначення рівнів розвитку процесів, опис властивостей кожного рівня та встановлення критеріїв переходу від одного рівня до іншого. Застосування цих моделей дозволяє організаціям послідовно вдосконалювати механізми кіберзахисту, визначати слабкі місця, формувати рекомендації щодо оптимізації процесів та оцінювати динаміку змін [9]. Особливої актуальності моделі зрілості набувають для критичної інформаційної інфраструктури, де навіть невеликий інцидент може спричинити значні соціально-економічні наслідки.

У практиці кібербезпеки найпоширенішими є такі моделі: CMMI, C2M2, NIST Cybersecurity Framework (CSF), а також галузеві та комбіновані підходи, які адаптують загальні концепції до специфічних потреб організацій [10].

CMMI є універсальною моделлю зрілості, яка була розроблена для оцінювання процесів у сфері програмної інженерії, але згодом стала використовуватися і в кібербезпеці. Її основа полягає у визначенні п’яти рівнів зрілості, де кожен наступний рівень передбачає більш системний та структурований підхід до управління безпекою [11].

Основні рівні CMMI:

1. Initial (початковий) – процеси хаотичні, реактивні, залежні від окремих фахівців.

2. Managed (керований) – з’являється базова документація, контроль та моніторинг.

3. Defined (визначений) – процеси стандартизовані, узгоджені між підрозділами.

4. Quantitatively Managed (кількісно керований) – прийняття рішень спирається на метрики.

5. Optimizing (оптимізований) – безперервне вдосконалення та інноваційність.

Використання CMMI у кібербезпеці дозволяє оцінити ступінь формалізації заходів, рівень системності процесів реагування, моніторингу, аналізу ризиків та інших аспектів. Проте модель не є вузькоспеціалізованою для галузі безпеки, тому часто застосовується в комбінації з іншими підходами.

C2M2 була розроблена Міністерством енергетики США для об’єктів критичної інфраструктури, і саме тому вона широко використовується в енергетичному секторі, промисловості та державному управлінні. На відміну від CMMI, вона повністю сфокусована на кібербезпеці та включає набір доменів, потрібних для комплексної оцінки [12].

Основні домени C2M2:

– управління ризиками;

– управління активами;

– загрози та вразливості;

– моніторинг;

– реагування та відновлення;

– управління персоналом;

– зовнішні взаємодії;

– ситуаційна обізнаність;

– кіберстійкість.

Модель містить три рівні зрілості (Tier 1–3), що дозволяє організації оцінити, наскільки її процеси є повторюваними, документованими та системно інтегрованими.

Перевагою C2M2 є її практична спрямованість, чітка структура та орієнтація на критичну інфраструктуру, що робить її зручним інструментом для державних установ та великих організацій з високими вимогами до безпеки (табл. 1.3).

Таблиця 1.3

Порівняння рівнів CMMI та C2M2

Рівень CMMI	**Характеристика**	**Відповідний рівень C2M2**	**Характеристика**
1	Хаотичні процеси	Tier 1	Реактивні дії
2	Документування	Tier 2	Повторюваність процесів
3–5	Інтеграція, метрики, оптимізація	Tier 3	Інтегрована система безпеки

NIST CSF є однією з найбільш відомих та універсальних моделей управління кібербезпекою. Її концептуальний підхід базується на виділенні п’яти основних функцій [13]:

1. Identify (Ідентифікація) – розуміння ресурсів, ризиків, процесів.
2. Protect (Захист) – впровадження заходів для запобігання інцидентам.
3. Detect (Виявлення) – моніторинг, аналітика, аналіз аномалій.
4. Respond (Реагування) – мінімізація шкоди від інцидентів.
5. Recover (Відновлення) – повернення систем до нормального стану.

Хоча NIST CSF не є класичною моделлю зрілості, у 2021–2023 роках були розроблені додаткові методики, що дозволяють оцінювати рівень зрілості відповідно до функцій та категорій фреймворку. Таким чином, організації можуть оцінювати наявність процесів, їхню якість, відповідність практикам NIST та ефективність впровадження [14].

Важливо, що NIST CSF є одним з найгнучкіших підходів і може використовуватися як основа для створення комбінованих моделей оцінювання зрілості.

У практиці кібербезпеки використовуються також інші моделі:

ISO/IEC 21827 (SSE-CMM)

Одна з перших спеціалізованих моделей зрілості для безпеки. Регламентує вимоги до процесів захисту в системах різного призначення. Охоплює як технічні, так і організаційні складові [15].

COBIT

Модель управління IT, що включає оцінювання зрілості компонентів управління безпекою. COBIT застосовується для великих організацій та у секторах, де високі вимоги до контролю IT-процесів [16].

MMCAF (Maturity Model for Cybersecurity Assessment Framework)

Використовується у ЄС для операторів критичних послуг. Ґрунтується на директивах NIS/NIS2 та забезпечує охоплення нормативних та технічних вимог [17].

MITRE CMM

Спеціалізована модель для аналізу кіберзагроз і протидії їм. Орієнтована на розвідувальні та оборонні структури [18].

Усе це підкреслює, що моделі зрілості є багатокомпонентним інструментом, і їх застосування залежить від специфіки організації, вимог галузі та рівня критичності інфраструктури.

Незважаючи на різноманітність моделей, вони мають кілька спільних характеристик [19]:

- ієрархічність рівнів;
- орієнтація на процесний підхід;

необхідність документування та узгодженості процесів;

акцент на безперервному вдосконаленні.

Однак відрізняються вони за призначенням:

1. CMMI – універсальний підхід;
2. C2M2 – спеціалізована модель для КІІ;
3. NIST CSF – регулятивно-методична база;
4. SSE-CMM – модель безпеки з технічним фокусом.

Це дозволяє організаціям обирати як одну модель, так і комбінувати їх.

В умовах розвитку штучного інтелекту та складності загроз зростає актуальність адаптивних моделей зрілості. Сучасні підходи передбачають [20]:

- застосування AI для аналізу процесів;
- автоматизоване створення метрик зрілості;
- використання динамічних моделей замість статичних;
- інтеграцію різних моделей для побудови комплексних оцінок.

Це забезпечує не лише відповідність стандартам, а й практичну ефективність кіберзахисту (табл. 1.4).

Таблиця 1.4

Порівняння ключових моделей зрілості

Модель	Призначення	Рівні зрілості	Сильні сторони
CMMI	Загальне процесне вдосконалення	5	Глибока структурність
C2M2	Кібербезпека КІІ	3	Орієнтація на критичні сектори
NIST CSF	Управління кіберризиками	Функціональні рівні	Гнучкість та універсальність
SSE-CMM	Захист інформаційних систем	5	Технічна фокусованість
COBIT	IT-управління	5	Управління корпоративними процесами

1.3. Нормативно-правові та стандартні вимоги до оцінювання зрілості систем кіберзахисту (Україна, ЄС, США)

Оцінювання зрілості систем кіберзахисту є важливим компонентом державної політики у сфері захисту критичної інформаційної інфраструктури, а також обов’язковим елементом корпоративного управління безпекою. Нормативно-правова база різних країн встановлює вимоги до рівня захищеності, процедур управління ризиками, стандартів безпеки та перевірки ефективності впроваджених механізмів. Важливим аспектом таких вимог є саме визначення

критеріїв зрілості процесів кіберзахисту, що дозволяє оцінювати не лише наявність технічних засобів, а й ступінь їхньої інтегрованості, системності та відповідності сучасним викликам.

Комплексний аналіз нормативних документів України, Європейського Союзу та США дає змогу простежити спільні тенденції: зростання ролі ризик-орієнтованих підходів, впровадження вимог щодо кіберстійкості, інтеграція стандартів ISO та NIST, розвиток моделей оцінювання процесів. Разом із тим кожен регіон має свої особливості, пов’язані з рівнем цифровізації, специфікою загроз та особливостями критичної інфраструктури.

Нормативно-правові вимоги України

В Україні проблема оцінювання зрілості систем кіберзахисту регулюється низкою законів, постанов і стандартів. Основою є законодавство, що визначає статус критичної інформаційної інфраструктури та вимоги до її захисту [21].

Основні нормативні документи України:

1. Закон України «Про основні засади забезпечення кібербезпеки України»

Регламентує загальні принципи побудови системи кіберзахисту, визначає об’єкти КІІ, встановлює вимоги щодо управління ризиками та забезпечення рівнів захисту.

2. Постанови Кабінету Міністрів України щодо ідентифікації та категоризації КІІ

Впроваджують критерії віднесення об’єктів до критичної інфраструктури, що є основою для формування вимог щодо кіберзахисту та оцінювання рівнів їхньої зрілості.

3. Нормативні документи Державної служби спеціального зв’язку та захисту інформації (ДССЗЗІ)

Встановлюють вимоги до аудиту інформаційної безпеки, проведення тестувань, сертифікації засобів захисту та впровадження стандартів ISO/IEC у державному секторі.

4.Національні стандарти (ДСТУ), гармонізовані з ISO/IEC 27000

Стандарти ДСТУ ISO/IEC 27001 та 27002 визначають політики, процеси й процедури забезпечення безпеки та містять інструментарій для оцінки їх зрілості.

Модель зрілості не прописана безпосередньо, однак рівні розвитку процесів можуть оцінюватися через механізми внутрішнього аудиту та аналізу ефективності заходів безпеки.

Нормативні вимоги України активно інтегруються з міжнародними фреймворками. Окрему увагу держава приділяє розвитку кіберстійкості, що відображено у стратегіях розвитку цифрової безпеки та нормативних документах щодо захисту КІІ.

Європейський Союз

ЄС має одну з найбільш розвинених нормативних систем у сфері кібербезпеки. Регулювання оцінювання зрілості систем базується на директивах, регламентах та уніфікованих європейських стандартах [22].

Ключові документи ЄС:

Директива NIS (Network and Information Security Directive)

Перша європейська директива у сфері кібербезпеки, яка визначила обов'язкові вимоги до операторів критично важливих послуг та цифрових сервісів. Зрілість процесів оцінюється через виконання вимог щодо управління ризиками, безперервності роботи та контролю безпеки .

Директива NIS2

Значно посилює вимоги попередньої директиви, вводячи чіткі критерії відповідності, підвищені вимоги до кіберстійкості та регулярних оцінок безпеки. Передбачає запровадження єдиної моделі оцінювання, яка включає рівні готовності та системності механізмів кіберзахисту.

Європейські стандарти ENISA (Агентства ЄС з кібербезпеки)

ENISA розробляє методології оцінювання зрілості кіберзахисту, у тому числі:

– моделі оцінювання для операторів важливих послуг;

– індикатори кіберстійкості;

– методики аудитів кібербезпеки.

Ці документи ґрунтуються на NIST CSF, ISO/IEC 27000 та ризик-орієнтованих практиках.

ISO/IEC 27000 та ISO/IEC 22301

ЄС активно впроваджує ці стандарти в національних законодавствах країн-членів. Вони забезпечують основу для оцінювання зрілості за рахунок вимог до процесів, політик, документування та моніторингу.

Європейський підхід характеризується високою системністю, формалізацією процедур та регулярними аудитами, що робить моделі оцінювання зрілості одним з ключових інструментів контролю якості кіберзахисту [23].

США мають найбільш розвинену систему стандартів у галузі кібербезпеки. Основну роль у визначенні вимог до оцінювання зрілості відіграють інституції NIST, Міністерство внутрішньої безпеки (DHS) та галузеві регулятори.

Основні документи та моделі США

NIST Cybersecurity Framework (CSF)

Встановлює функціональну модель управління кібербезпекою. Хоча NIST CSF не визначає рівнів зрілості як таких, у США активно використовуються додаткові профілі CSF, які дозволяють оцінювати ступінь відповідності вимогам фреймворку.

NIST SP 800-53

Один із найдетальніших стандартів кібербезпеки, який містить вимоги до контролів безпеки для державних органів і СІІ.

Зрілість оцінюється через ступінь впровадження контролів, їх ефективність та відповідність вимогам.

C2M2 (Cybersecurity Capability Maturity Model)

Розроблений у США, орієнтований на критичну інфраструктуру. Широко використовується у промисловості, енергетиці, транспорті та фінансовому секторі.

Містить три рівні зрілості й чіткі критерії для оцінки організаційної та технічної готовності.

FISMA (Federal Information Security Management Act)

Встановлює вимоги до кіберзахисту державних структур США та обов'язковість регулярних аудитів.

Містить індикатори оцінювання процесів, що фактично виконують роль рівнів зрілості.

MITRE ATT&CK та моделі зрілості інцидент-менеджменту

Використовуються для спеціалізованих оцінок, особливо в оборонній сфері та під час аналізу інцидентів.

Американський підхід вирізняється гнучкістю, широким спектром моделей та практичною спрямованістю, що дозволяє адаптувати вимоги до різних секторів критичної інфраструктури (рис. 1.3).

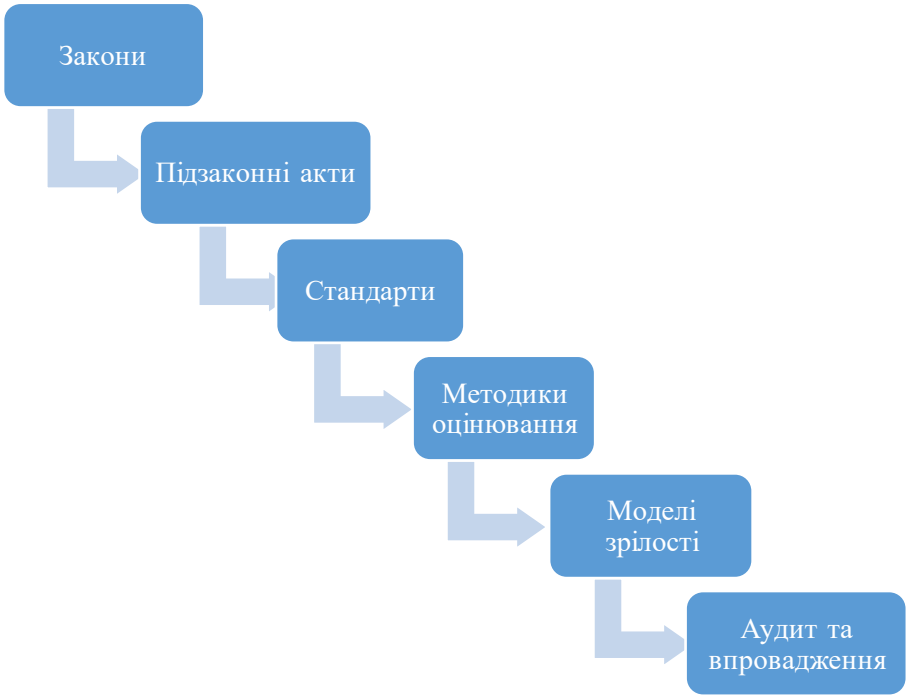

Рис.1.3 Структура нормативного забезпечення кіберзахисту

Попри різні регуляторні системи, можна виділити спільні риси:

–домінування ризик-орієнтованих методологій;

–інтеграція міжнародних стандартів ISO/IEC;

–вимоги щодо оцінювання життєвого циклу безпеки;

–акцент на кіберстійкості та безперервності роботи;

–регулярні аудити та тестування.

Водночас є й суттєві відмінності:

1.Україна зосереджується на гармонізації з європейськими вимогами.

2.ЄС робить акцент на міждержавній координації та стандартизації.

3.США використовують найбільш деталізовані моделі зрілості, орієнтовані на практичні інструменти та галузеву специфіку (табл. 1.5).

Таблиця 1.5

Порівняння нормативних вимог (Україна, ЄС, США)

Регіон	Основні документи	Фокус регулювання	Модель/метод оцінювання
Україна	Закон про кібербезпеку, ДСТУ, нормативи ДССЗЗІ	КІІ, аудит, стандарти	ISO/IEC, внутрішній аудит
ЄС	NIS, NIS2, ENISA, EN стандарти	Кіберстійкість, узгоджені вимоги	Моделі ENISA, профілі NIS2
США	NIST CSF, SP 800-53, C2M2, FISMA	Контролі, ризики, галузеві вимоги	C2M2, NIST maturity profiles

1.4. Проблеми й обмеження традиційних методів оцінювання зрілості

Традиційні методи оцінювання зрілості систем кіберзахисту тривалий час застосовувалися як основний інструмент аналізу рівня розвитку процесів, організації управління безпекою та ефективності впроваджених заходів. Вони ґрунтуються на стандартизованих підходах, регламентованих процедурах, опитувальниках, контрольних списках та аудитах, що дозволяє встановити базовий стан системи й визначити напрями подальшого вдосконалення. Проте розвиток сучасних кіберзагроз, ускладнення архітектури критичних інформаційних систем, динамічні зміни у технологічному середовищі та

зростання обсягів даних поставили під сумнів ефективність виключно традиційних підходів.

Незважаючи на важливість традиційних моделей зрілості, їхня обмеженість проявляється у низці аспектів: методологічних, технологічних, організаційних і практичних. Це створює бар'єри для адекватного оцінювання стану кіберзахисту, особливо в умовах, коли критична інфраструктура стає ціллю складних, багаторівневих і високотехнологічних атак [24].

1) Недостатня адаптивність до сучасних кіберзагроз

Однією з головних проблем є те, що традиційні методи оцінювання орієнтуються на статичні параметри. Більшість моделей передбачає оцінку стану процесів на певний момент часу, а не аналіз їх динаміки. У результаті:

– системи можуть отримати високий рівень зрілості навіть за умов низької готовності до нових типів атак;

– оцінка не враховує швидкість еволюції загроз;

– організація може формально відповідати стандартам, але не мати реальної кіберстійкості.

Сучасні APT-атаки, атаки на ланцюги постачання, застосування штучного інтелекту з боку зловмисників вимагають гнучкого, експресивного та автоматизованого оцінювання, чого традиційні методи забезпечити не можуть.

2) Залежність від суб'єктивного експертного оцінювання

Традиційні методи в значній мірі базуються на експертних інтерв'ю, ручному аналізі документів, опитувальниках та якісних оцінках. Це робить процес:

– суб'єктивним;

– залежним від компетентності конкретного аудитора;

– схильним до інтерпретацій;

– обмеженим у можливості відтворення результатів.

Навіть при використанні стандартизованих форм оцінювання різні аудитори можуть по-різному інтерпретувати однакові процеси. Це особливо критично для об'єктів КІІ, де важлива максимальна точність оцінки (табл. 1.6).

Таблиця 1.6

Основні обмеження традиційних методів оцінювання зрілості

Проблема	Прояв	Наслідки
Суб'єктивність	Оцінка залежить від аудитора	Неповторюваність результатів
Формалізм	Орієнтація на документацію	Нереалістична картина безпеки
Статичність	Фіксація стану на момент аудиту	Не враховує динаміку загроз
Відсутність автоматизації	Ручний аналіз	Висока трудомісткість
Обмежена масштабованість	Складність аудиту великих систем	Зниження ефективності

3) Орієнтація на формальну відповідність, а не на реальну ефективність

Більшість традиційних моделей оцінювання (ISO/IEC 27001, CMMI, SSE-CMM тощо) концентрується на:

– наявності документації;

– формалізації процедур;

– відповідності певним вимогам.

Однак наявність документів та політик не гарантує їх реального виконання і тим більше не свідчить про спроможність системи протистояти атакам. У багатьох випадках високий рівень зрілості є відображенням "паперової" відповідності, а не реальної практики.

4) Недостатня інтеграція з вимогами кіберстійкості

Сучасні стандарти НАТО, ЄС та США дедалі більше акцентують увагу не лише на кіберзахисті, а на кіберстійкості – здатності системи:

– протистояти атакам,

– функціонувати в умовах інциденту,

– швидко відновлюватися,

– забезпечувати безперервність критичних процесів.

Традиційні методи зрілості орієнтуються переважно на оцінку процесів управління безпекою, а не на реальну стійкість до збоїв. Це призводить до того, що організації можуть недооцінювати ризики, пов’язані з відмовами, кібератаками або кризовими ситуаціями.

5. Обмежена масштабованість та трудомісткість

Процес традиційного оцінювання зрілості:

– потребує значних людських ресурсів;

– займає багато часу;

– залежить від доступності інформації;

– важко масштабувати на великі організації.

Особливо це стосується організацій з розгалуженою інфраструктурою або з великою кількістю автономних підрозділів. Регулярне проведення аудиту стає надто дорогим та повільним, що знижує оперативність отримання результатів.

6. Відсутність автоматизації та аналітичних механізмів

Більшість традиційних методів не передбачає:

– аналізу великих масивів даних;

– автоматизованої обробки логів, подій чи телеметрії;

– використання моделей машинного навчання.

У результаті організації не використовують потенціал даних, які вже накопичуються у SIEM, SOC, IDS/IPS та інших системах.

Це знижує точність оцінювання та обмежує можливість прогнозування слабких місць.

7. Низька чутливість до поведінкових та аномальних показників

Традиційні моделі оцінки орієнтовані на процеси, а не на реальні події. Вони майже не враховують:

– аномальні патерни поведінки;

– тренди інцидентів;

– індикатори компрометації;

– фактичну продуктивність SOC.

Таким чином, вони не враховують реальний контекст і динаміку атак, а зосереджуються на статичних аспектах.

8. Відсутність інтеграції з сучасними DevSecOps-підходами

Традиційні моделі оцінювання були розроблені для класичних IT-середовищ, де процеси змінюються повільно.

У сучасних умовах DevOps, контейнеризації, мікросервісів та CI/CD це стає недоліком, оскільки:

– зміни відбуваються швидко;

– потребуються постійні оцінки у режимі near-real-time;

– безпека інтегрується в agile-процеси.

Традиційні оцінювання не встигають за темпом змін і не можуть адекватно відображати реальну картину [25].

9. Недостатня врахованість людського фактора

Організаційні проблеми є однією з головних причин інцидентів, проте традиційні підходи мало враховують:

–поведінку персоналу;

–культуру безпеки;

–компетентність співробітників;

– рівень підготовки до інцидентів.

У результаті рівень зрілості може бути формально високим, а реальна безпека – низькою.

10. Обмеження у порівнянні результатів між організаціями

Традиційні методи часто використовують різні підходи, шкали, інтерпретації. Це ускладнює:

–порівняння різних організацій;

–оцінку динаміки на національному рівні;

– аналіз стану КІІ у певному секторі.

Відсутність уніфікації призводить до фрагментації практик оцінювання. (рис. 1.4)

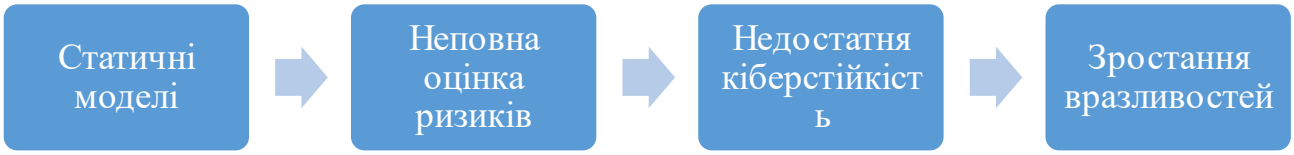

Рис. 1.4 Причинно-наслідковий зв’язок обмежень традиційних методів

Висновки до розділу 1

Розглянуто теоретичні та методологічні засади оцінювання зрілості систем кіберзахисту об’єктів критичної інформаційної інфраструктури, що дозволило сформувати комплексне уявлення про сутність, структуру та проблематику цього процесу. Аналіз продемонстрував, що системи кіберзахисту відіграють ключову роль у забезпеченні стійкого функціонування критичних секторів держави, а їхня зрілість є інтегральною характеристикою, що відображає ефективність, узгодженість та результативність заходів безпеки.

З’ясовано, що системи кіберзахисту КІІ являють собою багаторівневі та комплексні механізми, спрямовані на запобігання, виявлення, реагування і відновлення після кіберінцидентів. Їх значення визначається не лише технічними аспектами, а й організаційною культурою безпеки, нормативним регулюванням, готовністю до надзвичайних ситуацій та здатністю підтримувати безперервність критичних процесів.

Проаналізовано ключові підходи та моделі оцінювання зрілості, зокрема CMMI, C2M2, NIST CSF та інші. З’ясовано, що ці моделі забезпечують системний спосіб оцінювання рівня розвитку процесів безпеки, дозволяють стандартизувати вимоги та визначити дорожню карту підвищення зрілості. Одночасно було встановлено, що моделі значно різняться за структурою,

логікою, пріоритетами та глибиною охоплення циклу управління кіберризиками, а їх застосування потребує адаптації до специфіки критичної інфраструктури.

У підпункті 1.3 досліджено нормативно-правові та стандартні вимоги України, ЄС і США, що формують рамкові умови для здійснення оцінювання зрілості. Було показано, що українське законодавство поступово гармонізується з європейськими вимогами та міжнародними стандартами, зокрема у контексті NIS2, ISO/IEC 27001 і рамкових документів NIST. Це створює передумови для запровадження уніфікованих підходів до оцінювання зрілості систем кіберзахисту, розширює інструментарій для секторального аналізу та підвищує прозорість механізмів управління кібербезпекою.

Визначено обмеження та проблеми традиційних методів оцінювання зрілості. Серед ключових недоліків виокремлено статичність моделей, відсутність автоматизованої аналітики, залежність від експертних оцінок, орієнтацію на формальну відповідність документації, низьку інтеграцію з сучасними технологічними процесами (зокрема DevSecOps) та недостатнє урахування поведінкових показників і реальної динаміки загроз. Це створює розрив між формальним рівнем зрілості та фактичною здатністю системи протистояти розвиненим кібератакам.

Отже, проведений аналіз підтверджує, що хоча існуючі моделі та стандарти забезпечують необхідну базу для оцінювання зрілості систем кіберзахисту, їх ефективність у сучасних умовах значною мірою обмежена. Зростання складності кіберзагроз, масштабування інфраструктур, цифрова трансформація та розвиток штучного інтелекту вимагають створення нових, більш адаптивних, динамічних і автоматизованих методик оцінювання. Саме тому подальші дослідження у наступних розділах будуть спрямовані на розробку методичного підходу до оцінювання зрілості систем кіберзахисту із застосуванням технологій штучного інтелекту, що дозволить підвищити точність, об’єктивність і оперативність аналізу.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОЦІНЮВАННІ ТА УПРАВЛІННІ КІБЕРЗАХИСТОМ

2.1. Використання машинного навчання та AI у системах інформаційної безпеки

Еволюція застосування штучного інтелекту та машинного навчання в кіберзахисті стала наслідком технічних обмежень традиційних підходів та стрімкого зростання обсягів даних, які генерують сучасні інформаційні системи. Початкові засоби захисту базувалися на сигнатурному аналізі, що передбачав співставлення подій із наперед визначеними шаблонами відомих атак. Такий механізм був ефективним на ранніх етапах розвитку кіберзагроз, однак втратив актуальність у середовищі, де домінують модифіковані, поліморфні та zero-day атаки. Сигнатурні засоби не здатні реагувати на невідомі поведінкові вектори, що робить їх непридатними для своєчасного виявлення сучасних інцидентів, а також створює значну кількість хибних спрацювань через обмеженість контексту.

Паралельно з ускладненням кіберзагроз відбувалося стрімке зростання кількості подій, які мають бути оброблені системами безпеки. Логування мережевого трафіку, події автентифікації, телеметрія кінцевих пристроїв, журнали міжмережевих екранів, сигнали IDS/IPS і потоки загрозової розвідки сформували дані такого масштабу, що традиційний аналіз став технічно неможливим. У центрів безпеки з'явилася потреба не лише в централізованому збиранні подій, але й у здатності аналізувати їх у реальному часі, зменшувати хибні спрацювання, виявляти невідомі типи атак та автоматизувати реагування [26].

Відповіддю на ці потреби став перехід до поведінкових моделей, у яких вирішальну роль відіграють алгоритми машинного навчання. На відміну від сигнатурних методів, поведінкові моделі аналізують зміни у звичайних

шаблонах діяльності користувачів і систем. У результаті стає можливим виявлення неочевидних відхилень, які не можуть бути описані фіксованими правилами. Використання як контрольованих, так і неконтрольованих методів машинного навчання дозволило формувати профілі нормальної поведінки та виявляти аномалії навіть у разі відсутності міток класів або історичних прикладів конкретних атак. Значну роль у цьому відіграли алгоритми кластеризації, дерев рішень, аналізу часових послідовностей та глибокого навчання, здатні працювати з нерегулярними, неструктурованими та неоднорідними даними.

Цей технологічний зсув збігся з появою інтегрованих платформ SIEM, SOAR та XDR, які почали включати ML у свої аналітичні ядра. SIEM-системи, які раніше виконували переважно збір і кореляцію подій, отримали можливість застосовувати машинне навчання для виявлення аномалій, ранжування сигналів та скорочення кількості хибних оповіщень. SOAR, у свою чергу, інтегрував AI/ML для автоматизації реагування – від класифікації інцидентів до запуску узгоджених сценаріїв ізоляції чи блокування. XDR об'єднав телеметрію мережі, кінцевих пристроїв та хмарних ресурсів у єдине середовище, де ML аналізує корельовані дані з різних шарів інфраструктури для виявлення атак, які залишаються непомітними в окремих сегментах.

Проблематика великих даних, обмеження традиційних систем і недоліки ручного аналізу спричинили формування багаторівневих архітектур, у яких машинне навчання працює у зв'язці зі стандартними механізмами кореляції, правилами та статистичним аналізом. Це дозволило значно підвищити точність виявлення, зменшити навантаження на аналітиків і підвищити швидкість прийняття рішень. Водночас еволюція ML у кіберзахисті позначила і нові виклики: залежність від великих датасетів, чутливість моделей до якості даних, потребу в мінімізації хибних прогнозів та необхідність інтерпретації рішень моделей, що призвело до розвитку Explainable AI у сфері безпеки [27].

Основні задачі, які вирішуються за допомогою AI, пов'язані з автоматизованим аналізом телеметрії, зменшенням навантаження на аналітиків та підвищенням оперативності реагування на інциденти.

Однією з базових задач AI є автоматизоване виявлення аномалій у реальному часі. Машинне навчання дозволяє формувати динамічні профілі нормальної поведінки користувачів, пристроїв і сервісів на основі історичних даних та безперервних потоків подій. На відміну від статичних правил, ці профілі адаптуються до змін середовища та дозволяють фіксувати відхилення, які не мають заздалегідь визначених сигнатур.

Наступною ключовою задачею є класифікація та пріоритизація інцидентів, відома як alert triage. Надмірна кількість сповіщень є однією з головних проблем сучасних систем безпеки. AI використовується для аналізу контексту подій, кореляції індикаторів та групування пов'язаних сигналів у логічні інциденти. За рахунок цього зменшується ефект alert fatigue, а аналітики отримують вже агреговану інформацію з попередньою оцінкою критичності. Машинне навчання застосовується для ранжування інцидентів за потенційним впливом, що дозволяє першочергово реагувати на події з високим ризиком, не витрачаючи ресурси на низькопріоритетний шум.

Окрему роль AI відіграє у виявленні zero-day загроз через поведінкове моделювання. Оскільки такі атаки не мають відомих сигнатур і часто використовують легітимні механізми системи, їх виявлення можливе лише через аналіз непрямих ознак і атипових ланцюгів дій. Поведінкові моделі дозволяють виявляти приховані фази атак, зокрема розвідку, латеральне переміщення та поступову ескалацію привілеїв. Такий підхід є ключовим для протидії APT-кампаніям і довготривалим атакам, які навмисно маскуються під нормальну активність [28].

Завершальною, але не менш важливою задачею є автоматизація реагування на інциденти. AI ініціює стандартизовані дії у відповідь на підтверджені або високоймовірні загрози. Йдеться про автоматичне блокування підозрілих IP-адрес, ізоляцію скомпрометованих вузлів, обмеження доступу або деактивацію облікових записів із аномальною поведінкою. Такі дії виконуються відповідно до наперед визначених сценаріїв і дозволяють мінімізувати час між виявленням та стримуванням загрози. Автоматизація є ефективною насамперед для типових

і повторюваних інцидентів, натомість, складні випадки потребують участі фахівця.

У практиці інформаційної безпеки вибір ML-моделі визначається не «модністю» алгоритму, а типом даних, вимогами до пояснюваності та часовими обмеженнями детекції. Дані кіберзахисту надходять як потоки необроблених подій (мережевий трафік, системні логи, поведінка користувачів), що спочатку проходять нормалізацію, очищення, інтеграцію та редукцію ознак, після чого розділяються на розмічені й нерозмічені підмножини. Розмічені дані потрібні для стабільної побудови правил класифікації й пріоритизації реагування, однак їх якість ускладнюється підтримкою актуальності, збиранням релевантних прикладів і ризиком упередженості; нерозмічені дані є критичними для пошуку загроз та виявлення відхилень, де структура даних не описана наперед і виявляється алгоритмічно через виявлення патернів. У цьому конвеєрі результатом роботи моделей стають не лише мітки, а й агреговані вагові оцінки для звітів і панелей моніторингу, що зводять технічні характеристики подій до керованих сигналів для операційної команди [29].

Для контрольованого навчання у кіберзахисті домінують класифікатори, які добре працюють із високорозмірними ознаками та потребують контрольованої якості розмічених даних. Типовими є Support Vector Machine (SVM), Logistic Regression, Decision Tree/Random Forest, Naive Bayes, k-NN, а також ensemble-підходи, які знижують ризик перенавчання через усереднення рішень. У прикладних задачах [30] виявлення загроз такі моделі оцінюють за precision/recall/F1 score і придатністю до шумних даних: ансамблеві методи на кшталт Random Forest та Extra Trees демонструють найвищі значення точності серед розглянутих базових підходів, але при цьому підкреслюється залежність результатів від властивостей конкретного датасету та обчислювальні витрати при масштабуванні.

Неконтрольоване навчання застосовується там, де класи атак невідомі або розмітка неповна, а задача формулюється як пошук відхилень від нормальної поведінки. Кластеризація (зокрема k-means), ієрархічні методи та інші підходи

до структуризації без міток використовуються для виділення груп схожих подій і подальшого маркування нетипових кластерів як підозрілих. У контексті кіберзахисту саме нерозмічена телеметрія (дані IoT-сенсорів, поведінка користувачів, логи, мережеві записи) є базою для таких методів, оскільки дозволяє знаходити приховані патерни, які не покриваються сигнатурами чи правилами [31].

Глибоке навчання застосовують тоді, коли дані мають складну структуру або часову залежність, яку важко описати вручну створеними ознаками. Для аналізу послідовностей подій або трафіку релевантними є рекурентні архітектури (RNN/LSTM), а для виділення локальних шаблонів у представленнях трафіку чи інших картах ознак використовують CNN-підходи.

Навчання з підкріпленням фігурує як окремий клас ML-підходів, що концептуально узгоджується з потребою оптимізувати послідовність дій у реагуванні. Зокрема, технологічні набори SOC інтегрують ML-аналітику в SIEM, SOAR, XDR та UEBA для детекції майже в реальному часі, кореляції подій із різних джерел (кінцеві пристрої, мережа, логи серверів/міжмережевих екранів), пріоритизації інцидентів і зниження хибних спрацювань шляхом контекстної кореляції та поведінкової аналітики. Механізми на основі сигнатур не здатні надійно виявляти zero-day атаки, тоді як вбудована в ML поведінкова аналітика орієнтується на виявлення незвичних шаблонів та невідомих атак, хоча конкретні типи алгоритмів, вбудованих у продукти, постачальники часто не деталізують у відкритих матеріалах [32].

Показовим прикладом прикладної supervised-класифікації є автоматизація обробки звітів про інциденти у вигляді тікетів: текстові описи інцидентів перетворюються на ознаки через TF-IDF, після чого алгоритми на кшталт SVM, k-NN, Naive Bayes і Decision Trees виконують автоматичне віднесення звернень до класів таксономії та прискорюють узгодженість наступних кроків реагування. Це підсилює загальну логіку застосування моделей у SOC-процесах: від потоку подій і первинної нормалізації до класифікації, ранжування та формування

сигналів для реагування, де ефективність визначається балансом між точністю, затримкою та стійкістю до зміни профілю загроз.

Застосування ML/DL у кіберзахисті підсилює автоматизацію аналізу подій та виявлення відхилень, однак водночас створює проблему «чорної скриньки»: навіть розробники можуть не мати повного уявлення, як саме модель сформувала конкретний висновок після навчання на даних, особливо коли йдеться про складні моделі з великою кількістю параметрів. Така непрозорість небезпечна тим, що приховує дефекти (упередженість, неточності), ускладнює аудит і може провокувати як хибну довіру, так і надмірну залежність від автоматизованих рішень, що є критичним у середовищі реагування на інциденти [33].

Explainable Artificial Intelligence (XAI) спрямована на те, щоб перетворити результат роботи моделі на пояснюваний для людини артефакт, який дає відповідь не лише «що сталося», а й «чому система дійшла саме такого висновку». У цьому контексті розрізняються три близькі, але різні властивості: «прозорість» як можливість осягнути модель (на рівні всієї моделі, компонентів або алгоритму навчання), інтерпретованість як ступінь зрозумілості отриманого рішення людиною, та пояснюваність як здатність надати зрозуміле обґрунтування конкретного прогнозу/класифікації.

У SOC-контексті вимога інтерпретованості безпосередньо пов'язана з керованістю процесу triage та обґрунтуванням пріоритизації: коли модель пропонує класифікацію інциденту або аномалії, аналітик має швидко оцінити підстави рішення, зрозуміти межі застосовності та визначити, чи потрібна ескалація. Додатково, проблема хибних спрацювань у виявленні загроз призводить до перевантаження потоком алертів і втрати довіри до автоматизованих рекомендацій, тому пояснення, які атрибутують внесок ознак або показують логіку класифікації, стають практичним механізмом контролю якості детекції й зменшення операційних втрат.

Підходи XAI узагальнено поділяються на самоінтерпретовані («white box») моделі та постфактум пояснення для «black box» моделей. Самоінтерпретований підхід закладає інтерпретованість у саму конструкцію моделі: алгоритм і

перетворення ознак у результат є відносно прямими для пояснення. Натомість для складних архітектур, зокрема глибокого навчання, очікувати повної самопояснюваності нераціонально, оскільки навіть візуалізація внутрішніх представлень може бути не менш складною за саму модель; тому для таких систем типовим стає постфактум підхід, де пояснення генеруються після отримання рішення [34].

Постфактум пояснення, у свою чергу, поділяються на глобальні та локальні. Глобальні дають узагальнене розуміння поведінки моделі (наприклад, через важливість ознак або вилучення правил), тоді як локальні пояснюють конкретний випадок спрацювання – саме цей формат найбільш придатний для операційного аналізу аномалії або алерта, де важлива причина рішення для цього конкретного випадку. Два поширені локальні модельно-незалежні методи – LIME та SHAP. LIME формує серію контрольованих модифікацій вхідних даних, спостерігає зміну виходу моделі та на цій основі будує просту змінну модель, яка локально апроксимує поведінку «black box» і показує, які ознаки вплинули на результат. SHAP базується на ідеї Shapley values з теорії кооперативних ігор: для конкретного прогнозу він обчислює внесок кожної ознаки з урахуванням можливих комбінацій ознак, надаючи уніфіковану оцінку локальної важливості; у розширених оглядах XAI цей підхід віднесено до класу методів визначення релевантності ознак, де оцінюється внесок/важливість ознак для конкретного прогнозу та підкреслюються властивості на кшталт локальної точності, пропущеності й узгодженості.

Концептуально взаємодію XAI в операційному циклі можна описати як послідовність: потоки подій/телеметрії формують вхідні ознаки, модель детекції генерує оцінку/клас (алерт), далі XAI-шар будує пояснення у вигляді внесків ознак або локальної апроксимації, після чого аналітик виконує валідацію та приймає рішення щодо реагування [35]. Критично, XAI не усуває ризики автоматизації сама по собі: пояснення можуть бути надто складними або, навпаки, спрощеними до втрати змісту, що веде до хибної інтерпретації; окремо відзначається ризик надмірної довіри (упередженості автоматизації), коли

наявність пояснення підвищує ймовірність сліпого прийняття рекомендації без належної перевірки. Тому інтерпретація пояснень має залишатися частиною контрольованого процесу з людським наглядом, де пояснення використовується як інструмент аудиту й обґрунтування, а не як заміна експертного рішення.

2.2. Методи AI для оцінювання ризиків, виявлення аномалій та прогнозування рівня безпеки

Методологія застосування AI для оцінювання рівня кібербезпеки ґрунтується на формалізації безпекового стану як динамічного процесу, що розвивається в часі під впливом множини спостережуваних факторів. На відміну від класичних підходів, де ризик визначається як статичне співвідношення загроз і вразливостей, AI-орієнтовані методи розглядають ризик як змінну величину, що безперервно оновлюється на основі потоку подій. Центральним елементом цього підходу є перехід від дискретного аналізу окремих інцидентів до безперервного оцінювання стану системи з використанням числових індикаторів.

Оцінювання ризику в AI-контурі починається з побудови вхідного простору ознак, які відображають поведінкові характеристики системи. Ці ознаки формуються як агреговані показники активності у визначених часових вікнах і можуть включати інтенсивність подій, варіативність дій, повторюваність однакових шаблонів, часову концентрацію відхилень та їх взаємозв’язок. Методологічно важливо, що оцінка ризику не базується на семантичній інтерпретації кожної події, а на числовому аналізі структури потоку.

Подальший етап полягає у трансформації векторів ознак у ризикову оцінку. У supervised-підходах це реалізується як функція класифікації або регресії, де вихід моделі інтерпретується як імовірність небезпечного стану або значення ризикового індексу. У unsupervised- і semi-supervised-підходах ризик обчислюється як функція відстані або ймовірності належності спостереження до області нормальної поведінки. В обох випадках ключовою методологічною

ідеєю є відмова від бінарних рішень на користь безперервної шкали, яка дозволяє порівнювати різні стани системи між собою [36].

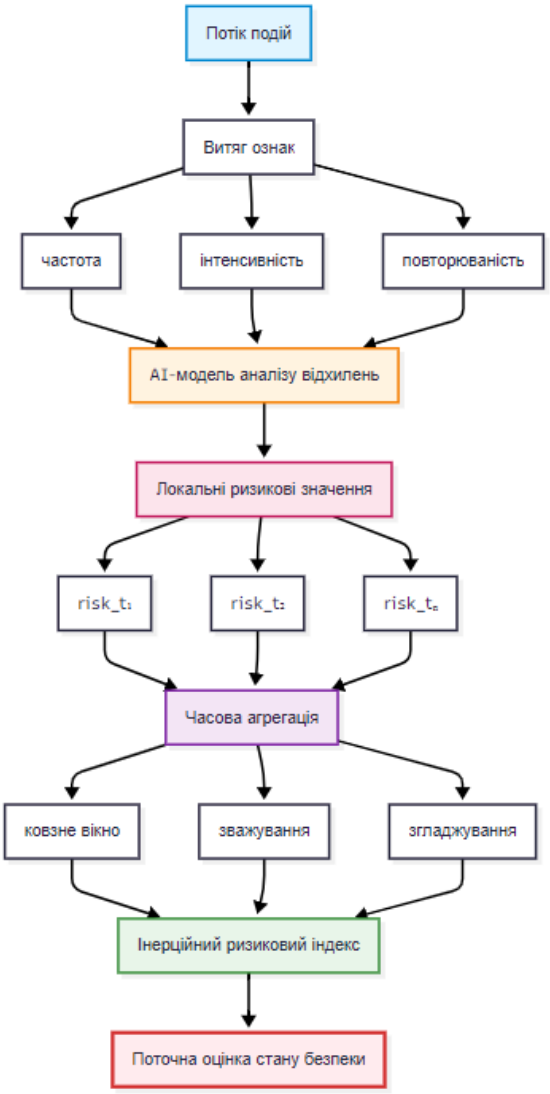

Рис. 2.1. Схема інерційного формування ризикової оцінки на основі AI-аналізу подій

Для забезпечення стійкості оцінювання використовуються методи часової агрегації ризикових значень. Окремі оцінки, отримані на коротких інтервалах, піддаються згладжуванню або накопиченню, що дозволяє відокремити випадкові коливання від систематичних змін. Методологічно це реалізується через ковзні вікна, експоненційне згладжування або зважені суми, де більш нові спостереження мають більший вплив на поточний стан. Такий підхід забезпечує

інерційність ризикової оцінки, що є необхідною умовою для уникнення реакції на шум.

Виявлення аномалій у цьому контурі виконує функцію генерації первинних сигналів, з яких формується ризик. Аномалія визначається не як факт порушення, а як кількісна характеристика нетиповості поведінки. Методологічно це означає, що кожному спостереженню відповідає числовий показник аномальності, який відображає ступінь його відхилення від очікуваного профілю. Цей показник не має самостійного управлінського значення, але слугує базовою змінною для подальших обчислень [37].

Ключовим методичним аспектом є розрізнення між локальною аномальністю та стійкою аномальною поведінкою. Локальна аномалія характеризується короткочасним відхиленням, яке не змінює загальний профіль системи. Стійка аномалія проявляється через послідовність відхилень, які в сукупності формують нову поведінкову траєкторію. Методи AI дозволяють ідентифікувати обидва типи, але методологія оцінювання ризику орієнтована саме на другий випадок, оскільки він відображає накопичувальний характер загрози.

Таблиця 2.1

Порівняння локальної та стійкої аномальної поведінки в контексті оцінювання ризику

Критерій порівняння	**Локальна аномалія**	**Стійка аномальна поведінка**
Тривалість	Короткочасна	Тривала або повторювана
Частота появи	Поодинокі події	Серія подій
Вплив на профіль поведінки	Не змінює	Формує нову траєкторію
Характер відхилення	Імпульсний	Кумулятивний
Роль в оцінюванні ризику	Мінімальна	Ключова
Необхідність реагування	Низька	Висока
Ймовірність шуму	Висока	Низька

Для цього використовується аналіз часових рядів показників аномальності. Кожна нова оцінка порівнюється не лише з порогом, а з історією попередніх значень. Якщо аномальність має тенденцію до зростання або зберігається на

підвищеному рівні протягом тривалого періоду, методологія інтерпретує це як сигнал деградації безпекового стану.

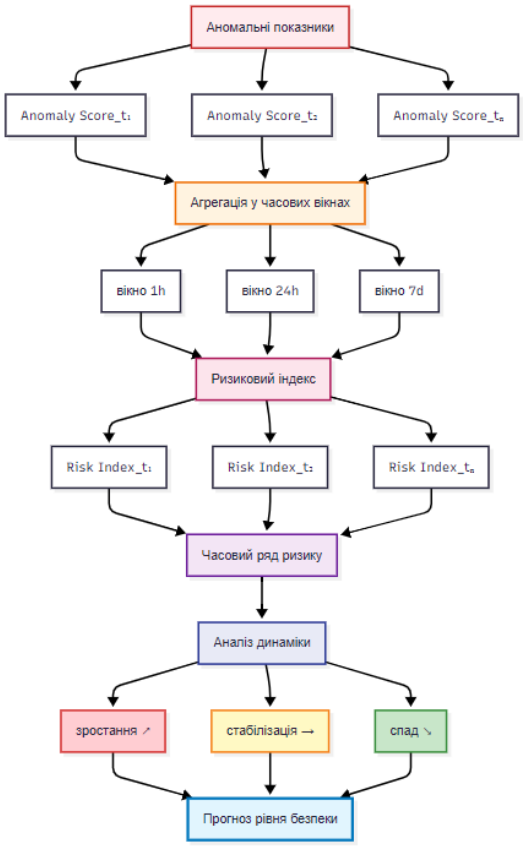

Рис. 2.2. Методологічний ланцюг від аномалій до прогнозування рівня безпеки

Прогнозування рівня безпеки реалізується як аналіз і екстраполяція динаміки ризикових індексів. Методологічно прогноз не спрямований на передбачення конкретних інцидентів, а на оцінку майбутнього стану системи в цілому. Для цього використовуються часові моделі, які аналізують тренди, темпи змін і циклічні компоненти ризикових показників. Вихід прогнозної моделі інтерпретується як очікуваний рівень ризику у заданому часовому горизонті.

Важливим аспектом прогнозування є врахування швидкості зміни ризику. Навіть за відносно низького поточного значення ризику, швидке зростання індексу може вказувати на наближення критичного стану. Методологія AI дозволяє виявляти такі ситуації шляхом аналізу похідних або різниць часових

рядів ризикових оцінок. Це забезпечує випереджальний характер аналізу та дозволяє реагувати до настання явної деградації безпеки [38].

Окрему роль відіграє узгодження часових масштабів аналізу. Короткострокові моделі фіксують швидкі зміни, тоді як довгострокові відображають загальні тенденції. Методологічно ці масштаби поєднуються шляхом багаторівневого аналізу, де результати короткострокового прогнозування використовуються для уточнення довгострокових оцінок. Це дозволяє уникнути ситуацій, коли короткочасні сплески маскують повільну деградацію або, навпаки, довгострокова стабільність приховує раптову ескалацію.

Таблиця 2.2

Роль AI-методів у контурі оцінювання безпеки

Рівень аналізу	**Роль AI**	**Результат**
Подієвий	Виявлення відхилень	Anomaly score
Оціночний	Агрегація та інерція	Risk index
Прогностичний	Аналіз трендів	Forecasted security level

2.3. Порівняння ефективності класичних і AI-орієнтованих методів оцінювання зрілості

Оцінювання зрілості кіберзахисту виступає прикладним механізмом управління, який переводить різнорідні ознаки організаційної та технічної спроможності в узгоджений профіль, придатний для планування змін і контролю прогресу. У цій постановці зрілість не зводиться до наявності окремих засобів або формальних документів, а відображає керованість циклу захисту, відтворюваність контрольних процедур і здатність системи безпеки підтримувати стабільний рівень результативності за умов змін у середовищі. Саме тому в практиці оцінювання зрілості часто співвідноситься з рамковими

підходами, де спроможності структуруються функціонально, а результат подається як профіль реалізованості та керованості практик [39].

Класичні методи оцінювання зрілості зазвичай побудовані навколо дискретних рівнів і якісних описів практик, що належать кожному рівню. Операційна логіка полягає у співвіднесенні «як організація працює» з «як має бути організовано» відповідно до моделі: збирається доказова база, аналізуються політики й процедури, проводяться інтерв'ю, після чого виконуються експертне узгодження та інтерпретація відповідності критеріям. Поширеність дискретних рівнів пояснюється їхньою управлінською зручністю: вони стискають складну картину стану у невелику кількість градацій, придатних для комунікації та постановки цілей. Узагальнення maturity models у суміжних доменах цифрової трансформації демонструє, що п'ятирівневі шкали домінують як компроміс між деталізацією та керованою складністю, але паралельно зустрічаються чотири- і трирівневі схеми, шестирівневі варіанти, а також підходи без фіксованих рівнів або з розширеною кількістю ступенів, що впливає на точність розрізнення станів і на трудомісткість оцінки.

Ефективність класичних методів у кібербезпеці насамперед проявляється у відтворюваності процедури та нормативній прозорості результату. Дискретний рівень легко інтерпретується керівництвом і дозволяє формувати дорожні карти підвищення зрілості через gap-аналіз, не вимагаючи складної інфраструктури даних. Крім того, класичні підходи підтримують довіру до висновків через орієнтацію на перевірювані артефакти: політики, регламенти, протоколи виконання контрольних дій, результати перевірок, звітність. У середовищах, де домінує відповідність стандартам і регуляторним очікуванням, така орієнтація є критичною, оскільки оцінювання стає не лише внутрішнім інструментом керування, а й способом доведення виконання вимог. Разом із цим класичні методики тяжіють до статичності: вони фіксують стан на момент оцінювання та слабо відображають оперативні зміни в ефективності контролів між циклами перевірок. Ускладнюється й обробка великої кількості операційних сигналів,

оскільки ручне оцінювання природно спирається на обмежений обсяг доказів і на узагальнену експертну інтерпретацію [40].

AI-орієнтовані методи оцінювання зрілості формують іншу методичну основу, фокусуючись на кількісності, відтворюваності та чутливості до поточного стану. У загальному вигляді AI розглядається як набір predictive та automated інструментів, здатних обробляти великі масиви даних у реальному часі, підвищуючи agility, accuracy і швидкість управлінських рішень порівняно з підходами, що покладаються на статичний аналіз та історичні записи. Для оцінювання зрілості це означає перехід від домінування перевірки «наявності практик» до обчислення індикаторів, які відображають «фактичну роботу практик» на підставі даних. Методологічно такий підхід потребує формалізованих доменів оцінки й набору кількісних показників, що живлять домени, а також правил агрегування, які перетворюють індикатори на зрозумілий управлінський результат.

Показовою ілюстрацією індикаторної логіки є підхід типу AI Maturity Matrix, де оцінювання організовано як поєднання двох осей: вплив порушень, спричинених AI та готовність використовувати потенціал AI й пом'якшувати ризики. Методична цінність такої побудови полягає в тому, що готовність розкладається на кілька вимірів, які наповнюються конкретними індикаторами з вагами, а різнорідні дані приводяться до спільної шкали за рахунок нормалізації. Додатково важливим є те, що оцінювання може комбінувати різні типи джерел і допускати розбіжності між ними, оскільки різні сигнали (наприклад, ринкові, інституційні, поведінкові) можуть реагувати на зміни з різною затримкою [41].

Інший клас AI-орієнтованих методів демонструє підхід на кшталт AIMAA (AI Maturity Assessment and Alignment), де оцінювання оформлюється як структурована самооцінка із числовими градаціями 0–5 та система оцінювання. Методична відмінність такого підходу полягає в навмисному переході від суто описових стадій застосування кількісної системи оцінювання, що забезпечує можливість track progress, будувати порівняння між організаціями та формувати цільові плани дій. У межах AIMAA наголошується також на потребі управління

та зменшення ризиків як елементах, що впливають на придатність AI до застосування й на довіру до рекомендацій. Додатковою методичною вимогою є орієнтація на вхідні дані на основі даних і необхідність підтримувати актуальність оцінювання через моніторинг після розгортання, зокрема в контексті змін середовища та потреби коригувати підхід до моделей.

У кібербезпеці аналогічна механіка означає, що оцінювання зрілості може базуватися на поєднанні організаційних артефактів (політик, процедур, регламентів) з операційними сигналами (журнали подій, телеметрія, результати контролів), а підсумковий профіль формується через агрегування індикаторів за доменами. Технічна передумова для такої логіки пов'язана з наявністю інфраструктури збору та кореляції даних і компонентів звітності, оскільки саме звітування/метрики дозволяють формувати KPIs, відстежувати ефективність процесів моніторингу та реагування, а також підтримувати управлінську звітність. У такому випадку AI-орієнтована зрілість перестає бути «разовим зрізом» і наближається до динамічного профілю, який оновлюється разом із даними, що надходять, і відображає фактичні зміни в результативності контролів [42].

Таблиця 2.3

Порівняння ефективності класичних і AI-орієнтованих методів оцінювання зрілості кіберзахисту

Критерій порівняння	**Класичні методи оцінювання зрілості**	**AI-орієнтовані методи оцінювання зрілості**
Об'єкт вимірювання	Наявність і керованість практик, відповідність критеріям моделі	Фактична результативність і динаміка стану через індикатори, що обчислюються з даних
Тип даних	Переважно якісні докази: документи, процедури, інтерв'ю, результати аудитів	Переважно кількісні сигнали: індикатори з подій/телеметрії + структуровані управлінські артефакти
Принцип оцінювання	Експертне співвіднесення доказів із рівнями/критеріями	Нормалізація показників, індикаторний підхід, вагове агрегування в інтегральний скор

Критерій порівняння	Класичні методи оцінювання зрілості	AI-орієнтовані методи оцінювання зрілості
Форма результату	Дискретний рівень і/або профіль за доменами	Числовий скор + профіль за вимірами з можливістю частого оновлення
Частота оновлення	Періодична (аудитний цикл), залежить від ресурсу оцінювання	Потенційно частіша, залежить від надходження даних і підтримки моделі/індикаторів
Чутливість до змін	Нижча: зміни між циклами можуть бути непомітні	Вища: зміни відображаються через динаміку індикаторів і скорингу
Інтерпретованість результату	Висока: рівні зрозумілі управлінськи, легко комунікуються	Залежить від прозорості скорингу; потребує пояснюваності та опису індикаторів/ваг
Трудомісткість	Висока в частині збору доказів і експертного узгодження	Висока в частині побудови конвеєра даних, налаштування індикаторів, супроводу моделей
Залежність від якості даних	Помірна: основний ризик – неповні/неактуальні документи	Висока: некоректні/неповні дані або дрейф призводять до хибного скорингу
Стійкість до “шуму” в подіях	Обмежено релевантно, бо оцінка не подієва	Критично: потрібні методи агрегації/фільтрації, інакше росте ризик хибних сигналів
Порівнюваність між організаціями	Добра за умови спільної моделі/критеріїв	Можлива, але потребує однакових індикаторів, нормалізації й правил агрегування
Основні ризики	Суб’єктивність, статичність, «зрізовість», затримка відносно реального стану	Непрозорість скору, помилки через дані, витрати впровадження, потреба governance
Найкращий сценарій застосування	Формальна оцінка відповідності, аудит, планування змін	Безперервний моніторинг зрілості, раннє виявлення деградації, швидка корекція
Практичний компроміс	-	Гібрид: класична модель як каркас + AI-індикатори як вимірювальний шар

Порівняння ефективності класичних і AI-орієнтованих методів потребує різних критеріїв. Для класичних методик центральними є стандартизація процедури, інтерпретованість шкали та порівнюваність результатів між підрозділами або організаціями. Такі методики особливо сильні, коли управлінським пріоритетом є відповідність рамкам і здатність формально довести наявність та керованість практик. Водночас їхня точність обмежується

дискретністю: близькі, але не ідентичні профілі можуть потрапити до одного рівня, а зміни між циклами оцінювання можуть залишатися непоміченими. Збільшення кількості рівнів або перехід до більш деталізованих шкал потенційно підвищує точність, але підсилює складність інтерпретації та трудомісткість збору доказів, що знижує практичну застосовність.

Для AI-орієнтованих методів критеріями ефективності стають актуальність, відтворюваність скорингу, чутливість до змін і можливість підтримувати безперервне вимірювання. Їхня сильна сторона полягає у здатності агрегувати різнорідні індикатори, нормалізувати їх до спільної шкали та застосовувати ваги, формуючи підсумкову оцінку, яка може оновлюватися частіше за традиційний аудит. Проте ця ефективність має умови застосовності. По-перше, потрібні витрати на впровадження й супровід, що прямо зазначається як загальний бар'єр інтеграції AI через витрати на впровадження [43]. По-друге, залежність від якість даних означає, що невідповідність, неповнота або неузгодженість джерел здатні зруйнувати відтворюваність результату й створити помилкові управлінські сигнали. По-третє, зростає значущість етики, управління і довіри до автоматизованих рекомендацій, оскільки на основі скорингу можуть прийматися рішення, що впливають на процеси та людей, а непрозорість механіки скорингу послаблює прийнятність результату для відповідальних ролей.

З огляду на ці властивості, практичною точкою балансу є гібридний підхід, який поєднує надійність conventional контрольних процедур із обчислюваністю та оперативністю AI-орієнтованих індикаторів. У гібридній конфігурації класична методика зберігає роль «каркасу»: вона задає домени, критерії та правила інтерпретації, забезпечує нормативну узгодженість і керованість процедури. AI-компонент виступає «сенсорним шаром», який заповнює каркас кількісними сигналами, формує динаміку профілю та дозволяє виявляти розриви між формально задекларованими практиками й фактичним функціонуванням контролів. Такий підхід також узгоджується з ідеєю, що AI може підвищувати швидкість управлінських рішень, але потребує контролю якості даних,

належного governance та готовності персоналу до роботи з автоматизованими оцінками.

Схематично відмінність двох підходів доцільно показувати як два конвеєри формування оцінки, які можуть працювати окремо або в гібридній комбінації:

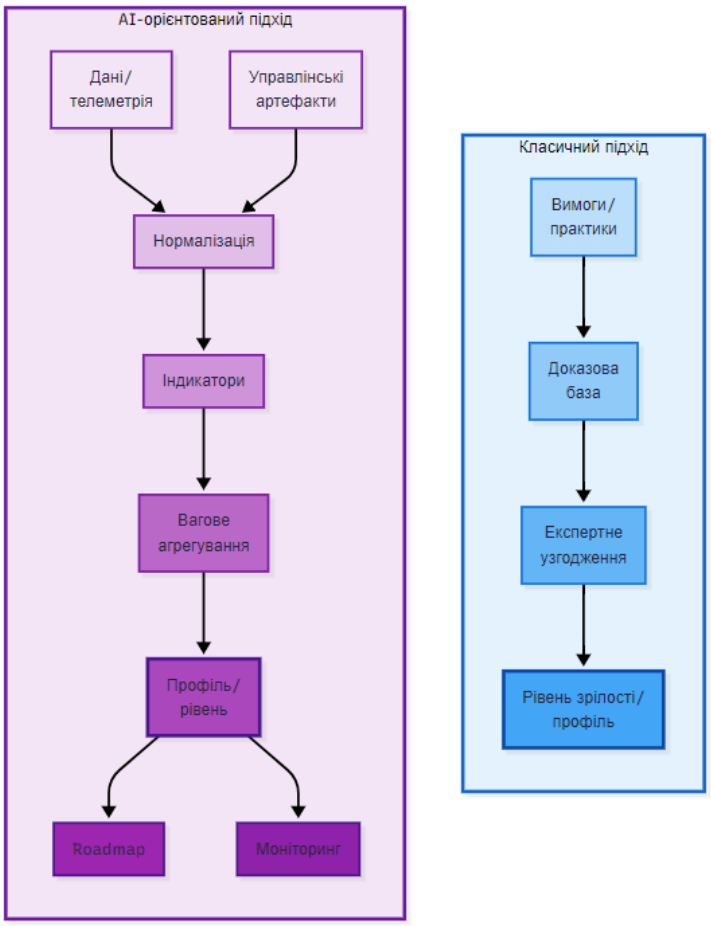

Рис. 2.3. Відмінність двох підходів

Підсумково ефективність класичних і AI-орієнтованих методів оцінювання зрілості визначається тим, яке управлінське завдання є домінуючим і які обмеження існують у середовищі. Класичні підходи забезпечують стандартизований, зрозумілий і доказово контрольований «зріз» спроможностей, що є особливо цінним для відповідності рамкам і для довгострокового планування. AI-орієнтовані підходи забезпечують кількісність, оперативність і можливість трактувати зрілість як динамічний профіль, що відображає поточний

стан через індикатори, нормалізацію та ваговий скоринг, але висувають вимоги до інфраструктури даних, якості джерел і керованості ризиків застосування AI [44]. У практичному управлінні кіберзахистом найбільш стійкою конфігурацією виступає гібридна модель, де класична шкала надає інтерпретаційну стабільність, а AI-індикатори забезпечують вимірюваність і актуальність профілю зрілості.

2.4. Аналіз існуючих інструментів і платформ AI у сфері кібербезпеки

Інструменти та платформи кібербезпеки з використанням AI/ML у практичному вимірі доцільно аналізувати не за наявністю “інтелектуальних” функцій як таких, а за тим, як саме вони вбудовуються в технологічний контур захисту та які контрольовані результати дають. У виробничих середовищах ключовою проблемою є масштаб і різнорідність даних безпеки: журнали подій, мережеві потоки, телеметрія кінцевих точок, дані поштової та веб-взаємодії. Саме на цьому фоні формується клас платформ, які перетворюють високошвидкісний потік сигналів на керовані рішення: оцінку підозрілості, класифікацію, пріоритизацію та рекомендацію дії. Ефективність таких рішень визначається тим, чи забезпечують вони зменшення помилкових спрацювань, стабільну точність на різних типах активності, прийнятний час реагування та інтеграційну сумісність із наявними процесами безпеки. Окремим виміром стає те, що поширення AI створює нову поверхню атаки: у міру того як AI-компоненти включаються у процеси ухвалення рішень, виникають інструментальні потреби не лише “захищати за допомогою AI”, а й “захищати AI”, тобто контролювати дані, моделі, інтерфейси та поведінку AI-систем як активів [45].

З технічної точки зору платформи захисної аналітики з AI/ML відрізняються насамперед типом об’єкта спостереження та характером моделей. Частина інструментів орієнтована на мережевий рівень і будує профіль “нормальної” активності, щоб виділяти відхилення як потенційні атаки. У таких

рішеннях цінність дає не тільки виявлення одиничного відхилення, а й здатність пов’язувати послідовність аномалій у часовій динаміці, щоб не реагувати на шум і водночас не пропустити накопичувальні сценарії. Інша група зосереджена на поведінці користувачів і сутностей, де метою є виявлення внутрішніх загроз або компрометації облікових записів через зміни шаблонів доступу. Третій сегмент орієнтований на кінцеві точки, де критичною є здатність моделі зупиняти виконання шкідливого коду до того, як він розгорне наслідки, використовуючи прогнозування або розпізнавання ознак шкідливої поведінки. Окремо виділяються засоби для протидії фішингу, де аналізується вміст і ознаки повідомлень, а рішенням стає класифікація та блокування або маркування підозрілих листів.

Практичний аналіз таких інструментів доцільно будувати як процедуру вимірювання, а не як опис функцій. Для цього інструмент розглядається як система, яка отримує вхідні дані, застосовує аналітичний механізм і видає результат, який можна перевірити. Вимірюваними показниками виступають частка коректно виявлених загроз, частота хибнопозитивних і хибнонегативних рішень, а також часові характеристики, пов’язані з виявленням і реагуванням. Якщо оцінювання проводиться в контрольованому середовищі, результат зводиться до зіставлення виходів інструмента з наперед визначеним “еталоном” сценарію. Якщо оцінювання доповнюється експертним компонентом, то формалізуються також показники зручності, прийнятності та впливу на робочий процес аналітика. Важливо, що така методика дозволяє порівнювати інструменти різних класів не за маркетинговими тезами, а за однаковими метриками, при цьому враховуючи, що набір метрик має бути узгоджений з доменом: мережеві рішення чутливі до шуму трафіку, засоби для фішингу – до варіативності контенту, а кінцеві точки – до різноманітності середовищ виконання [46].

У сегменті мережевого виявлення загроз характерним є підхід, де модель будує уявлення про типову активність мережі, пристроїв і користувачів, а потім виділяє відхилення як потенційні загрози, включно з невідомими раніше. Для

цього класу рішень принципово важливо, що механізм не прив'язаний до фіксованих сигнатур і може відслідковувати аномалії в режимі безперервного спостереження. Типовий вихід у такому випадку – сигнал про нетипову поведінку з уточненням, що саме відхилилося від профілю. Практичне значення такого рішення проявляється, коли інструмент здатний коректно відокремити атакувальні патерни від легітимних відхилень, оскільки саме на мережевому рівні помилкові спрацювання можуть швидко перевантажити процес обробки інцидентів. Тому оцінювання таких платформ у порівняльному аналізі повинно включати не тільки "виявляє чи ні", а й стабільність рівня помилок за зміни трафікових умов і навантаження.

Поведінкова аналітика користувачів і сутностей формує інший технічний профіль: об'єктом оцінювання стає не пакет або запит, а узгодженість дій суб'єкта з його типовою моделлю. У таких інструментах ключова цінність полягає в тому, що вони виявляють нетипові дії, які можуть свідчити про компрометацію облікового запису або внутрішню загрозу, причому відхилення може проявлятися не в одиничній події, а в зміні послідовності, часу доступу, частоти операцій або "географії" взаємодій. З технічної точки зору платформа повинна забезпечити побудову базової лінії поведінки та механізм детекції відхилень, а також представлення результату так, щоб аналітик міг інтерпретувати сигнал як компонент інциденту. Для порівняння ефективності важливо, чи знижує така аналітика частку "шумових" сповіщень, чи дозволяє фокусувати увагу на стійких відхиленнях і чи масштабується на великі організації, де профілі поведінки мають високу різноманітність [47].

Інструменти для кінцевих точок із AI/ML орієнтовані на те, щоб прогнозувати або попереджати виконання шкідливого коду, аналізуючи характеристики програм або поведінкові ознаки активності. У таких рішеннях технічний ефект досягається не лише виявленням уже відомих зразків, а й здатністю відокремлювати потенційно шкідливі виконувані об'єкти від легітимних за сукупністю ознак. Відповідно, порівняльний аналіз повинен включати показники точності, а також оцінку того, як інструмент поводиться у

випадках, коли шкідливий код прагне уникнути детекції. Оскільки кінцеві точки часто є місцем початкового проникнення, практична цінність таких інструментів визначається не стільки кількістю спрацювань, скільки здатністю обмежити виконання небезпечної активності до того, як вона стане інцидентом із широким впливом.

Фішингові детектори з AI/ML формують ще один клас, де модель аналізує повідомлення за вмістом і додатковими ознаками та виносить рішення про підозрілість. У таких інструментах критичним є баланс між чутливістю до нових, більш переконливих повідомлень і рівнем помилкових блокувань, які можуть порушувати робочі процеси. Технічний аналіз у межах "платформ" зводиться до того, чи забезпечує рішення систематичне виявлення підозрілих повідомлень без надмірного шуму, а також чи має механізм оновлення, який не знижує ефективність при зміні тактик атак.

Окремого аналізу потребують платформи аналітики подій і журналів, у яких AI/ML використовується для виявлення відхилень і надання узагальненого уявлення про стан безпеки організації в режимі постійної обробки даних. У таких рішеннях практично важливо, що результатом стає не лише окреме сповіщення, а контекст, який допомагає аналітику швидше інтерпретувати подію як частину інциденту. Оскільки обсяг журналів великий, ключовою вимогою стає масштабованість обробки й можливість формувати "реальний стан" на основі потоку даних. У межах інструментального аналізу це означає оцінювання здатності системи надавати корисну аналітичну картину, яка зменшує ручне навантаження і водночас не приховує критичних сигналів. У таких платформах AI/ML виконує роль механізму відбору, узагальнення та підсилення кореляції, що і визначає практичну відмінність від суто правилового підходу [48].

Паралельно з розвитком захисних платформ формується напрям інструментів і практик, спрямованих на захист AI-систем як активів. У цьому контексті важливою є модель "трикутника впливів AI на кібербезпеку", яка розділяє три взаємопов'язані площини: посилення кібератак завдяки використанню AI з боку зловмисників, посилення оборонних засобів завдяки

застосуванню AI захисниками, а також розширення поверхні атаки й ризиків для організацій унаслідок впровадження AI-систем у процеси. Саме третя площина формує окрему категорію інструментальних вимог, оскільки AI-система складається з даних, середовищ навчання та виконання, моделі, інтерфейсів, журналювання й моніторингу, а атаки можуть бути спрямовані на будь-яку з цих ланок. Технічний наслідок полягає в тому, що організації мають розширювати свій набір контрольних механізмів так, щоб охоплювати не лише “традиційні” компоненти, а й специфічні загрози для даних навчання, механізмів взаємодії та цілісності виходів.

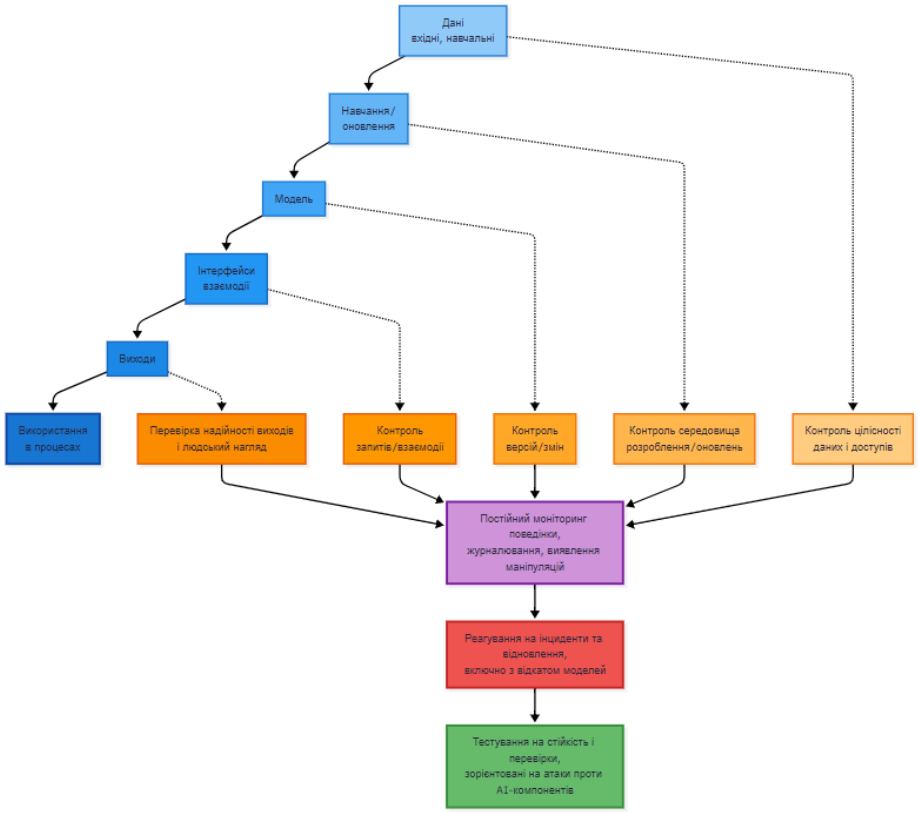

Рис. 2.4 Життєвий цикл безпеки AI-системи

У практичній площині це означає необхідність інвентаризації AI-застосунків, що дозволяє розуміти, які саме моделі та компоненти використовуються, зменшувати ризики неконтрольованого використання та враховувати залежності ланцюга постачання [49]. Далі потрібне вбудовування

принципу безпеки на етапі проєктування, де захисні вимоги застосовуються до даних, моделей і технологій виконання так само, як до класичних інформаційних систем. Важливим стає й управління інформацією: дотримання політик щодо даних, контроль доступів, відповідність вимогам захисту даних у процесах навчання та експлуатації. До цього додаються оновлені процедури реагування на інциденти та безперервності бізнесу з урахуванням сценаріїв компрометації AI-компонентів, включно з механізмами відновлення та контролюованого “відкату” моделі, коли поведінка системи стає ненадійною.

Висновки до розділу 2

Розділ 2 узагальнює сучасні підходи до застосування AI/ML у кіберзахисті як перехід до обробки великих потоків подій і телеметрії з орієнтацією на підвищення точності виявлення, зменшення помилкових спрацювань і скорочення часу реагування. AI використовується для автоматизованого виявлення аномалій у режимі близькому до реального часу, для класифікації та пріоритизації інцидентів, для виявлення загроз без опори на наперед відомі сигнатури через поведінкове моделювання, а також для автоматизації реакцій у межах заданих політик. У межах розглянутих підходів показано, що практична реалізація таких задач спирається на різні класи моделей, які застосовуються відповідно до типу даних і постановки задачі: методи з учителем для класифікації, без учителя для виявлення відхилень у потоках журналів і трафіку, глибокі моделі для роботи з послідовностями подій, а також підходи, спрямовані на оптимізацію дій реагування.

Окремо зафіксовано, що для операційного використання результатів моделей важливо забезпечувати інтерпретованість рішень і можливість пояснення, оскільки це підвищує керованість процесу аналізу та знижує недовіру до автоматизованих рекомендацій. Розглянуто концепції пояснюваного AI як

практичний інструмент обґрунтування висновків моделей у задачах виявлення аномалій і прийняття рішень.

У частині оцінювання ризиків і прогнозування рівня безпеки розділ фіксує методологічну послідовність переходу від сигналів відхилення до інтегральних оцінок через часову агрегацію, а далі до прогнозування на основі динаміки таких оцінок. Порівняння підходів до оцінювання зрілості показує відмінність між дискретними експертними оцінками та індикаторними схемами зі скорингом і нормалізацією. Аналіз інструментів і платформ у сфері AI-кібербезпеки подано через вимірювані критерії ефективності, а також через необхідність врахування ризиків, пов’язаних із захистом AI-систем як активів, включно з контролем даних, моніторингом поведінки та процедурами відновлення.

РОЗДІЛ 3
РОЗРОБКА МЕТОДИКИ ОЦІНЮВАННЯ ЗРІЛОСТІ СИСТЕМ КІБЕРЗАХИСТУ ІЗ ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

3.1. Постановка задачі та вимоги до методики оцінювання

У практиці забезпечення кібербезпеки все частіше використовуються комплексні технічні та організаційні рішення, які поєднують засоби моніторингу, реагування, аналітичної обробки подій та управління інцидентами. Водночас наявні підходи до оцінювання стану та ефективності таких систем здебільшого мають фрагментарний характер, орієнтуються на окремі показники або зводяться до формального аналізу відповідності вимогам стандартів. За таких умов виникає потреба у розробці методики, яка б дозволяла системно та узгоджено оцінювати рівень зрілості систем кіберзахисту з урахуванням як кількісних показників, так і складних взаємозв'язків між ними.

Основною задачею розроблюваної методики є формування формалізованого підходу до оцінювання зрілості системи кіберзахисту організації, який забезпечує узагальнену характеристику її стану на основі об'єктивних даних. Така оцінка повинна відображати не лише факт наявності технічних засобів захисту, а й рівень їх інтегрованості, ефективність процесів виявлення та реагування на інциденти, аналітичну спроможність системи, а також здатність до адаптації в умовах динамічної зміни загрозового середовища. Важливим аспектом постановки задачі є необхідність переходу від ізольованих показників до інтегральної оцінки, що характеризує систему кіберзахисту як цілісний об'єкт управління [50].

У межах даної роботи оцінювання зрілості розглядається як процес аналітичного узагальнення результатів функціонування системи кіберзахисту за визначений період часу. Вхідними даними для такого оцінювання є кількісні вимірювання, отримані з операційних джерел, зокрема журналів подій, результатів моніторингу, статистики інцидентів та показників роботи захисних

механізмів. На їх основі формуються аналітичні метрики, які дозволяють оцінити ефективність окремих функціональних складових системи. Подальша агрегація цих метрик дає змогу визначити інтегральний показник зрілості та віднести систему до відповідного рівня розвитку.

Суттєвою проблемою традиційних підходів до оцінювання є складність аналізу великих обсягів різнорідних даних, а також обмежена можливість виявлення прихованих закономірностей і аномальних відхилень у процесах кіберзахисту. У зв'язку з цим у постановці задачі передбачається використання методів штучного інтелекту як інструменту аналітичної підтримки процесу оцінювання. Застосування інтелектуальних методів дозволяє автоматизувати обробку даних, підвищити точність узагальнення показників та забезпечити більш об'єктивне формування оцінки зрілості. При цьому штучний інтелект розглядається не як автономний механізм прийняття рішень, а як складова системи підтримки прийняття управлінських рішень, що доповнює експертний аналіз [51].

Важливим елементом постановки задачі є вимога пояснюваності результатів оцінювання. Оскільки інтегральний показник зрілості формується на основі складної обробки даних та застосування аналітичних моделей, результати повинні бути інтерпретованими та прозорими для фахівців з кібербезпеки. Це означає, що методика має забезпечувати можливість простежити зв'язок між первинними вимірюваннями, сформованими метриками та кінцевою оцінкою рівня зрілості. Такий підхід підвищує довіру до результатів оцінювання та дозволяє використовувати їх як основу для прийняття практичних рішень щодо вдосконалення системи кіберзахисту.

До ключових вимог розроблюваної методики належить універсальність та узагальнений характер застосування. Методика не повинна бути прив'язаною до конкретних програмно-апаратних рішень, постачальників або галузевих особливостей, що забезпечує можливість її використання в організаціях різного профілю. Водночас вона має бути достатньо гнучкою для адаптації до специфіки інформаційної інфраструктури та рівня розвитку процесів кіберзахисту. Це

досягається шляхом використання абстрактних вимірів оцінювання та можливості налаштування набору метрик і вагових коефіцієнтів [52].

Окремою вимогою є масштабованість методики та можливість її застосування в умовах зростання обсягів даних і ускладнення системи кіберзахисту. Методика повинна підтримувати поетапне вдосконалення, коли на початкових рівнях зрілості використовуються базові показники, а з підвищенням рівня розвитку системи – більш складні аналітичні метрики та інтелектуальні методи обробки.

3.2. Архітектура методики та модель інтеграції AI у процес оцінювання зрілості

Архітектура інтеграції штучного інтелекту у процес оцінювання зрілості систем кіберзахисту ґрунтується на багаторівневій моделі обробки даних, у межах якої інтелектуальні методи застосовуються як аналітичний інструмент узагальнення та інтерпретації результатів функціонування системи. Такий підхід передбачає чітке розмежування функціональних рівнів, що забезпечує прозорість оцінювання, масштабованість методики та можливість адаптації до різних організаційних умов. Штучний інтелект у даній моделі не виступає окремим або автономним компонентом, а інтегрується у загальний процес оцінювання як логічний аналітичний шар між рівнем формування метрик та рівнем прийняття управлінських рішень.

Основою архітектури є рівень операційних даних, який акумулює інформацію про функціонування системи кіберзахисту. До таких даних належать журнали подій, результати моніторингу, статистика інцидентів, показники ефективності захисних механізмів та інші кількісні характеристики, що відображають реальний стан системи. Ці дані є різнорідними за структурою, часовою динамікою та ступенем деталізації, що унеможливлює їх безпосереднє використання для оцінювання зрілості без попередньої аналітичної обробки.

Саме тому архітектура передбачає їх подальше впорядкування та узгодження в межах наступного функціонального рівня.

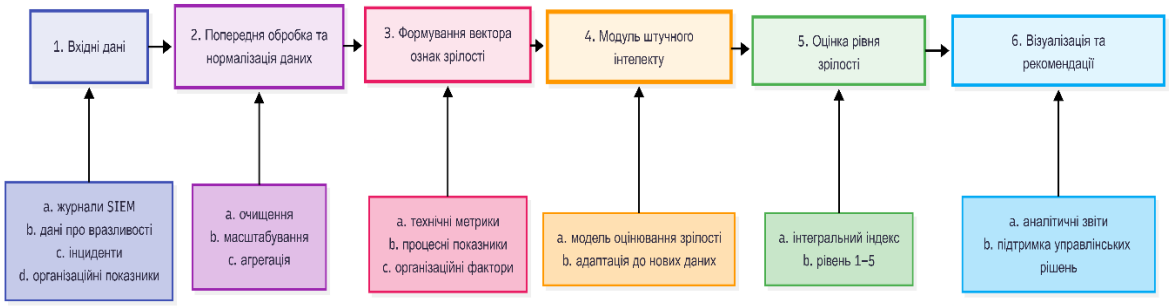

Рис. 3.1 Блок-схема методики оцінювання зрілості систем кіберзахисту об’єктів критичної інформаційної інфраструктури із застосуванням штучного інтелекту

На рівні кількісних вимірювань здійснюється первинна обробка операційних даних, спрямована на виділення спостережуваних показників, що можуть бути використані для оцінювання ефективності окремих аспектів системи кіберзахисту. Ці показники мають об’єктивний характер і відображають конкретні властивості процесів виявлення, реагування та управління інцидентами. Важливою особливістю даного рівня є автоматизований характер збору та обробки даних, що знижує вплив суб’єктивних факторів і підвищує достовірність результатів [53].

Наступним етапом архітектури є рівень аналітичних метрик, на якому здійснюється узагальнення первинних вимірювань у більш високорівневі показники. Метрики формуються шляхом агрегування, нормалізації та узгодження кількісних показників відповідно до визначених вимірів оцінювання зрілості. Саме на цьому рівні відбувається перехід від ізольованих характеристик до системного уявлення про ефективність та керованість кіберзахисту. Рівень метрик є ключовим з точки зору інтеграції штучного інтелекту, оскільки забезпечує структуроване та інтерпретоване представлення даних, придатне для інтелектуального аналізу.

Інтелектуальний аналітичний рівень є центральним елементом розроблюваної архітектури. На цьому рівні застосовуються методи штучного інтелекту для аналізу сформованих метрик з метою виявлення закономірностей, узагальнення станів системи та підтримки процесу оцінювання зрілості. Штучний інтелект використовується для вирішення аналітичних задач, пов'язаних із класифікацією стану системи, групуванням об'єктів оцінювання за подібними характеристиками та виявленням аномальних відхилень у процесах кіберзахисту. При цьому результати інтелектуального аналізу не є остаточним рішенням, а формують аналітичну основу для подальшої інтерпретації.

Важливою вимогою до архітектури є забезпечення пояснюваності результатів інтелектуального аналізу. З цією метою передбачено окремий рівень інтерпретації, який забезпечує зв'язок між вхідними показниками, аналітичними метриками та інтегральною оцінкою зрілості. На цьому рівні результати роботи інтелектуального модуля подаються у формі, зрозумілій для фахівців з кібербезпеки, що дозволяє простежити причинно-наслідкові залежності та обґрунтувати отримані висновки. Такий підхід відповідає концепції систем підтримки прийняття рішень, у межах яких штучний інтелект підсилює аналітичні можливості експерта, але не замінює його [54].

Завершальним етапом архітектури є формування інтегральної оцінки зрілості та аналітичних рекомендацій щодо вдосконалення системи кіберзахисту. Інтегральна оцінка формується на основі узагальнених метрик з урахуванням результатів інтелектуального аналізу та дозволяє віднести систему до одного з визначених рівнів зрілості. Рекомендації, що генеруються на цьому етапі, мають аналітичний характер і спрямовані на підвищення ефективності процесів, усунення виявлених недоліків та забезпечення подальшого розвитку системи [55].

Узагальнену архітектурну модель інтеграції штучного інтелекту у процес оцінювання зрілості систем кіберзахисту можна подати у вигляді такої послідовності функціональних рівнів на Рис. 3.2.

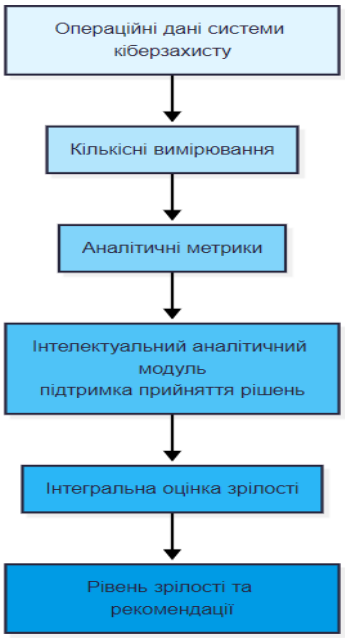

Рис. 3.2. Архітектура інтеграції штучного інтелекту в процес оцінювання зрілості

Запропонована архітектура забезпечує цілісність процесу оцінювання, узгоджує класичні підходи до побудови показників кіберзахисту з можливостями інтелектуального аналізу та створює методичне підґрунтя для реалізації алгоритмічних і технічних засобів оцінювання, які розглядаються у наступному підрозділі.

3.3. Алгоритмічні та технічні засоби для реалізації оцінювання

Алгоритмічні та технічні засоби в межах розроблюваної методики оцінювання зрілості систем кіберзахисту застосовуються для аналітичної обробки сформованих метрик та підтримки процесу формування узагальненої оцінки. На відміну від традиційних підходів, де оцінювання здійснюється шляхом порівняння окремих показників із фіксованими пороговими значеннями, запропонована методика передбачає використання методів штучного інтелекту для виявлення складних залежностей, узагальнення станів системи та аналізу її

поведінки в динаміці. Алгоритмічні засоби інтегруються в інтелектуальний аналітичний рівень архітектури, описаної у попередньому підрозділі, та працюють з аналітичними метриками як з формалізованим представленням стану системи кіберзахисту [56].

Загальна логіка застосування алгоритмічних методів у процесі оцінювання зрілості може бути подана у вигляді узгодженого ланцюга аналітичної обробки, у межах якого кожен клас алгоритмів виконує окрему функцію, на Рис. 3.2.

Ключовим алгоритмічним засобом у межах методики є класифікація, яка використовується для формального віднесення системи кіберзахисту до одного з визначених рівнів зрілості. Задача визначення рівня зрілості за своєю природою є задачею класифікації, оскільки на основі набору вхідних ознак, представлених аналітичними метриками, необхідно визначити клас, що відповідає поточному стану системи.

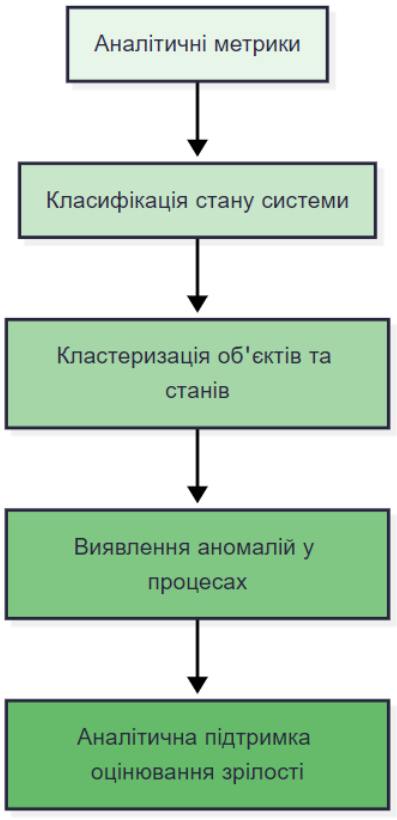

Рис. 3.3. Загальна алгоритмічна логіка процесу оцінювання зрілості

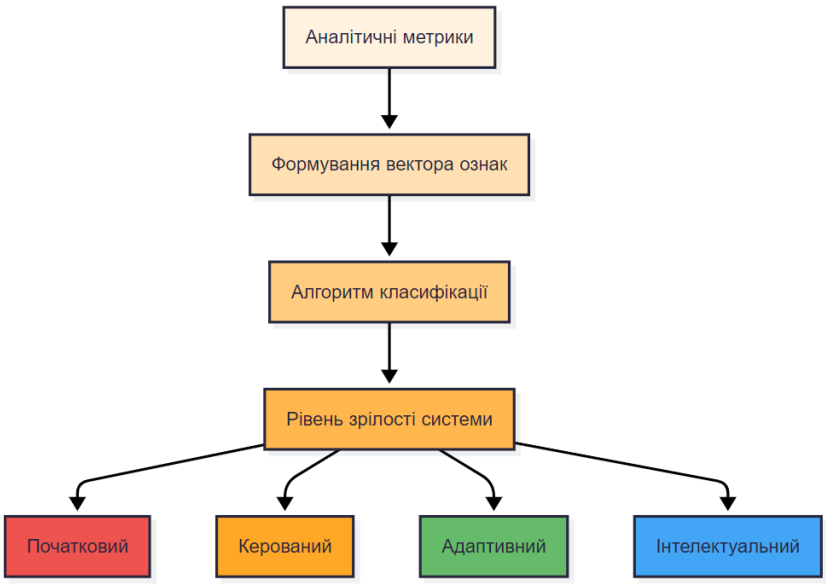

Рис. 3.4. Класифікація рівня зрілості за аналітичними метриками

У цьому контексті метрики виступають узагальненими характеристиками ефективності процесів кіберзахисту, а результат класифікації відображає інтегральну оцінку їх зрілості. Використання класифікаційного підходу дозволяє формалізувати процес оцінювання та забезпечити порівнюваність результатів у часі, що є важливим для аналізу розвитку системи та контролю ефективності впроваджених змін [57].

Класифікація у межах методики не розглядається як жорсткий механізм прийняття остаточного рішення, а використовується як інструмент аналітичної підтримки. Результат класифікації формує обґрунтовану рекомендацію щодо рівня зрілості, яка може бути додатково інтерпретована та уточнена експертом. Такий підхід забезпечує поєднання формалізованого аналізу з можливістю урахування контекстних факторів, що не завжди можуть бути повністю відображені у числових показниках.

Доповненням до класифікаційного аналізу є кластеризація, яка застосовується для структурного аналізу стану системи кіберзахисту. Кластеризація дозволяє групувати об’єкти оцінювання або окремі сегменти системи за подібністю їх характеристик, що є особливо важливим у випадках, коли система є неоднорідною та включає різні підсистеми або функціональні

компоненти [58]. У межах оцінювання зрілості кластеризація не використовується для безпосереднього визначення рівня, проте забезпечує глибше розуміння внутрішньої структури системи та дозволяє виявити ділянки з різним рівнем розвитку.

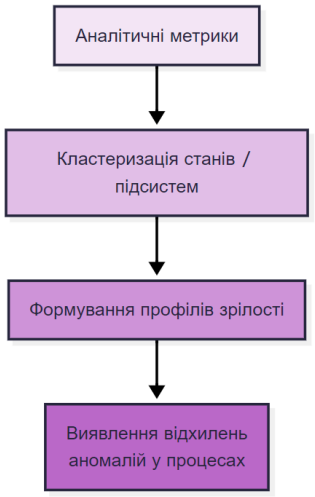

Рис. 3.5. Кластеризація та виявлення аномальних відхилень

Алгоритмічний підхід кластеризації є корисним для аналізу відмінностей між підрозділами, процесами або часовими інтервалами функціонування системи кіберзахисту. Результати кластеризації дозволяють визначити, чи є система цілісною з точки зору зрілості, чи її окремі компоненти перебувають на різних етапах розвитку. Це створює додаткову аналітичну основу для прийняття управлінських рішень та формування адресних рекомендацій щодо вдосконалення окремих елементів системи.

Ще одним важливим алгоритмічним засобом у межах методики є виявлення аномалій, яке застосовується для контролю стабільності процесів кіберзахисту та виявлення нетипових відхилень у їх функціонуванні. У контексті оцінювання зрілості аномалія розглядається не як безпосередня ознака кіберінциденту, а як відхилення від усталеного профілю функціонування системи або очікуваного рівня ефективності процесів. Такі відхилення можуть свідчити про деградацію окремих механізмів, зниження якості реагування або порушення узгодженості між компонентами системи [59].

Виявлення аномалій дозволяє доповнити статичну оцінку зрілості динамічним аналізом, що враховує зміни стану системи у часі. Алгоритмічні методи аналізу відхилень забезпечують раннє виявлення проблемних тенденцій та створюють підґрунтя для своєчасного коригування процесів кіберзахисту. Таким чином, anomaly detection виконує функцію індикатора стабільності та надійності системи в межах обраного рівня зрілості.

Узгоджене використання класифікації, кластеризації та виявлення аномалій дозволяє реалізувати комплексний аналітичний підхід до оцінювання зрілості систем кіберзахисту. Класифікація забезпечує формалізоване визначення рівня зрілості, кластеризація – структурний аналіз та виявлення неоднорідності, а виявлення аномалій – контроль динаміки та стабільності процесів. Сукупність цих алгоритмічних засобів формує інтелектуальний аналітичний механізм, який підсилює класичні методи оцінювання та забезпечує більш глибоке і обґрунтоване розуміння стану системи кіберзахисту.

3.4. Розробка критеріїв та показників оцінювання зрілості

Оцінювання зрілості систем кіберзахисту потребує формалізованого підходу до визначення тих властивостей системи, які відображають рівень її розвитку, ефективності та керованості. У межах розроблюваної методики така формалізація досягається шляхом побудови системи критеріїв та показників, що забезпечують перехід від спостережуваних даних до інтегральної оцінки зрілості. Критерії та показники виконують роль зв’язувальної ланки між архітектурою оцінювання, алгоритмічними засобами аналізу та кінцевим результатом у вигляді визначеного рівня зрілості системи кіберзахисту.

Критерій у межах методики розглядається як узагальнена характеристика певної функціональної властивості системи кіберзахисту, що має принципове значення для оцінювання її зрілості. Критерії формуються на високому рівні абстракції та відображають ключові аспекти функціонування системи, зокрема ефективність виявлення загроз, якість реагування на інциденти, аналітичну

спроможність, формалізацію процесів та здатність до адаптації. Важливою особливістю критеріїв є їх відносна стабільність у часі, оскільки вони не залежать від конкретних технічних рішень або інструментів, а відображають фундаментальні властивості системи кіберзахисту як об’єкта управління [60].

Для забезпечення можливості практичного оцінювання кожен критерій деталізується через набір показників. Показники є кількісними, спостережуваними характеристиками, які формуються на основі операційних даних системи кіберзахисту. Вони відображають конкретні аспекти реалізації відповідного критерію та можуть бути отримані автоматизовано з журналів подій, статистики інцидентів або результатів моніторингу. Таким чином, показники забезпечують об’єктивність оцінювання та зменшують залежність результатів від суб’єктивних експертних суджень.

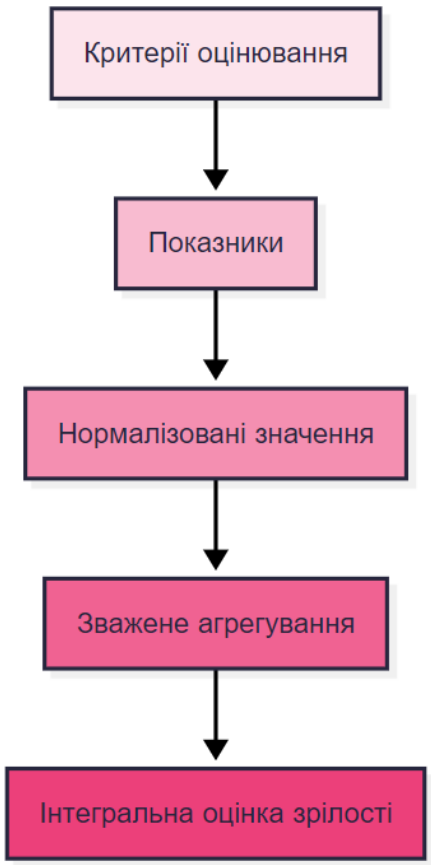

Рис. 3.6. Взаємозв’язок між критеріями, показниками та інтегральною оцінкою зрілості

Показники, що описують різні критерії, можуть мати різні одиниці вимірювання, масштаби та діапазони значень. Це унеможливлює їх безпосереднє агрегування без попередньої обробки [61]. У зв'язку з цим методика передбачає нормалізацію показників, метою якої є приведення їх значень до єдиної шкали. Нормалізовані значення відображають відносний рівень досягнення відповідної властивості системи та створюють основу для подальшого зваженого узагальнення. Нормалізація дозволяє забезпечити порівнюваність показників та коректність інтегральної оцінки незалежно від їх початкової природи.

Рис. 3.7. Формалізація процесу нормалізації показників

Після нормалізації показників виникає необхідність урахування різної значущості окремих критеріїв для загальної оцінки зрілості. Не всі властивості системи кіберзахисту однаково впливають на її загальний рівень розвитку, тому методика передбачає використання вагових коефіцієнтів. Ваги відображають відносну важливість відповідних критеріїв у межах оцінювання та можуть коригуватися залежно від контексту застосування методики, типу організації або цілей аналізу. Такий підхід забезпечує гнучкість методики та можливість її адаптації без зміни загальної структури моделі.

Інтегральна оцінка зрілості формується шляхом зваженого агрегування нормалізованих значень показників або метрик, що відповідають окремим критеріям. У загальному вигляді інтегральний показник зрілості може бути поданий як зважена сума відповідних складових:

$$M = \sum_{i=1}^{n} w_i \times C_i \tag{3.1}$$

де C_i є узагальненим значенням метрики відповідного критерію, а w_i – ваговим коефіцієнтом, що відображає його значущість. Отримане значення інтегрального показника використовується для віднесення системи кіберзахисту до одного з визначених рівнів зрілості, що забезпечує формалізований та відтворюваний результат оцінювання.

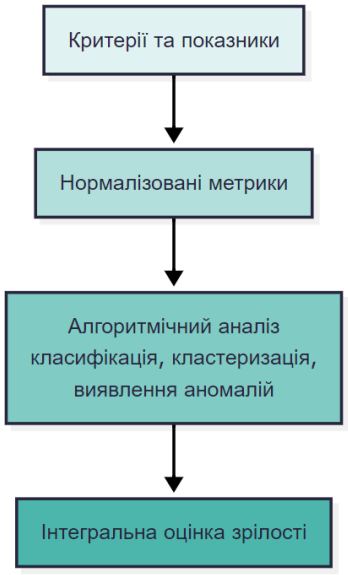

Рис. 3.8. Взаємодія критеріїв, показників та алгоритмічних методів оцінювання

Розробка критеріїв та показників оцінювання зрілості є ключовим етапом методики, який забезпечує її формальну визначеність та практичну застосовність. Саме коректність вибору критеріїв, адекватність показників та обґрунтованість їх агрегування визначають якість отриманих результатів і можливість їх подальшого використання для аналітичної підтримки управлінських рішень. Запропонований підхід створює методичне підґрунтя для

практичної апробації методики оцінювання зрілості систем кіберзахисту, яка розглядається у наступному підрозділі.

3.5. Апробація розробленої методики оцінювання зрілості систем кіберзахисту

Апробація розробленої методики оцінювання зрілості систем кіберзахисту здійснюється на умовній моделі організації з метою демонстрації практичної реалізації запропонованого підходу та наочності аналітичних результатів. Використання умовної моделі дозволяє проілюструвати повний цикл оцінювання – від формування вхідних показників до інтерпретації інтегральної оцінки – без залучення реальних конфіденційних даних. Усі числові значення, наведені в межах підрозділу, є умовними та використовуються виключно для візуалізації процесу апробації методики.

Як об’єкт апробації розглядається умовна організація середнього рівня складності з розподіленою інформаційною інфраструктурою. У системі кіберзахисту реалізовано централізований збір подій безпеки, базові механізми реагування на інциденти та формалізовані організаційні процедури. За умовний період спостереження система реєструє близько 120 подій безпеки на місяць, з яких орієнтовно 30 подій класифікуються як інциденти, що потребують реагування. Середній час первинного реагування становить близько 4 годин, рівень автоматизації реагування – близько 40 %, а – аналітична обробка подій здійснюється переважно на основі кореляційних правил [62].

На першому етапі апробації формується набір показників відповідно до критеріїв оцінювання, визначених у підрозділі 3.4. Для критерію ефективності виявлення загроз використовуються умовні показники частки виявлених інцидентів та рівня хибних спрацювань. Для критерію реагування враховуються середній час реагування та рівень автоматизації процедур. Аналітична спроможність характеризується часткою корельованих подій і стабільністю аналітичних правил. Формалізація процесів оцінюється через наявність

регламентів і рівень їх дотримання, а здатність до адаптації – через частоту перегляду правил і процедур кіберзахисту.

Після нормалізації показників до єдиної шкали формується аналітичний профіль зрілості системи кіберзахисту. Для умовної моделі отримано такі нормалізовані значення критеріїв: ефективність виявлення загроз – 0,68; ефективність реагування – 0,55; аналітична спроможність – 0,60; формалізація процесів – 0,70; здатність до адаптації – 0,50. Отримані значення відображають нерівномірний розвиток окремих складових системи та створюють основу для подальшого аналітичного узагальнення.

Аналітичний профіль зрілості доцільно подати у вигляді радарної діаграми, що дозволяє наочно відобразити співвідношення між критеріями.

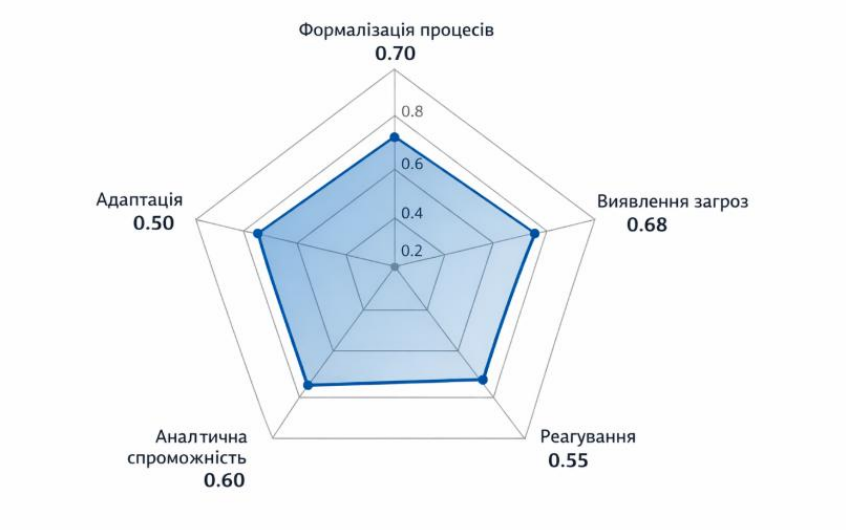

Рис. 3.9 Профіль зрілості

Дана діаграма демонструє асиметричний характер зрілості системи: більш високі значення формалізації процесів і виявлення загроз поєднуються з відносно нижчими показниками реагування та адаптації. Такий профіль не завжди очевидний при прямому аналізі окремих показників, однак стає наочно видимим у межах комплексного оцінювання.

На наступному етапі застосовується інтелектуальний аналітичний шар, який працює з нормалізованими значеннями критеріїв. У межах апробації

розглядаються два аналітичні представлення стану системи: базове агрегування показників та скориговане представлення після інтелектуального узгодження.

Таблиця 3.1

Результати порівняння

Критерій	**Стан А (пряме агрегування)**	**Стан В (після інтелектуального аналізу)**
Виявлення загроз	0,65	0,68
Реагування на інциденти	0,52	0,55
Аналітична спроможність	0,55	0,60
Формалізація процесів	0,70	0,70
Адаптація	0,45	0,50

Стан А відповідає прямому агрегуванню показників без урахування структурних залежностей та аномальних відхилень, тоді як Стан В відображає результати інтелектуального аналізу, який дозволяє зменшити вплив шумових характеристик та узгодити значення критеріїв. Важливо підкреслити, що наведене порівняння не відображає зміну стану системи у часі, а демонструє різні аналітичні представлення одного і того ж набору умовних даних.

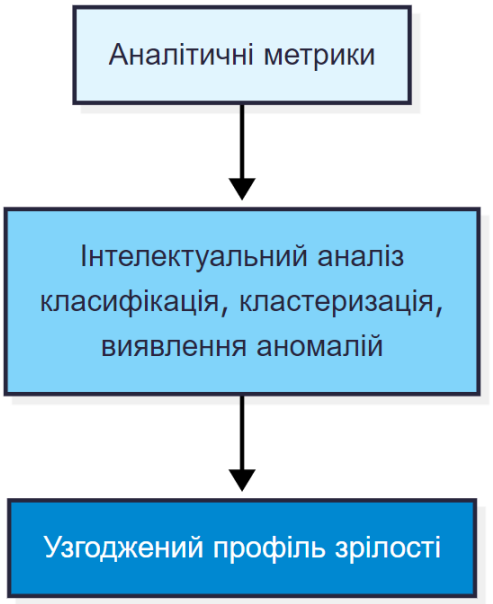

Рис. 3.10. Загальна логіка аналітичного узгодження

На основі скоригованого аналітичного профілю виконується зважене агрегування критеріїв із використанням рівномірних вагових коефіцієнтів. У результаті інтегральна оцінка зрілості умовної системи кіберзахисту становить 0,61. Отримане значення відповідає **адаптивному рівню зрілості**, що характеризується наявністю формалізованих процесів, використанням аналітичних механізмів та здатністю до часткової адаптації до змін загрозового середовища.

Інтерпретація результату апробації свідчить, що методика дозволяє не лише формально віднести систему до певного рівня зрілості, але й виявити дисбаланс між окремими критеріями. Зокрема, нижчі значення показників реагування та адаптації порівняно з рівнем формалізації процесів вказують на потенційні напрями вдосконалення системи кіберзахисту.

3.6. Оцінка результатів та формування рекомендацій для практичного застосування

Оцінка результатів апробації методики оцінювання зрілості систем кіберзахисту ґрунтується на аналізі інтегральної оцінки та аналітичного профілю критеріїв, сформованих у попередньому підрозділі. Отриманий результат у вигляді адаптивного рівня зрілості відображає загальний стан системи кіберзахисту умовної організації та свідчить про наявність формалізованих процесів, базових аналітичних механізмів і здатності до часткової адаптації до змін загрозового середовища. Водночас сам по собі рівень зрілості не є вичерпною характеристикою, оскільки не відображає внутрішньої структури розвитку системи та співвідношення між окремими її складовими. Саме тому ключовим елементом оцінювання виступає аналітичний профіль критеріїв, який забезпечує пояснюваність та інтерпретованість отриманого результату.

Аналіз аналітичного профілю показує нерівномірність розвитку окремих аспектів системи кіберзахисту. Вищі значення критеріїв формалізації процесів та ефективності виявлення загроз свідчать про наявність регламентованих

процедур і базової здатності системи ідентифікувати інциденти. Водночас відносно нижчі значення критеріїв реагування та адаптації вказують на обмеження в оперативності та гнучкості процесів кіберзахисту. Такий дисбаланс є типовим для систем, що перебувають на адаптивному рівні зрілості, і відображає перехідний характер їх розвитку від керованих до більш інтелектуалізованих підходів.

Важливою особливістю запропонованої методики є те, що рекомендації формуються не на основі інтуїтивної експертної оцінки, а випливають безпосередньо з результатів аналітичного оцінювання. Це означає, що напрями вдосконалення визначаються з урахуванням конкретних дисбалансів між критеріями та їхнього впливу на загальний рівень зрілості. Такий підхід забезпечує обґрунтованість рекомендацій і дозволяє використовувати їх як основу для прийняття управлінських рішень у сфері кіберзахисту.

Для системи кіберзахисту з адаптивним рівнем зрілості першочерговими є рекомендації, спрямовані на підвищення ефективності реагування на інциденти. Зокрема, доцільним є оптимізація процедур реагування шляхом зменшення часу первинної реакції, підвищення рівня автоматизації типових дій та чіткого розмежування відповідальності між учасниками процесу. Реалізація таких заходів дозволяє не лише покращити оперативні показники, але й підвищити узгодженість реагування з аналітичними результатами системи моніторингу.

Окремим напрямом рекомендацій є розвиток аналітичної спроможності системи кіберзахисту. Аналітичний профіль свідчить, що наявні механізми аналізу подій забезпечують базову кореляцію, однак мають обмежені можливості щодо виявлення прихованих залежностей та нетипових сценаріїв. У практичному застосуванні це означає доцільність розширення аналітичних підходів, зокрема шляхом удосконалення правил кореляції, підвищення якості вхідних даних та регулярного перегляду аналітичних моделей. Такі заходи сприяють більш точній інтерпретації подій і створюють підґрунтя для переходу до інтелектуального рівня зрілості.

Рекомендації щодо підвищення адаптивності системи кіберзахисту пов’язані з необхідністю забезпечення системного перегляду та оновлення процесів. Низька або середня здатність до адаптації часто зумовлена статичністю регламентів і відсутністю механізмів зворотного зв’язку між результатами оцінювання та управлінськими рішеннями. У цьому контексті практичне застосування методики передбачає використання результатів оцінювання зрілості як вхідної інформації для регулярного коригування політик, процедур і аналітичних налаштувань системи кіберзахисту.

Запропонована методика може використовуватися не лише для разового оцінювання, а й як інструмент регулярного моніторингу розвитку системи кіберзахисту. Періодичне повторення оцінювання з використанням однакових критеріїв і показників дозволяє відстежувати динаміку змін, оцінювати ефективність управлінських рішень та своєчасно виявляти негативні тенденції. У такому форматі методика виконує функцію системи підтримки прийняття рішень, забезпечуючи аналітичну основу для планування заходів з підвищення рівня зрілості.

Водночас слід враховувати обмеження застосування методики. Якість отриманих результатів безпосередньо залежить від повноти, достовірності та узгодженості вхідних даних. Крім того, методика не замінює експертну оцінку, а доповнює її, надаючи формалізований інструмент аналітичної підтримки. Застосування штучного інтелекту в межах методики не є самоціллю і не гарантує автоматичного підвищення рівня зрілості, а слугує засобом покращення якості оцінювання та інтерпретації результатів.

Висновки до розділу 3

У третьому розділі роботи розроблено методику оцінювання зрілості систем кіберзахисту об'єктів критичної інформаційної інфраструктури із застосуванням методів штучного інтелекту як інструменту аналітичної підтримки процесу оцінювання.

Сформульовано вимоги до методики оцінювання, серед яких ключовими є системність аналізу, пояснюваність результатів, універсальність застосування та масштабованість. Визначено основну задачу методики як формування інтегральної оцінки стану системи кіберзахисту на основі об'єктивних кількісних даних з урахуванням складних взаємозв'язків між показниками ефективності.

Розроблено багаторівневу архітектуру інтеграції штучного інтелекту в процес оцінювання, яка включає рівень операційних даних, кількісних вимірювань, аналітичних метрик, інтелектуального аналізу, інтерпретації та формування інтегральної оцінки. Запропонована архітектура забезпечує прозорість процесу оцінювання та чітке розмежування функцій між аналітичними компонентами та механізмами підтримки прийняття рішень.

Визначено алгоритмічні засоби реалізації методики, які включають класифікацію для віднесення системи до рівня зрілості, кластеризацію для структурного аналізу неоднорідності компонентів та виявлення аномалій для контролю стабільності процесів кіберзахисту. Узгоджене використання цих методів формує комплексний інтелектуальний аналітичний механізм оцінювання.

Розроблено систему критеріїв та показників оцінювання зрілості, яка охоплює ефективність виявлення загроз, якість реагування на інциденти, аналітичну спроможність, формалізацію процесів та здатність до адаптації. Формалізовано підхід до нормалізації показників та їх зваженого агрегування в інтегральну оцінку, що забезпечує порівнюваність результатів та відтворюваність процесу оцінювання.

Апробація методики виконана на умовній моделі організації середнього рівня складності. Сформовано аналітичний профіль зрілості з нормалізованими значеннями критеріїв та отримано інтегральну оцінку 0,61, що відповідає адаптивному рівню зрілості. Виявлено нерівномірність розвитку окремих складових системи кіберзахисту, зокрема відносно нижчі показники реагування та адаптації порівняно з формалізацією процесів.

На основі результатів апробації сформовано практичні рекомендації щодо вдосконалення системи кіберзахисту, які випливають безпосередньо з аналітичного профілю та включають оптимізацію процедур реагування, розвиток аналітичної спроможності та підвищення адаптивності системи до змін загрозового середовища.

Розроблена методика забезпечує формалізований та відтворюваний підхід до оцінювання зрілості систем кіберзахисту, поєднує можливості інтелектуального аналізу з експертною інтерпретацією та може використовуватися як інструмент регулярного моніторингу розвитку систем кіберзахисту організацій.

ВИСНОВКИ

У кваліфікаційній роботі здійснено комплексне дослідження теоретичних, методологічних та прикладних аспектів оцінювання зрілості систем кіберзахисту об’єктів критичної інформаційної інфраструктури із застосуванням технологій штучного інтелекту. Обрана тема є надзвичайно актуальною в умовах цифровізації суспільства, зростання залежності держави, бізнесу та населення від стабільного функціонування критичних інформаційних систем, а також постійного ускладнення та еволюції кіберзагроз, які мають як технічний, так і організаційний та соціальний характер.

У процесі дослідження встановлено, що об’єкти критичної інформаційної інфраструктури становлять основу життєзабезпечення держави та суспільства, а порушення їх функціонування внаслідок кіберінцидентів може призвести до значних економічних втрат, загроз національній безпеці та суспільній стабільності. У зв’язку з цим системи кіберзахисту таких об’єктів мають відповідати високим вимогам щодо надійності, адаптивності та керованості, а рівень їх зрілості повинен регулярно оцінюватися з метою своєчасного виявлення проблемних аспектів і визначення напрямів подальшого розвитку.

У першому розділі дипломної роботи узагальнено теоретичні та методологічні засади оцінювання зрілості систем кіберзахисту. Розкрито сутність і значення систем кіберзахисту для об’єктів критичної інформаційної інфраструктури, що дозволило обґрунтувати необхідність комплексного підходу до забезпечення безпеки, який поєднує технічні, організаційні та процесні компоненти. Проаналізовано основні підходи та моделі зрілості в кібербезпеці, зокрема моделі, що базуються на процесному управлінні, ризик-орієнтованому підході та безперервному вдосконаленні систем безпеки.

Окрему увагу приділено аналізу нормативно-правових і стандартних вимог до оцінювання зрілості систем кіберзахисту відповідно до міжнародних стандартів та рекомендацій, таких як ISO/IEC, NIST, ENISA та інших профільних організацій. Встановлено, що чинні стандарти створюють необхідну

методологічну основу для побудови систем кіберзахисту, проте не завжди забезпечують достатню гнучкість та адаптивність до динамічних умов кіберпростору. У результаті аналізу проблем і обмежень традиційних методів оцінювання зрілості виявлено їх основні недоліки, зокрема високий рівень суб'єктивності експертних оцінок, значну трудомісткість процедур, статичність моделей та обмежені можливості щодо обробки великих обсягів різнорідних даних.

Другий розділ роботи присвячено аналізу сучасних підходів до застосування штучного інтелекту в оцінюванні та управлінні кіберзахистом. Досліджено можливості використання методів машинного навчання, аналізу великих даних та інтелектуального аналізу поведінки для підвищення ефективності систем інформаційної безпеки. Показано, що технології штучного інтелекту здатні забезпечити більш глибокий і динамічний аналіз стану кіберзахисту за рахунок автоматизованого виявлення аномалій, прогнозування розвитку загроз та оцінювання ризиків у режимі, наближеному до реального часу.

У межах другого розділу проведено порівняльний аналіз класичних та AI-орієнтованих методів оцінювання зрілості систем кіберзахисту. Результати аналізу свідчать, що використання штучного інтелекту дозволяє суттєво підвищити точність і об'єктивність оцінювання, зменшити вплив людського фактору та забезпечити масштабованість методик. Водночас визначено низку викликів, пов'язаних із впровадженням AI-рішень, зокрема потребу в якісних даних, складність інтерпретації результатів та необхідність інтеграції інтелектуальних моделей у існуючі системи управління кібербезпекою. Також проаналізовано сучасні інструменти та платформи, що використовуються у сфері кібербезпеки, та оцінено їх потенціал щодо підтримки процесів оцінювання зрілості.

У третьому розділі дипломної роботи розроблено методику оцінювання зрілості систем кіберзахисту об'єктів критичної інформаційної інфраструктури із застосуванням штучного інтелекту. Сформульовано постановку задачі та

визначено основні вимоги до методики, зокрема універсальність, адаптивність, об’єктивність та можливість практичного впровадження. Запропоновано архітектуру інтеграції AI у процес оцінювання зрілості, яка передбачає поетапний збір і обробку даних, аналіз показників стану кіберзахисту та формування інтегральної оцінки рівня зрілості.

У рамках розробки методики визначено алгоритмічні та технічні засоби її реалізації, а також сформовано систему критеріїв і показників оцінювання зрілості, що охоплює організаційні, процесні та технічні аспекти функціонування систем кіберзахисту. Запропоновані критерії дозволяють комплексно оцінювати рівень зрілості з урахуванням специфіки об’єктів критичної інформаційної інфраструктури та сучасних вимог до кібербезпеки. Наведений приклад апробації методики підтвердив її практичну придатність та можливість використання для формування обґрунтованих рекомендацій щодо підвищення ефективності систем кіберзахисту.

Загалом результати дослідження свідчать, що застосування технологій штучного інтелекту в процесах оцінювання зрілості систем кіберзахисту забезпечує підвищення якості аналітичної підтримки управлінських рішень, сприяє своєчасному виявленню слабких місць у системах безпеки та створює передумови для їх безперервного вдосконалення. Запропонована методика може бути використана органами державної влади, підприємствами та організаціями, що експлуатують об’єкти критичної інформаційної інфраструктури, а також слугувати основою для подальших наукових досліджень у сфері інтелектуалізації управління кібербезпекою та розвитку адаптивних систем кіберзахисту.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Agha A. Bolstering the cyber defenses of critical infrastructure: an in-depth analysis of ai-driven security for industrial control systems. *SSRN electronic journal*. 2025. URL: https://doi.org/10.2139/ssrn.5010490

2. Agus Kurniati. Study of the artificial intelligence role in achieving cybersecurity for critical information infrastructure. *Monas: jurnal inovasi aparatur*. 2024. Vol. 6, no. 2. P. 154–165. URL: https://doi.org/10.54849/monas.v6i2.251

3. Ajimatanrareje G. A., Agbesi J. S. AI-Powered zero trust architectures for critical infrastructure protection: a comprehensive framework for next-generation cybersecurity. *International journal of scientific research and modern technology*. 2025. P. 40–56. URL: https://doi.org/10.38124/ijsrmt.v4i9.792

4. An automated compliance framework for critical infrastructure security through artificial intelligence / S. M. Ali et al. *IEEE access*. 2025. P. 1. URL: https://doi.org/10.1109/access.2024.3524496

5. A systematic review and critical evaluation of the available research on artificial intelligence approaches for asthma / P. K. Shukla et al. *Artificial intelligence and information technologies*. London, 2024. P. 348–352. URL: https://doi.org/10.1201/9781003510833-57

6. Autonomous ai-based cybersecurity framework for critical infrastructure: real-time threat mitigation / J. Paulraj et al. *2025 IEEE/ACIS 29th international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD)*, Busan, Korea, Republic of, 25–27 June 2025. 2025. P. 925–931. URL: https://doi.org/10.1109/snpd65828.2025.11254587

7. Bright Ojo, Chukwudi Tabitha Aghaunor. AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. *International journal of science and research archive*. 2024. Vol. 12, no. 2. P. 1716–1726. URL: https://doi.org/10.30574/ijsra.2024.12.2.1401

8. Buzdugan A., Căpățână G. A formal intelligent metric system for measuring cyber security maturity. *Proceedings of 22nd international conference on*

informatics in economy (IE 2023). Singapore, 2024. P. 249–258. URL: https://doi.org/10.1007/978-981-99-6529-8_21

9. de Oliveira Silva H. CSAI-4-CPS: a cyber security characterization model based on artificial intelligence for cyber physical systems. *2022 52nd annual IEEE/IFIP international conference on dependable systems and networks - supplemental volume (DSN-S)*, Baltimore, MD, USA, 27–30 June 2022. 2022. URL: https://doi.org/10.1109/dsn-s54099.2022.00032

10. Eze Chinelo E. C., Umeanozie P., Alozie C. E. Enhancing threat intelligence for critical infrastructure protection through artificial intelligence: a proactive cyber defence approach. *International journal of scientific research and modern technology*. 2025. P. 20–29. URL: https://doi.org/10.38124/ijsrmt.v4i5.513

11. Govea J., Gaibor-Naranjo W., Villegas-Ch W. Transforming cybersecurity into critical energy infrastructure: a study on the effectiveness of artificial intelligence. *Systems*. 2024. Vol. 12, no. 5. P. 165. URL: https://doi.org/10.3390/systems12050165

12. Gujar S. S. Optimizing threat mitigation in critical infrastructure through ai-driven cybersecurity solutions. *2024 global conference on communications and information technologies (GCCIT)*, BANGALORE, India, 25–26 October 2024. 2024. P. 1–7. URL: https://doi.org/10.1109/gccit63234.2024.10862689

13. Hasanov I. I. Methodology for assessing the security of critical information infrastructure objects based on semantic analysis and graph attack models. *Вопросы безопасности*. 2025. No. 3. P. 26–38. URL: https://doi.org/10.25136/2409-7543.2025.3.75745

14. Mmaduekwe E. AI-Driven cyber threat detection for securing national critical infrastructure. *Asian journal of research in computer science*. 2025. Vol. 18, no. 6. P. 424–431. URL: https://doi.org/10.9734/ajrcos/2025/v18i6711

15. M M U. AI-Powered cybersecurity for critical infrastructure: a comprehensive survey. *International journal for research in applied science and engineering technology*. 2025. Vol. 13, no. 7. P. 2678–2680. URL: https://doi.org/10.22214/ijraset.2025.73439

16. Mokhor V., Honchar S., Onyskova A. Cybersecurity risk assessment of information systems of critical infrastructure objects. *2020 IEEE international conference on problems of infocommunications. science and technology (PIC S&T)*, Kharkiv, Ukraine, 6–9 October 2020. 2020. URL: https://doi.org/10.1109/picst51311.2020.9467957

17. Parshenkova Y., Maksimova E., Matveev A. Analysis of information security risks at critical information infrastructure facilities using neural networks and fuzzy cognitive maps. *Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia»*. 2024. Vol. 2024, no. 3. P. 86–97. URL: https://doi.org/10.61260/2218-130x-2024-3-86-97

18. Sithungu S., Lipps C. Critical infrastructure security and the role of AI: an overview. *European conference on cyber warfare and security*. 2025. Vol. 24, no. 1. P. 656–664. URL: https://doi.org/10.34190/eccws.24.1.3770

19. Wen S.-F., Shukla A., Katt B. Artificial intelligence for system security assurance: a systematic literature review. *International journal of information security*. 2024. Vol. 24, no. 1. URL: https://doi.org/10.1007/s10207-024-00959-0

20. Wen S.-F., Shukla A., Katt B. Artificial intelligence for system security assurance: a systematic literature review. *International journal of information security*. 2024. Vol. 24, no. 1. URL: https://doi.org/10.1007/s10207-024-00959-0

21. Critical infrastructure autonomous defense / A. Al Maqousi et al. Advances in computational intelligence and robotics. 2025. P. 501–526. URL: https://doi.org/10.4018/979-8-3373-0954-5.ch017

22. Critical infrastructure systems of systems assessment methodology. / P. E. Sholander et al. US : Sandia National Laboratories, 2006. URL: https://doi.org/10.2172/899076

23. Kulugh V. E., Faki A. S., Onu E. Theoretical framework of cybersecurity resilience maturity assessment model for critical information infrastructure. Dutse journal of pure and applied sciences. 2025. Vol. 11, no. 1b. P. 75–85. URL: https://doi.org/10.4314/dujopas.v11i1b.9

24. Multi-aspect rule-based AI: methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures / I. H. Sarker et al. Internet of things. 2024. P. 101110. URL: https://doi.org/10.1016/j.iot.2024.101110

25. Thapaliya S., Bokani A. Leveraging artificial intelligence for enhanced cybersecurity: insights and innovations. Sadgamaya. 2024. Vol. 1, no. 1. P. 46–52. URL: https://doi.org/10.3126/sadgamaya.v1i1.66888

26. Kabanda G. Performance of Machine Learning and Big Data Analytics Paradigms in Cyber-security and Cloud Computing Platforms. *International Conference on Innovations in Computer and Information Science*, Ganzhou, China, 27–29 August 2021. 2021. URL: https://doi.org/10.5220/0010789900003167

27. Social Listening H., Data B., Apply in the Business Decision Process A. Machine Learningin FMCG. *Human Interaction and Emerging Technologies (IHIET-AI 2022) Artificial Intelligence and Future Applications*. 2022. URL: https://doi.org/10.54941/ahfe100920

28. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions / M. Ozkan-Ozay et al. *IEEE Access*. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3355547

29. Sarker I. H. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*. 2022. URL: https://doi.org/10.1007/s40745-022-00444-2

30. M. Hesham, M. Essam, M. Bahaa, A. Mohamed, M. Gomaa, M. Hany, W. ElsersyEvaluating Predictive Models in Cybersecurity: A Comparative Analysis of Machine and Deep Learning Techniques for Threat Detection. MSA University. 2024. URL: https://doi.org/10.48550/arXiv.2407.06014

31. Sarker I. H., Furhad M. H., Nowrozy R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*. 2021. Vol. 2, no. 3. URL: https://doi.org/10.1007/s42979-021-00557-0

32. Kurawle N. H. AI and Machine Learning for Enhanced Cybersecurity Defense: Challenges and Opportunities. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. 2025. Vol. 09, no. 06. P. 1–9. URL: https://doi.org/10.55041/ijsrem50694

33. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques / A. H. Salem et al. *Journal of Big Data*. 2024. Vol. 11, no. 1. URL: https://doi.org/10.1186/s40537-024-00957-y

34. Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research / Z. Zhang et al. *IEEE Access*. 2022. P. 1. URL: https://doi.org/10.1109/access.2022.3204051

35. Machine learning and AI for security mechanisms: A Systematic Literature Review Using a PRISMA Framework / H. Mambwe et al. *LatIA*. 2025. Vol. 3. P. 331. URL: https://doi.org/10.62486/latia2025331

36. Machine Learning and Deep Learning Approaches for CyberSecurity: A Review / A. Halbouni et al. *IEEE Access*. 2022. Vol. 10. P. 19572–19585. URL: https://doi.org/10.1109/access.2022.3151248

37. Ali S., Wang J., Leung V. C. M. AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms– A comprehensive review. *Information Fusion*. 2025. Vol. 118. P. 102922. URL: https://doi.org/10.1016/j.inffus.2024.102922

38. Dai D., Boroomand S. A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges. *Archives of Computational Methods in Engineering*. 2021. URL: https://doi.org/10.1007/s11831-021-09628-0

39. Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence / S. Ankalaki et al. *IEEE Access*. 2025. P. 1. URL: https://doi.org/10.1109/access.2025.3547433

40. Poluyan A., Purchina O., Fugarov D. Opportunities for Applying Artificial Intelligence by Commercial Organizations in Data Security and Cyber Threat

Monitoring. *International Journal of Basic and Applied Sciences*. 2025. Vol. 14, no. 2. P. 281–287. URL: https://doi.org/10.14419/bh5z5x68

41. Kaur R., Gabrijelčič D., Klobučar T. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*. 2023. P. 101804. URL: https://doi.org/10.1016/j.inffus.2023.101804

42. The Role of Machine Learning in Cybersecurity / G. Apruzzese et al. *Digital Threats: Research and Practice*. 2022. URL: https://doi.org/10.1145/3545574

43. Artificial intelligence maturity model: a systematic literature review / R. B. Sadiq et al. *PeerJ Computer Science*. 2021. Vol. 7. P. e661. URL: https://doi.org/10.7717/peerj-cs.661

44. Huang D., Zhan Y., Lonsdale C. Utilising Artificial Intelligence to Enhance Firm Circular Economy Maturity: A Thematic Review via Machine Learning. *Business Strategy and the Environment*. 2025. URL: https://doi.org/10.1002/bse.4291

45. Artificial Intelligence and Machine Learning for Maturity Evaluation and Model Validation / T. Hanne et al. *ICEME 2022: 2022 13th International Conference on E-business, Management and Economics*, Beijing China. New York, NY, USA, 2022. URL: https://doi.org/10.1145/3556089.3556102

46. Romano S. P., Sperlì G., Vignali A. An NLP-based approach to assessing a company's maturity level in the digital era. *Expert Systems with Applications*. 2024. Vol. 252. P. 124292. URL: https://doi.org/10.1016/j.eswa.2024.124292

47. Proposing a maturity model for assessing Artificial Intelligence and Big data in the process industry / R. Fornasiero et al. *International Journal of Production Research*. 2024. P. 1–21. URL: https://doi.org/10.1080/00207543.2024.2372840

48. Establishment of a maturity model to assess the development of industrial AI in smart manufacturing / W. Chen et al. *Journal of Enterprise Information Management*. 2021. Ahead-of-print, ahead-of-print. URL: https://doi.org/10.1108/jeim-10-2020-0397

49. Development and Evaluation of a Maturity Model for AI Deployment Capability of Manufacturing Companies / M. Sonntag et al. *Information Systems Management*. 2024. P. 1–31. URL: https://doi.org/10.1080/10580530.2024.2319041

50. Systematic comparison of digital maturity assessment models / B. Cognet et al. *Journal of Industrial and Production Engineering*. 2023. P. 1–19. URL: https://doi.org/10.1080/21681015.2023.2242340

51. Reichl G., Gruenbichler R. MATURITY MODELS FOR THE USE OF ARTIFICIAL INTELLIGENCE IN ENTERPRISES: A LITERATURE REVIEW. *19th International Scientific Conference on Industrial Systems*. 2023. URL: https://doi.org/10.24867/is-2023-vp1.1-5_07341

52. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions / M. Ozkan-Ozay et al. *IEEE Access*. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3355547

53. Sarker I. H. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*. 2022. URL: https://doi.org/10.1007/s40745-022-00444-2

54. Sarker I. H., Furhad M. H., Nowrozy R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*. 2021. Vol. 2, no. 3. URL: https://doi.org/10.1007/s42979-021-00557-0

55. Kurawle N. H. AI and Machine Learning for Enhanced Cybersecurity Defense: Challenges and Opportunities. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. 2025. Vol. 09, no. 06. P. 1–9. URL: https://doi.org/10.55041/ijsrem50694

56. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques / A. H. Salem et al. *Journal of Big Data*. 2024. Vol. 11, no. 1. URL: https://doi.org/10.1186/s40537-024-00957-y

57. Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research / Z. Zhang et al. *IEEE Access*. 2022. P. 1. URL: https://doi.org/10.1109/access.2022.3204051

58. Machine Learning and Deep Learning Approaches for CyberSecurity: A Review / A. Halbouni et al. *IEEE Access*. 2022. Vol. 10. P. 19572–19585. URL: https://doi.org/10.1109/access.2022.3151248

59. Ali S., Wang J., Leung V. C. M. AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms– A comprehensive review. *Information Fusion*. 2025. Vol. 118. P. 102922. URL: https://doi.org/10.1016/j.inffus.2024.102922

60. Dai D., Boroomand S. A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges. *Archives of Computational Methods in Engineering*. 2021. URL: https://doi.org/10.1007/s11831-021-09628-0

61. Poluyan A., Purchina O., Fugarov D. Opportunities for Applying Artificial Intelligence by Commercial Organizations in Data Security and Cyber Threat Monitoring. *International Journal of Basic and Applied Sciences*. 2025. Vol. 14, no. 2. P. 281–287. URL: https://doi.org/10.14419/bh5z5x68

62. Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence / S. Ankalaki et al. *IEEE Access*. 2025. P. 1. URL: https://doi.org/10.1109/access.2025.3547433