ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Методи моделювання кіберзагроз та стратегій реагування для забезпечення високого рівня кібербезпеки»

на здобуття освітнього ступеня бакалавра
зі спеціальності *124 Системний аналіз*
(код, найменування спеціальності)
освітньо-професійної програми *Системний аналіз*
(назва)

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

(підпис) *Вероніка ОЛЬШЕВСЬКА*
Ім'я, ПРІЗВИЩЕ здобувача

Виконав: здобувачка вищої освіти гр.САД-41
Вероніка ОЛЬШЕВСЬКА
Ім'я, ПРІЗВИЩЕ
Керівник: к.ф-м.н., Ровіл НАФЄЄВ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Інформаційних систем та технологій
Ступінь вищої освіти бакалавр
Спеціальність 124 Системний аналіз
Освітньо-професійна прорама Системний аналіз

ЗАТВЕРДЖУЮ
Завідувач кафедри ІСТ
_____ Каміла СТОРЧАК

"____" _____2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ольшевська Вероніка Віталіївна
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: «Методи моделювання кіберзагроз та стратегій реагування для забезпечення високого рівня кібербезпеки»
керівник кваліфікаційної роботи: Ровіл НАФЄЄВ, к.ф.-м.н
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025 р. № 56

2. Строк подання кваліфікаційної роботи «30» травня 2025 р.

3. Вихідні дані кваліфікаційної роботи:
3.1 Сучасні методи класифікації та моделювання кіберзагроз.
3.2 Підходи до оцінки ризиків кібербезпеки та управління інцидентами.
3.3 Технології машинного навчання та аномаліє-орієнтованого виявлення атак.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1 Теоретико-методологічні засади моделювання кіберзагроз.
4.2 Дослідження методів виявлення та моделювання кіберзагроз.
4.3 Аналіз стратегій реагування та забезпечення кіберстійкості.

5.Перелік ілюстраційного матеріалу: презентація

6. Дата видачі завдання «24» лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір технічної літератури	24.02-03.03.25	Виконано
2.	Теоретико-методологічні засади моделювання кіберзагроз	04.03-17.03.25	Виконано
3.	Дослідження методів виявлення та моделювання кіберзагроз	18.03-31.03.25	Виконано
4.	Аналіз стратегій реагування та забезпечення кіберстійкості	01.04-24.04.25	Виконано
5.	Висновки по роботі	25.04-16.05.25	Виконано
6.	Розробка демонстраційних матеріалів, доповідь.	19.05-20.05.25	Виконано
7.	Оформлення бакалаврської роботи	21.05-30.05.25	Виконано

Здобувачка вищої освіти _____ Вероніка ОЛЬШЕВСЬКА
(підпис) *(ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ровіл НАФЄЄВ
(підпис) *(ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття ступня бакалавр: 60 стор., 5 рис., 16 табл., 59 джерел.

Мета роботи – формування системного уявлення про методи моделювання кіберзагроз і побудову ефективних стратегій реагування для забезпечення стійкості та високого рівня кібербезпеки інформаційних систем.

Об'єкт дослідження – процеси формування, розвитку та нейтралізації кіберзагроз у сучасних інформаційних системах.

Предмет дослідження – методи моделювання кіберзагроз і стратегії реагування, спрямовані на забезпечення ефективного рівня кіберстійкості.

Короткий зміст роботи. У кваліфікаційній роботі проведено комплексний аналіз сучасних підходів до моделювання кіберзагроз та розробки стратегій реагування. Досліджено теоретико-методологічні засади моделювання кіберзагроз, включаючи їх класифікацію та сучасні моделі оцінки ризиків. Проаналізовано методи виявлення кіберзагроз, зокрема аномаліє-орієнтовані підходи, застосування машинного навчання та побудову сценаріїв загроз на основі атака-графів. Розглянуто стратегії реагування та забезпечення кіберстійкості, включаючи моделі реагування на інциденти, формування адаптивних стратегій протидії та оцінку ефективності систем кібербезпеки.

КЛЮЧОВІ СЛОВА: КІБЕРЗАГРОЗИ, МОДЕЛЮВАННЯ ЗАГРОЗ, КІБЕРБЕЗПЕКА, МАШИННЕ НАВЧАННЯ, АТАКА-ГРАФИ, СТРАТЕГІЇ РЕАГУВАННЯ, АДАПТИВНИЙ ЗАХИСТ, АНОМАЛІЄ-ОРІЄНТОВАНІ МЕТОДИ, КІБЕРСТІЙКІСТЬ.

ЗМІСТ

ВСТУП 8
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ 11
1.1. Поняття та класифікація кіберзагроз 11
1.2. Методологічні підходи до моделювання загроз у кіберпросторі 18
1.3. Огляд сучасних моделей оцінки ризиків кібербезпеки 23
РОЗДІЛ 2. МЕТОДИ ВИЯВЛЕННЯ ТА МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ. 29
2.1. Аномаліє-орієнтовані методи виявлення атак 29
2.2. Використання машинного навчання у моделюванні кіберзагроз 37
2.3. Побудова сценаріїв загроз на основі атака-графів 43
РОЗДІЛ 3. СТРАТЕГІЇ РЕАГУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ 52
3.1. Моделі реагування на інциденти у системах кіберзахисту 52
3.2. Формування адаптивних стратегій протидії кіберзагрозам 57
3.3. Оцінка ефективності та стійкості систем кібербезпеки 62
ВИСНОВКИ 67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 71
ДОДАТКИ 77
ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ(ПРЕЗЕНТАЦІЯ)……79

ВСТУП

Актуальність теми полягає в тому, що з розвитком інформаційних технологій кіберпростір перетворився на критичне середовище, уразливе до широкого спектра загроз, які можуть мати суттєві наслідки як для окремих організацій, так і для національної безпеки загалом. Деструктивна активність у мережевому середовищі дедалі частіше має ознаки системних, цілеспрямованих впливів, які ґрунтуються на використанні штучного інтелекту, автоматизованих інструментів та складної координації. У відповідь на це виникає потреба в науково обґрунтованих підходах до ідентифікації, моделювання та передбачення кіберзагроз, в ефективних стратегіях реагування, що забезпечують кіберстійкість інформаційних систем. Забезпечення високого рівня кібербезпеки неможливе без системного застосування аналітичних методів, які дають змогу виявляти потенційні вектори атак та оцінювати ризики, будувати сценарії загроз та адаптувати захисні механізми до умов динамічного середовища.

У цьому контексті особливої актуальності набуває вивчення сучасних моделей оцінювання ризиків, алгоритмів поведінки шкідливих об’єктів, механізмів прогнозування та адаптації. Інтеграція таких методів у системи прийняття рішень дає змогу зменшити ймовірність реалізації загроз та мінімізувати наслідки їхнього впливу. Зростає значущість технологій штучного інтелекту, машинного навчання, для побудови поведінкових моделей зловмисників, автоматичного виявлення аномалій і формування сценаріїв реагування. Поглиблене дослідження методів моделювання кіберзагроз та розроблення стратегій кіберзахисту дозволяє формалізувати підходи до оцінювання безпеки та побудови адаптивних, контекстно чутливих стратегій реагування, що є необхідною умовою функціонування будь-якої критичної інфраструктури у цифрову епоху.

Інформаційна база дослідження охоплює наукові публікації у сфері кібербезпеки, результати прикладних досліджень у галузі моделювання кіберзагроз, відкриті звіти спеціалізованих аналітичних центрів (ENISA, NIST, MITRE), міжнародні стандарти, дані емпіричних досліджень з реальних кейсів інцидентів інформаційної безпеки.

Мета кваліфікаційної роботи полягає у формуванні системного уявлення про методи моделювання кіберзагроз і побудову ефективних стратегій реагування для забезпечення стійкості та високого рівня кібербезпеки інформаційних систем.

Завдання роботи:

- Проаналізувати поняття кіберзагроз та провести їх класифікацію відповідно до сучасних підходів;
- Дослідити основні методологічні підходи до моделювання загроз у кіберпросторі;
- Здійснити огляд сучасних моделей оцінки ризиків кібербезпеки;
- Розглянути методи виявлення атак, що базуються на аналізі аномалій;
- Вивчити застосування алгоритмів машинного навчання у контексті моделювання кіберзагроз;
- Охарактеризувати підхід побудови сценаріїв загроз із використанням атака-графів;
- Проаналізувати моделі реагування на інциденти у системах кіберзахисту;
- Обґрунтувати формування адаптивних стратегій протидії кіберзагрозам;
- Запропонувати підхід до оцінки ефективності та стійкості систем кібербезпеки.

Об’єкт дослідження кваліфікаційної роботи — процеси формування, розвитку та нейтралізації кіберзагроз у сучасних інформаційних системах.

Предмет дослідження кваліфікаційної роботи — методи моделювання кіберзагроз і стратегії реагування, спрямовані на забезпечення високого рівня кіберстійкості.

Методи дослідження включають структурно-функціональний аналіз, методи системного підходу, логіко-семантичне моделювання, статистичний аналіз даних, побудову графів атак, елементи машинного навчання для класифікації та прогнозування загроз.

Практичне значення одержаних результатів полягає у можливості використання сформульованих підходів для розробки адаптивних систем кіберзахисту, що здатні ефективно реагувати на зміну умов у кіберпросторі та підвищувати загальний рівень кібербезпеки організацій.

Структура кваліфікаційної роботи складається зі вступу, трьох розділів основної частини, висновків, списку використаних джерел і додатків. У першому розділі розглядаються теоретико-методологічні основи моделювання кіберзагроз. Другий розділ присвячено аналізу методів виявлення й побудови моделей загроз. Третій розділ містить опис стратегій реагування та підходів до забезпечення кіберстійкості.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ

1.1. Поняття та класифікація кіберзагроз

Поняття кіберзагрози належить до категорії фундаментальних у сфері інформаційної безпеки та має складну багаторівневу структуру, що охоплює технічні, поведінкові, правові та організаційні компоненти. В умовах інтенсивної цифровізації діяльності більшості суспільних інститутів постала необхідність у точному концептуальному визначенні загроз, що виникають у кіберпросторі, з урахуванням їх еволюційного характеру та потенційної шкоди. Василенко М.Д. визначає кіберзагрозу як усвідомлену чи випадкову дію в інформаційно-телекомунікаційному середовищі, яка здатна порушити цілісність, конфіденційність або доступність інформаційних ресурсів [1, с. 26].

У сучасних умовах класифікація кіберзагроз дедалі частіше базується на технічних параметрах та на оцінці мотивації суб’єктів, які їх генерують. Окреслений метод відкриває можливості для побудови моделей поведінки зловмисників, що дозволяє своєчасно ідентифікувати патерни дій, притаманні окремим групам атакуючих. Агресивні кампанії з політичним або ідеологічним забарвленням мають виражений сценарний профіль: вони використовують символічні цілі, впроваджують атаки в критичні моменти соціальної нестабільності та супроводжуються інформаційними вкидами. Тоді як комерційно вмотивовані загрози тяжіють до мінімізації слідів, точковості та швидкої монетизації компрометованих ресурсів.

Змістовне розкриття поняття кіберзагрози передбачає врахування кількох критично важливих аспектів: наявності джерела загрози, цільового об’єкта, вектора впливу та засобів реалізації. Як зазначають Довгань О., Литвинова Л. і Дорогих С., кіберзагроза формується у взаємозв’язку між намірами суб’єкта атаки, ступенем уразливості системи та технічними засобами впливу [2, с. 55]. Отже, визначення кіберзагрози не може бути

обмеже технічним аспектом; воно має охоплювати комплекс передумов, які спільно утворюють можливість негативного втручання.

Дослідники сходяться на думці, що загроза в кіберпросторі завжди постає як латентна можливість реалізації шкідливого впливу, незалежно від того, була вона активована чи ні. Пістунов І.М. і Кочура Є.В. акцентують, що кіберзагроза може існувати як у формі виявленого вразливого модуля системи, так і у вигляді змодельованого сценарію атаки, що ще не відбувся, але має потенціал до реалізації [4, с. 18].

У теоретичному дискурсі важливо виокремити відмінність між термінами «загроза», «ризик» та «атака». Загроза становить собою можливість нанесення шкоди, незалежно від фактичної реалізації, тоді як ризик характеризує ймовірність реалізації цієї загрози з певними наслідками, а атака є вже здійсненим актом впливу на систему. Головкін Б.М. зазначає, що саме диференціація цих понять є ключовою умовою формування ефективної системи управління кібербезпекою, оскільки дозволяє виділити етапи прогнозування, запобігання та реагування [3, с. 66]. У зв’язку з цим запропоновано узагальнену типологізацію підходів до визначення кіберзагроз, яка представлена в таблиці 1.1.

Таблиця 1.1

Основні підходи до теоретичного визначення кіберзагроз

Підхід	Ключові характеристики
Технократичний	Орієнтація на вразливості ПЗ, мережеву активність, сигнатури
Системно-поведінковий	Аналіз взаємодії між об'єктами, користувачами та середовищем
Юридико-нормативний	Інтерпретація загроз через призму правових наслідків та норм
Організаційно-функціональний	Розгляд загроз у контексті управління ризиками й стратегіями
Геополітичний	Кіберзагроза як інструмент протидії між державними суб’єктами

Джерело: складено на основі [5; 6]

Теоретичне підґрунтя дослідження кіберзагроз неможливе без урахування категоріального апарату, до якого входять терміни, як «інцидент»,

«вразливість», «експлойт» та «зловмисник». Кожне з цих понять має своє функціональне значення у контексті аналізу загроз. Інцидент передбачає вже відбутий факт порушення безпеки, тоді як вразливість — лише технічну або логічну слабкість системи. У свою чергу, зловмисник як суб'єкт впливу може бути внутрішнім або зовнішнім, організованим або ізольованим, що безпосередньо впливає на вибір стратегій моделювання загроз. Формалізація таких понять у методологічному дискурсі сприяє створенню цілісної аналітичної системи безпеки.

Поняття «кіберзагроза» є багатофакторним, включає як суто технічні, так і соціально-поведінкові та нормативні аспекти, і має розглядатися не ізольовано, а в контексті взаємодії між технологічною платформою, користувачем і середовищем ризику. Міждисциплінарний підхід забезпечує необхідну повноту аналізу та створює підґрунтя для побудови ефективних моделей виявлення, класифікації та нейтралізації загроз.

Особливе значення у контексті понятійного аналізу має принцип сценарності загроз. Ідея полягає в тому, що кожна потенційна загроза має розгортатися як певний сценарій — з початковою умовою, тригером, механізмом реалізації та очікуваними наслідками. Сценарний підхід дає змогу аналізувати загрозу як абстракцію та формалізувати її в рамках математичних, логічних або імітаційних моделей. Як стверджує Луцик В.В., системна реалізація сценарного підходу дозволяє проводити прогнозування ризиків на етапі проєктування інфраструктури [3, с. 144].

У сучасній науці набуває значення інтегральне трактування кіберзагроз як системної характеристики середовища, що проявляється у змінності рівня безпеки під впливом внутрішніх і зовнішніх факторів. Відповідний підхід базується на припущенні, що загроза — не ізольований елемент, а інтерактивний процес, що виникає внаслідок взаємодії між множиною об'єктів, процесів та умов.

Проблематика класифікації кіберзагроз набуває дедалі більшого значення в умовах цифрової трансформації ключових сфер економіки та

публічного управління. Внаслідок активного впровадження електронної комерції, хмарних технологій, блокчейн-інфраструктур і автоматизованих систем управління, зростає складність кіберпростору, а отже — і різноманіття потенційних загроз. Романюк П. зазначає, що в умовах багатофакторної цифровізації підвищується ризик виникнення нових типів уразливостей, пов’язаних не стільки з програмними помилками, скільки з логікою бізнес-процесів і міжсистемною взаємодією [5, с. 34]. Зумовлює необхідність побудови класифікаційної моделі, яка б охоплювала як традиційні технічні ризики, так і сучасні концептуальні загрози.

У структурі прикладних систем кіберзахисту класифікація кіберзагроз повинна враховувати рівень впливу на об’єкти цифрової економіки, перш за все на транзакційні системи, обробку персональних даних, сервіси електронної ідентифікації. Як підкреслюють Садчикова І., Тарасенко А. та Дубина М., у межах електронної комерції спостерігається тенденція до зростання комбінованих загроз, що поєднують методи фішингу, соціальної інженерії та атак на канали зв’язку [6]. Наявні виклики для систем виявлення, які повинні бути реактивними та проактивними — здатними ідентифікувати загрозу ще до її безпосереднього прояву. Класифікація має інтегрувати параметри, як рівень передбачуваності загрози, її часовий горизонт, інтенсивність впливу та наявність поведінкових маркерів.

Системи автоматизованого аналізу загроз у межах кіберінфраструктури можуть інтегрувати класифікаційні схеми у власні алгоритми роботи. Завдяки цьому, програмні агенти здатні проводити самостійну оцінку типу виявленої аномалії, співвідносити її з визначеним класом загроз і запускати відповідні протоколи реагування. Можливоа зменшити навантаження на аналітиків безпеки, забезпечити швидкість прийняття рішень і сформувати наскрізну логіку “виявлення — класифікація — реакція”. Для реалізації подібної інтеграції необхідно, щоб класифікація була формалізованою, уніфікованою, чітко структурованою та взаємозв’язаною з інформаційними потоками у межах організації.

Важливо враховувати, що класифікація кіберзагроз не є самодостатньою метою — вона є проміжним етапом у більш загальному циклі керування ризиками. Її ефективність вимірюється не кількістю класів чи рівнем деталізації, а здатністю забезпечити підвищення оперативності й точності захисних рішень. У цьому сенсі занадто складні класифікаційні системи можуть стати непридатними для використання у стресових умовах, коли рішення мають прийматись негайно. Оптимальною вважається така структура, яка балансує між глибиною аналітичної обробки та швидкістю доступу до релевантної інформації, забезпечуючи гнучкість у залежності від обраної моделі захисту.

Особливу складність у класифікації становлять загрози, що змінюють свою поведінку відповідно до реакції цільової системи. Така поведінкова пластичність характерна для новітніх типів зловмисного ПЗ та програм-агентів, які аналізують середовище виконання та активуються лише за певних умов. У цьому випадку класифікація має бути дескриптивною та передбачувальною: необхідно закладати потенціал трансформації загрози та її здатність переходити з однієї категорії в іншу.

Особливу увагу в сучасних підходах до класифікації слід приділяти типам атак, що використовують машинні та математичні моделі поведінки користувача. Шевченко С.М. у своїх дослідженнях наголошує на необхідності диференціації загроз за ознакою їхньої динамічної поведінки у часі, через використання фрактального аналізу та кластерних моделей [8, с. 33]. Класифікація дозволяє виявити атипові закономірності, що свідчать про підготовку атаки, навіть якщо на перший погляд дії зловмисника не порушують жодних політик доступу. Із цього випливає критерій класифікації — структурна непередбачуваність, яка визначає здатність системи виявити невідомий тип загрози, що відхиляється від звичних шаблонів.

Актуальним напрямом у класифікації є використання мережевої теорії та графових моделей, які дозволяють описувати кіберзагрози як сукупність взаємопов’язаних подій, що формують сценарії вторгнення. Шевченко С.М.,

Жданова Ю.Д. та інші дослідники доводять ефективність застосування графових структур для аналізу складних, багатоступеневих атак, де кожен вузол графа відповідає за певний етап проникнення, а ребра — за логічні або часові зв'язки між ними [9, с. 135]. У цьому контексті стає можливим виокремлення типів загроз за такими характеристиками, як глибина проникнення, кількість етапів, рівень прихованості та взаємозв'язаність з іншими атаками. У таблиці 1.2. представлено класифікаці. схему, яка охоплює ключові типи загроз у цифровому середовищі та їх відповідність сценаріям моделювання.

Таблиця 1.2.

Модульна класифікація кіберзагроз у цифрових інформаційних системах

Критерій	Типи загроз	Опис / Приклади
Поведінкова структура	Лінійні / Стохастичні / Фрактальні	Простий скрипт / Випадкові мутації / Складні коливання
Сценарна глибина	Одноетапні / Багатоступеневі	Сканування порту / Ланцюгова атака (APT)
Геометрія впливу	Централізовані / Децентралізовані	Атака з однієї IP / Botnet з тисяч машин
Темпоральна характеристика	Разові / Постійні / Сплячі	Одноразовий злам / Постійна присутність / Затримка запуску
Інформаційний вектор	Дані / Метадані / Комунікації	Крадіжка ПІБ / Моніторинг листування / Злом API

Джерело: складено на основі [12]

Суттєвий вплив на класифікаційний підхід мають математичні методи виявлення аномалій, що реалізуються у форматі машинного навчання. Шевченко С.М. у співавторстві з колегами пропонує інтегрувати у класифікацію ознаку «кластерної належності загрози», яка визначається за результатами аналізу логів, трафіку або подій в інформаційній системі [7, с. 261]. Замість статичного поділу загроз можлива побудова динамічної карти кластерів загроз, де кожен кластер відповідає за тип поведінки зловмисника.

Окремим вектором класифікації виступає контекст реалізації загрози. Йдеться про те, що загроза має різний рівень критичності залежно від середовища, у якому вона проявляється: для банківської системи атака на

протокол аутентифікації матиме інший рівень ризику, ніж для державного реєстру чи системи дистанційного навчання. Як наголошує Романюк П., класифікація повинна бути чутливою до галузевої специфіки, регуляторних вимог і рівня довіри до системи [5, с. 36].

Загрози, що проявляються у вигляді «ланцюгових» атак або вторгнень із багатоетапною архітектурою, потребують окремого класифікаційного підходу. У таких випадках загроза не може бути коректно віднесена до одного класу, оскільки її реалізація охоплює одразу кілька типів дій: сканування, фішинг, проникнення, підвищення привілеїв, встановлення бекдорів, видалення слідів, ексфільтрацію. Кожна з цих фаз може бути типологізована окремо, проте у комплексі загроза набуває системного характеру. Розв’язанням цієї проблеми є модульна класифікація, де загроза описується як сукупність структурних компонентів, кожен з яких ідентифікується та аналізується в контексті загального сценарію.

У системах кіберзахисту нового покоління дедалі більшого значення набувають методи ситуаційної обізнаності, в межах яких класифікація кіберзагроз розглядається як частина загальної картини кіберсередовища. Мета такої моделі — забезпечити аналітику поточного стану системи та потенційних змін загрозового фону. У цьому підході класифікація виконує функцію джерела для генерації гіпотез, формування очікувань щодо дій супротивника та побудови проактивних стратегій.

Отже, класифікація кіберзагроз має бути таксономічним інструментом та функціональним елементом системи управління ризиками. Її ефективність визначається здатністю адаптуватися до змін середовища, інтегрувати сучасні методи виявлення, ураховувати специфіку загроз для різних галузей і забезпечувати підґрунтя для прийняття обґрунтованих рішень у сфері кіберзахисту. В умовах стрімкого розвитку штучного інтелекту та автономних систем критичне значення має побудова гнучких, аналітично насичених класифікаційних моделей, що можуть бути інтегровані у контури автоматизованого реагування на кіберінциденти.

1.2. Методологічні підходи до моделювання загроз у кіберпросторі

Методологічна основа моделювання кіберзагроз охоплює широкий спектр наукових та прикладних підходів, які спрямовані на аналіз можливих сценаріїв шкідливого впливу в кіберпросторі, їхню структуризацію, прогнозування та визначення потенційної шкоди. Ефективне моделювання є ключовим етапом у створенні системи управління ризиками, оскільки дозволяє формувати проактивні стратегії реагування, адаптивні алгоритми протидії, ресурсоорієнтовані заходи щодо локалізації інцидентів. Як підкреслює Лисенко Н.О., одним з головних завдань моделювання є опис уже відомих загроз та виявлення нових типів атак, які ще не були зафіксовані, але мають високий потенціал до реалізації [13, с. 92].

Суттєвим доповненням до формальних моделей загроз є концепція багаторівневого моделювання, в основі якої лежить ідея одночасного аналізу загроз на стратегічному, тактичному й операційному рівнях. Стратегічний рівень охоплює макроскопічне бачення системи кіберзахисту: аналіз загальної архітектури, виявлення вразливих зон, оцінку системних залежностей. Тактичний рівень фокусується на конкретних підсистемах, їх конфігураціях, політиках доступу та взаємодії. Операційний рівень стосується подій у реальному часі — мережевого трафіку, логів, активності користувачів.

Іншою важливою методологічною категорією є принцип контекстної релевантності, згідно з яким моделювання загрози повинно враховувати конкретні умови, у яких функціонує інформаційна система. Одна й та сама вразливість може мати різний рівень критичності залежно від ролі системи, її призначення, часу доби, географічного розташування або навіть сезону. Наприклад, атака на фінансову систему перед завершенням банківського дня несе значно більший ризик, ніж у період низького навантаження. Відповідно, методи моделювання повинні мати змінні компоненти, які автоматично адаптуються до змін контексту в реальному часі.

Ключовим напрямом моделювання є побудова формальних описів загроз з використанням математичних структур. Йдеться про логіко-математичні моделі, які описують послідовність дій зловмисника, правила переходів між станами інформаційної системи та обмеження, які накладаються політиками безпеки. Лаптєв О.А., Степаненко В.І. та Тихонов Ю.О. наголошують, що застосування дискретних структур, таких як скінченні автомати, графи станів та логічні формули, дозволяє досягти високої точності в описі поведінкових шаблонів атак [14, с. 60]. Формалізація загроз у відповідний спосіб дає змогу верифікувати моделі.

Окреслені сценарії можуть мати як лінійний, так і розгалужений характер, що відображає альтернативні варіанти розвитку подій. Гвоздьов Р.Ю. та Олійников Р.В. зазначають, що для реалізації сценарного підходу доцільно використовувати дерево рішень, графи залежностей та об'єктно-орієнтовані моделі, які відображають технічні аспекти та поведінкові та організаційні особливості кіберзагроз [18, с. 93]. Основні характеристики та переваги методів сценарного моделювання наведено в таблиці 1.3.

Таблиця 1.3

Основні методи сценарного моделювання кіберзагроз

Метод	Характеристика	Переваги застосування
Графи атак	Мережа логічно пов’язаних станів, що описує послідовність дій	Візуалізація шляху атаки, ефективність у складних системах
Дерева рішень	Модель з варіативними переходами на основі умов реалізації загроз	Аналіз альтернативних сценаріїв та вибір оптимальної реакції
Петрі-мережі	Формальна модель для опису паралельних і асинхронних процесів	Точне моделювання взаємодії між компонентами системи
Об'єктно-орієнтовані моделі	Моделі на основі класів загроз і об’єктів атаки	Масштабованість, можливість повторного використання
Імітаційне моделювання	Відтворення поведінки системи за допомогою чисельних експериментів	Висока реалістичність, здатність моделювати невизначеність

Джерело: складено на основі [14]

У межах сучасної парадигми кіберзахисту важливе значення має застосування імітаційного моделювання, яке дозволяє відтворити процес

розвитку загрози в умовах максимально наближених до реального функціонування системи. Цей підхід особливо ефективний для складних, багатокомпонентних інфраструктур, де взаємодія між елементами не може бути адекватно описана лише аналітичними методами. Тишик І.Я. підкреслює, що імітаційні моделі здатні виявляти вторинні ефекти впливу загроз, та навіть ті, що проявляються лише при поєднанні певних чинників, і тому їх виявлення неможливе через класичні інструменти [15, с. 219]. Особливо актуальним цей підхід є для тестування систем реагування, резервного копіювання та процедур ескалації в умовах кіберінцидентів.

Головним напрямом є використання метричних моделей, які дозволяють оцінити ступінь ризику, рівень загрози та ефективність захисту за допомогою кількісних показників. Моделі базуються на статистичних даних про інциденти, частоту експлуатації вразливостей, час реакції системи та інші параметри. Бєгун А.В. акцентує увагу на важливості побудови нормованих шкал загроз, які дозволяють уніфікувати результати аналізу і приймати рішення на основі порівнянних даних [17, с. 143]. Метричні підходи дозволяють класифікувати загрози та ранжувати їх за критичністю, що є основою для формування пріоритетів у політиці безпеки.

У процесі розроблення моделей кіберзагроз вагоме значення має поняття часової еластичності. Йдеться про врахування того, як загроза може змінювати інтенсивність або форму залежно від часу впливу. Деякі типи атак можуть бути ефективними лише у перші хвилини після ініціації вразливості, інші — навпаки, передбачають довготривале перебування в системі без виявлення. Моделі, які враховують час як ключову змінну, дають змогу будувати графіки ризику, визначати оптимальні моменти для втручання та тестувати сценарії відкладеного реагування.

У методології моделювання є інтероперабельність моделей загроз між різними платформами, підсистемами та організаціями. У багатьох випадках інформаційні системи мають різні технологічні стеки, протоколи обміну та механізми логування. Ефективне моделювання повинно враховувати ці

відмінності, забезпечуючи сумісність структур даних, форматів опису атак і механізмів взаємодії. Особливо важливо у випадках міжвідомчої кооперації, створення національних платформ реагування та спільних хмарних інфраструктур. Уніфіковані методології моделювання дають змогу забезпечити консистентність, оперативність і достовірність обміну інформацією про кіберзагрози між суб'єктами.

Формалізовані методи моделювання широко використовуються у контексті верифікації політик безпеки та автоматизованого генерування правил для систем виявлення вторгнень. Використання логіки предикатів, булевих виразів та аксіоматичних систем дозволяє описати допустимі та недопустимі стани системи у формалізованому вигляді. Лаптєв О.А. підкреслює, що підходи дозволяють здійснювати верифікацію відповідності системи заданим правилам та дають змогу автоматично генерувати сигнатури для IDS/IPS-систем [14, с. 61].

Перспективним напрямом є інтеграція моделей загроз у так звані цифрові двійники інформаційних систем, що дає змогу в режимі реального часу відтворювати стан інфраструктури та імітувати поведінку в умовах впливу загроз. Лисенко Н.О. зазначає, що цифрові двійники, які враховують параметри навантаження, топологію мережі, рівень доступу та інші змінні, дозволяють прогнозувати потенційні вектори атаки ще до їх реалізації [13, с. 99]. У поєднанні з технологіями машинного навчання цифрові моделі стають важливою складовою адаптивної системи безпеки, яка реагує та активно передбачає поведінку супротивника.

Методологія моделювання має враховувати й так звану «когнітивну складову загроз», пов'язану з маніпулюванням користувачем, поширенням дезінформації, фішинговими кампаніями та атаками соціального характеру. У таких випадках шкідливий вплив реалізується не через технічну вразливість, а через когнітивну слабкість — довіру до повідомлення, неуважність, звичку реагувати на зовнішні сигнали. Моделі, які враховують цю складову, повинні включати поведінкові шаблони, соціальні сценарії та лінгвістичний аналіз.

Вони мають бути гнучкими до культурних, професійних, демографічних змін серед користувачів, і водночас чутливими до тонких відхилень у поведінці.

Ефективним є побудова моделей з елементами самонавчання, які можуть самостійно адаптувати свої параметри під час функціонування. Моделі є частиною класу адаптивних систем, що включають еволюційні алгоритми, нейронні мережі та reinforcement learning. Вони не потребують постійного ручного оновлення й здатні виявляти нові загрози на основі відхилень від звичних патернів.

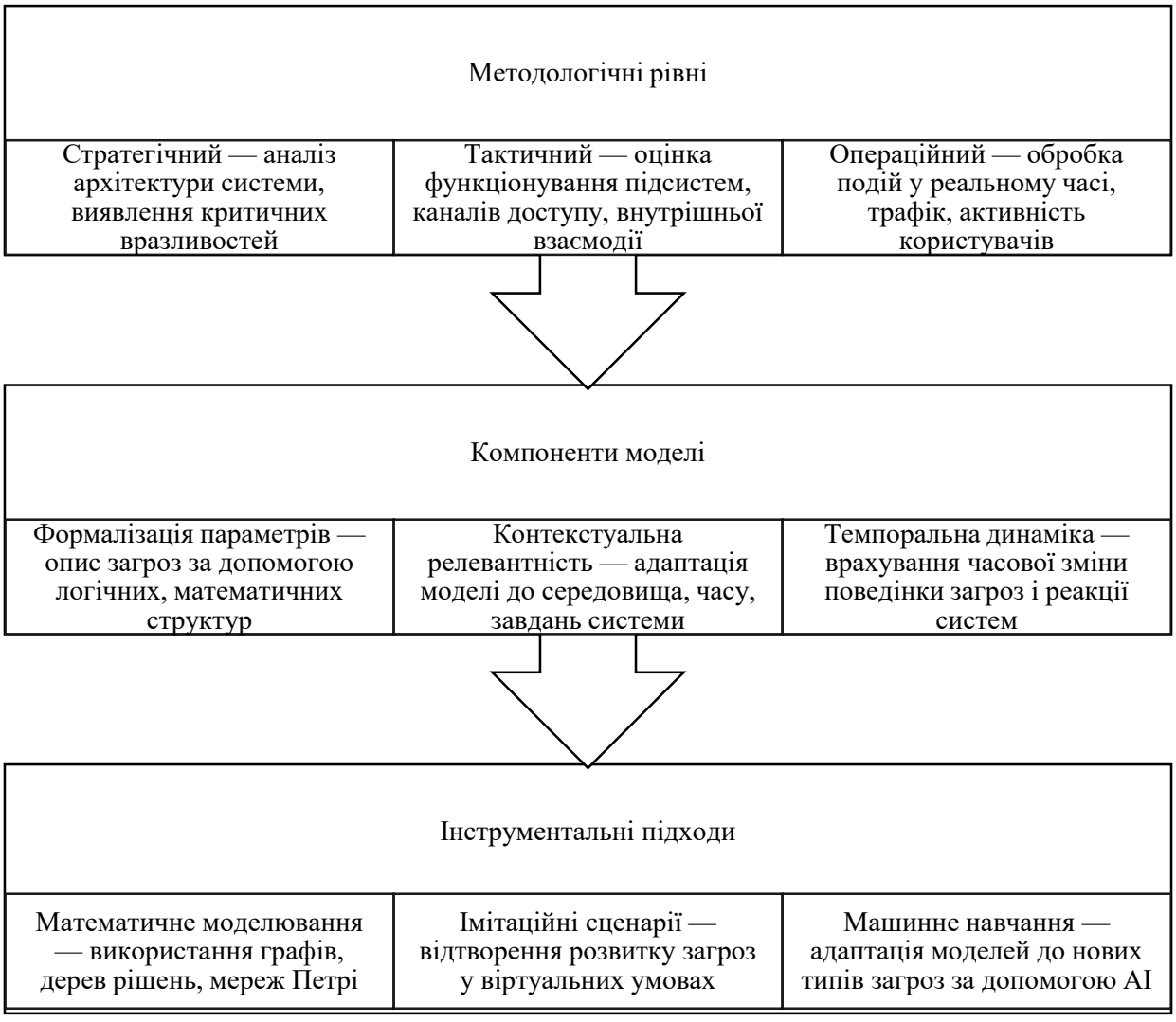

Рисунок 1.1. Структурна модель методологічного підходу до моделювання кіберзагроз

Джерело: складено на основі [11]

Методологія моделювання загроз повинна враховувати технічну реалізацію та правовий, організаційний та людський аспекти, оскільки більшість атак розгортаються у межах складної взаємодії між людьми та системами. Баранов О.А. наголошує, що формальні моделі мають бути доповнені семіотичним аналізом, який дозволяє вивчати комунікативні елементи загроз: соціотехнічні атаки, фішинг, маніпуляцію контентом [16, с. 59].

Загалом, методологічні підходи до моделювання кіберзагроз є багатокомпонентною системою, що поєднує формальні математичні методи, імітаційне моделювання, сценарні побудови та інтелектуальні алгоритми аналізу. Їх ефективне застосування забезпечує можливість оперативного виявлення, оцінки та прогнозування кіберризиків, що, у свою чергу, формує надійне підґрунтя для побудови стійких та адаптивних систем інформаційної безпеки. В умовах зростання складності цифрового середовища інтеграція кількох моделей у єдиний аналітичний контур є необхідною умовою для досягнення високого рівня кіберзахисту.

1.3. Огляд сучасних моделей оцінки ризиків кібербезпеки

Сучасні цифрові середовища характеризуються високим ступенем взаємозалежності, що ускладнює виявлення первинних джерел загроз і масштабування їхнього впливу. Ризик у цьому контексті розглядається як функція від імовірності реалізації кіберзагрози та очікуваних наслідків для критичних активів. Для адекватної оцінки такого ризику необхідно залучати технічні параметри та організаційні, поведінкові та правові змінні. Комплексність підходу до моделювання дозволяє виявляти вразливі точки та прораховувати економічну та операційну доцільність захисних заходів.

Однією з базових парадигм оцінювання ризиків є концепція CVSS (Common Vulnerability Scoring System), яка дає змогу присвоювати кожній вразливості числову оцінку за такими критеріями, як складність експлуатації,

вплив на цілісність, конфіденційність і доступність, наявність способів усунення. Попри популярність, CVSS критикують за обмежену гнучкість та ізоляцію від конкретного контексту, в якому реалізується загроза. У відповідь на ці обмеження з'являються моделі нового покоління, що поєднують статистичні, імовірнісні та алгоритмічні підходи для створення динамічної картини ризиків у реальному часі.

Значне поширення отримали методи, що поєднують сценарне моделювання з індикаторно-метричними оцінками. Лісовська Ю.П. підкреслює важливість формування інтегрованого показника ризику, який об'єднує ймовірнісну компоненту, економічні втрати, потенціал репутаційної шкоди та тривалість відновлення системи [27, с. 119]. У таблиці 1.1. подано порівняльний огляд сучасних моделей оцінки ризиків кібербезпеки, із зазначенням їхніх характеристик та практичної сфери застосування.

Таблиця 1.4.

Огляд сучасних моделей оцінки ризиків у сфері кібербезпеки

Назва моделі	Основні характеристики	Приклади застосування
CVSS	Статична шкала оцінювання вразливостей за фіксованими критеріями	Класифікація загроз у системах управління патчами
FAIR (Factor Analysis of Information Risk)	Кількісна оцінка інформаційного ризику з урахуванням фінансових наслідків	Аудит кіберстрахування
Bayesian Risk Assessment	Ймовірнісна модель із динамічним оновленням залежностей між подіями	Аналіз складних комбінованих атак
Risk Matrix	Таблична оцінка за шкалами імовірності та впливу	Побудова політик доступу
Fuzzy Logic-based Models	Нечіткі множини для оцінки ситуацій із високою невизначеністю	Анонімні атаки, недостатність даних
Attack Tree Quantification	Ієрархічна структура можливих шляхів атаки з розрахунком критичності	Проєктування систем безпеки

Джерело: складено на основі [18]

Когут Ю.І. зазначає, що сучасні організації активно впроваджують багатовимірні моделі оцінки ризику, які включають автоматизовану інвентаризацію цифрових активів, виявлення залежностей між системами та

розрахунок сценарного впливу потенційних атак [25, с. 191]. Вони часто базуються на логіко-математичних алгоритмах, баєсівському аналізі, дереві рішень та теорії нечітких множин. Дерево рішень дозволяє прораховувати альтернативні шляхи розвитку подій у разі впливу загрози, тоді як баєсівські мережі допомагають розраховувати ймовірність комбінацій атак з урахуванням множини змінних, які не є незалежними одна від одної.

В умовах гібридних загроз дедалі частіше використовуються композитні моделі, що поєднують у собі декілька підходів, адаптуючи методику під конкретну інфраструктуру. CVSS може виступати базовим рівнем оцінки технічних параметрів, тоді як модель на основі баєсівської мережі враховуватиме поведінкову складову, часові закономірності та вторинні ризики. Подібна інтеграція дозволяє будувати системи оцінювання, які не є жорстко зафіксованими, а навпаки — здатні до адаптації відповідно до змін умов середовища, стратегії захисту або навіть геополітичної ситуації.

Кормич Б.А. підкреслює, що для державного рівня оцінки ризиків кібербезпеки особливої ваги набувають методики, орієнтовані на прогнозування системного впливу атак — каскадного поширення порушень у критичних секторах [26, с. 287]. У цьому випадку класичні моделі ризиків потребують доповнення соціотехнічними змінними, які включають поведінку користувачів, етичні обмеження, динаміку прийняття рішень в умовах стресу.

Інтеграція моделей оцінки ризиків у процес прийняття рішень вимагає точності математичних розрахунків та зрозумілості результатів для управлінського персоналу. У зв’язку з цим формуються так звані візуальні панелі ризику (risk dashboards), які графічно представляють рівні загроз, динаміку змін, найбільш вразливі активи та зони критичності. Вони виконують роль інтерфейсу між технічними аналітиками і особами, що ухвалюють стратегічні рішення. Завдяки цьому забезпечується швидке розуміння пріоритетів, формування політики реагування і підтримка безперервного моніторингу.

У новітніх інформаційних системах все частіше реалізуються алгоритми автоматичного перерахунку ризику в режимі реального часу. Вони враховують нові події, зміни в архітектурі системи, результати сканування вразливостей, поведінкові дані користувачів. Якщо виявлено нову вразливість на сервері, рівень ризику автоматично підвищується, що запускає сценарії реакції без втручання людини. Алгоритми лежать в основі Zero Trust-архітектур, які передбачають постійну перевірку кожного компонента та адаптацію ризик-профілю відповідно до змінної поведінки системи.

Серед сучасних рішень, орієнтованих на оцінювання ризиків у кіберпросторі, особливу увагу привертає методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), розроблена SEI (Software Engineering Institute). Цей підхід поєднує технічні й організаційні аспекти управління ризиками, зосереджуючись на критично важливих активах та процесах. Особливість OCTAVE полягає в тому, що аналіз загроз та вразливостей виконується технічними фахівцями та керівниками підрозділів, що забезпечує комплексність розуміння ризиків у межах організації. Методика побудована на оцінці ймовірності, наслідків та рівня вразливості для кожного активу в контексті цілей бізнесу.

Іншим авторитетним фреймворком є NIST Risk Management Framework (RMF), який широко застосовується у державному секторі США та рекомендований до використання в міжнародній практиці. Він охоплює весь життєвий цикл системи: від категоризації активів і вибору заходів безпеки — до моніторингу залишкових ризиків. Основна перевага RMF — його гнучкість: модель дозволяє адаптувати рівень захисту залежно від типу організації, характеру даних та зовнішнього середовища. Модель працює у поєднанні з NIST SP 800-30 — документом, який містить методичні рекомендації щодо кількісного й якісного аналізу ризиків.

У секторі корпоративної безпеки великого поширення набула модель ISO/IEC 27005, яка є складовою частиною стандарту ISO/IEC 27000-серії. На відміну від більш технічних систем, ISO 27005 акцентує увагу на процесному

управлінні ризиками в межах інформаційної безпеки — формуванні політик, документації, періодичному перегляді рівня ризиків та інтеграції з іншими управлінськими стандартами (наприклад, ISO 31000). Вона не вимагає використання конкретних математичних моделей, але дозволяє їх інтегрувати залежно від контексту застосування.

Популярністю серед компаній, що працюють у сфері фінансових технологій, користується методологія MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), розроблена урядом Іспанії. Модель передбачає ієрархічну оцінку ризиків, де кожен компонент системи аналізується через призму впливу на конфіденційність, цілісність і доступність. MAGERIT тісно інтегрується з інструментом PILAR, який дозволяє автоматизувати процес побудови карти ризиків.

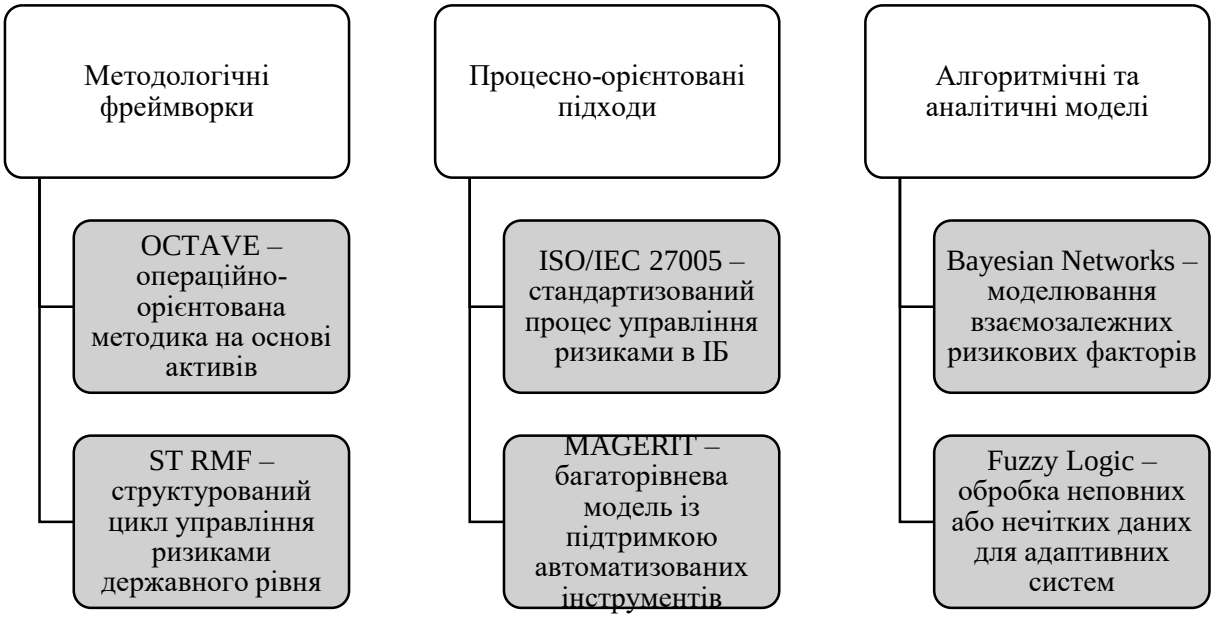

Рисунок 1.2. Основні напрями розвитку моделей оцінки ризиків кібербезпеки

Джерело: складено на основі [12]

Відчутне зростання ризиків у хмарних середовищах та розподілених системах спричинило розвиток моделей оцінки загроз, що враховують додаткові вектори атак — такі як порушення контролю доступу в

контейнеризованих середовищах, втрати даних у багатокористувацьких хмарах, атаки на API. У відповідь на ці виклики формуються domain-specific моделі: Cloud Risk Frameworks, які враховують властивості віртуалізованого простору, багаторівневої авторизації та сервісної орієнтації. У цих моделях оцінка ризику відбувається для конкретного активу та для взаємодії між сервісами та контексту їхнього виконання.

Значного розвитку набули методи, що застосовують ML-алгоритми для прогнозування ризиків — Random Forest, XGBoost, та Neural Network-архітектури. Моделі працюють на базі великих обсягів даних із систем моніторингу, журналів безпеки, поведінкових моделей користувачів. Вони здатні не просто оцінювати поточний ризик та передбачати майбутні вектори загроз, формуючи адаптивну карту ризику. Особливо ефективними ці алгоритми є в умовах непередбачуваних сценаріїв — наприклад, zero-day атак або кампаній соціальної інженерії зі змінною тактикою.

Загальною тенденцією розвитку моделей оцінки ризиків кібербезпеки є їх перехід від реактивного до проактивного характеру. Йдеться про створення систем, здатних виявляти латентні ознаки загрози, ще до її активної реалізації. Замість аналізу наслідків, фокус переноситься на аналіз намірів та запобігання аномальній поведінці. Важливою умовою для такого підходу є наявність високоякісних навчальних вибірок, адаптивних моделей оцінювання і тісної інтеграції з системами моніторингу в реальному часі. Саме тому моделі ризику стають інструментом аудиту та активним елементом системи кіберзахисту.

РОЗДІЛ 2. МЕТОДИ ВИЯВЛЕННЯ ТА МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ

2.1. Аномаліє-орієнтовані методи виявлення атак

Аномаліє-орієнтовані методи виявлення атак представляють клас підходів кіберзахисту, заснованих на ідентифікації відхилень від нормальної поведінки системи. На відміну від сигнатурних методів, вони здатні виявляти атаки нульового дня без попереднього опису їх шаблонів. Основний принцип функціонування полягає у створенні багатовимірного профілю нормальної мережевої активності за допомогою математичних моделей та алгоритмів машинного навчання. Суттєве відхилення від цього профілю класифікується як аномалія, що потенційно сигналізує про атаку. Ефективність даного підходу визначається точністю побудованої моделі, яка повинна враховувати динамічні характеристики інформаційної системи, сезонні коливання та легітимні зміни конфігурації або оновлення програмного забезпечення [45].

Технологічний процес аномаліє-орієнтованого виявлення включає чотири ключові етапи:

1) збір даних із множинних джерел (NetFlow, PCAP, системні журнали, логи додатків);

2) профілювання нормальної поведінки з використанням метрик на основі трафіку (пропускна здатність, розмір пакетів), часових рядів (інтервали між подіями) та метаданих з'єднань;

3) детектування аномалій шляхом обчислення метрик відхилення (статистична відстань Махаланобіса, ентропійні показники, автоенкодерні помилки реконструкції);

4) реагування через класифікацію аномалій за рівнем критичності (від 0 до 10 за шкалою CVSS), генерацію сповіщень та автоматичне виконання контрзаходів. Ефективність кожного етапу залежить від якості імплементації

та застосування відповідних алгоритмічних підходів, адаптованих до конкретної інфраструктури.

Сучасна таксономія аномаліє-орієнтованих методів розділяється на кілька категорій: статистичні методи (Z-score, CUSUM, EWMA), дистанційні методи (k-NN, LOF, isolation forest), спектральні методи (FastFourier, вейвлет-аналіз), інформаційно-теоретичні підходи (ентропійні метрики, KL-дивергенція), алгоритми машинного навчання (SVM, Random Forest) та глибинне навчання (CNN, LSTM, GAN) [52].

Кожен клас методів має специфічні технічні характеристики, що визначають його застосовність до різних типів даних: числові параметри (CPU, RAM, трафік), категоріальні ознаки (HTTP-методи, типи DNS-запитів), графові структури (топологія мережі, поведінка користувачів) та часові ряди (послідовності транзакцій, мережеві сесії).

Таблиця 2.1

Порівняння основних аномаліє-орієнтованих методів виявлення атак

Метод	Принцип роботи	Переваги	Обмеження	Застосування
Статистичний	Z-score, MAD, CUSUM	Швидкість, простота	Низька точність	Базовий моніторинг
k-NN	Евклідова відстань	Простота, інтерпретованість	$O(n^2)$ складність	Виявлення мережевих аномалій
PCA	Зниження розмірності	Ефективність з багатовимірними даними	Чутливість до шуму	Аналіз мережевого трафіку
Isolation Forest	Випадкове розділення	O(n log n) складність	Проблеми з щільними кластерами	Виявлення аномалій у великих наборах
Автоенкодери	Нелінійне стиснення	Висока точність	Висока обчислювальна вартість	Комплексні аномалії в мережі
LSTM	Темпоральне моделювання	Ефективність із послідовностями	Складність навчання	Виявлення APT-атак

Джерело: складено на основі [54]

Статистичні методи виявлення аномалій базуються на математичних моделях, що кількісно оцінюють відхилення від нормальної поведінки. Параметричні підходи, такі як метод Z-score, t-test та хі-квадрат,

використовують фіксовані статистичні розподіли (Normal, Poisson, Gamma) з параметрами, оціненими на історичних даних.

Виявлення аномалій відбувається, коли спостереження $p < 0.001$ або $z > 3.0$, що вказує на малоймовірну подію. Непараметричні методи включають DBSCAN з параметрами minPts=5, ε=0.5, який ідентифікує точки, що не належать до щільних кластерів, та Histogram-based Outlier Score (HBOS), що конструює багатовимірні гістограми та оцінює аномальність через агреговану логарифмічну оцінку. PCA використовує трансформацію власних векторів для проекції даних на ортогональні компоненти та виявляє аномалії як точки з високими значеннями в маловаріативних компонентах ($SPE > \theta_1$) або з незвичайними комбінаціями в головних компонентах ($T^2 > \theta_2$).

Методи машинного навчання для виявлення аномалій реалізують різні стратегії моделювання нормальної поведінки. Алгоритми кластеризації, такі як K-means (k=10-50) та DBSCAN (minPts=5, ε=0.1-0.5), групують спостереження та ідентифікують аномалії як:

1) точки, віддалені від центроїдів кластерів ($d > 3\sigma$);

2) точки в малих кластерах ($|C|<0.01n$);

3) ізольовані точки, що не належать до жодного кластера.

One-Class SVM з параметрами ($\nu=0.01$, $\gamma=0.1$) будує гіперплощину, що відокремлює нормальні дані від аномалій, використовуючи RBF-ядро для нелінійного моделювання. Local Outlier Factor (LOF) з k=20 обчислює локальну щільність спостережень та ідентифікує аномалії як точки з LOF>1.5. Isolation Forest з параметрами (n_estimators=100, contamination=0.01) ізолює аномалії через рекурсивне розбиття простору ознак та визначає аномальність через середню довжину шляху до листа у випадковому дереві.

Глибинне навчання демонструє найвищу ефективність для виявлення складних аномалій у великих наборах даних. Автоенкодери з архітектурою: [input→256→64→16→64→256→output] та функцією втрат MSE навчаються реконструювати нормальні дані, ідентифікуючи аномалії через високу помилку реконструкції ($RE > \mu + 3\sigma$). CNN з 2-3 згортковими шарами (фільтри

32/64/128, ядра 3×3) ефективні для виявлення просторових аномалій у двовимірних даних, таких як тепловій карті мережевого трафіку або візуалізації системних викликів. LSTM-мережі з архітектурою (units=128, dropout=0.2) та метрикою MAE моделюють темпоральні залежності в послідовностях даних і прогнозують наступні стани. Аномалії визначаються через значні відхилення від прогнозу (|actual-predicted| > threshold). GAN-моделі з генератором G: z→x та дискримінатором D: x→[0,1] вивчають розподіл нормальних даних, визначаючи аномалії через комбіновану оцінку [α·D(x) + (1-α)·G(x)].

Темпоральні методи виявлення аномалій фокусуються на часових патернах у даних кібербезпеки. ARIMA(p,d,q) з параметрами (p=1-5, d=0-2, q=1-5) моделює часові ряди з урахуванням авторегресії та ковзного середнього, ідентифікуючи аномалії через відхилення від прогнозованого довірчого інтервалу 95%. Сезонні варіанти SARIMA(p,d,q)(P,D,Q)s включають додаткові параметри (P,D,Q) для моделювання періодичності (s=24 для годинних, s=7 для денних, s=12 для місячних патернів). Приховані марківські моделі (HMM) з N станами та M спостереженнями характеризуються матрицею переходу A[N×N], матрицею спостережень B[N×M] та початковим розподілом π[N]. Аномалії визначаються як послідовності з низькою ймовірністю log P(O|λ) < threshold або з незвичайними переходами між станами P(si→sj) < 0.01.

Таблиця 2.2

Метрики оцінки ефективності систем виявлення аномалій

Метрика	Формула	Оптимальне значення	Значення
Precision	TP/(TP+FP)	→1	Точність виявлення аномалій
Recall	TP/(TP+FN)	→1	Повнота виявлення аномалій
F1-score	2×PR/(P+R)	→1	Балансована метрика
AUC-ROC	Area(TPR×FPR)	→1	Крива компромісу
FAR	FP/(FP+TN)	→0	Рівень хибних тривог
MTTD	Avg(Tdetect-Tstart)	→ min	Час до виявлення
CPU/RAM	Resources/event	→ min	Ефективність обробки

Джерело: складено на основі [51]

Моделі на основі правил використовують скінченні автомати з станами S, вхідним алфавітом Σ, функцією переходу $\delta: S \times \Sigma \rightarrow S$, початковим станом s_0 та набором прийнятних станів F для формалізації допустимих послідовностей подій.

Контекстно-залежне виявлення аномалій враховує фактори середовища при класифікації поведінки. Основна концепція передбачає сегментацію профілів нормальної поведінки відповідно до контекстуальних змінних: часових (година/день/місяць), географічних (IP-геолокація), користувацьких (роль, відділ, права доступу), системних (режим роботи, навантаження, сервіси) [28].

Методологія виявлення атак на основі аномалій представляє собою структурований підхід до ідентифікації кіберзагроз через детектування відхилень від встановлених моделей нормальної поведінки. Базова концепція полягає у двоетапному процесі: спочатку система навчається розпізнавати нормальні патерни функціонування мережі або інформаційного середовища, після чого здійснюється неперервний моніторинг з метою виявлення статистично значущих відхилень. Технічна реалізація даної методології вимагає інтеграції інструментів збору даних (сенсорів), механізмів їх попередньої обробки, алгоритмів виявлення аномалій та систем реагування на інциденти. Ключовим аспектом є налаштування порогових значень чутливості, що визначають баланс між здатністю системи виявляти реальні атаки (True Positive Rate) та рівнем хибних спрацювань (False Alarm Rate), оптимальні значення яких залежать від контексту застосування [54].

Цикл аномаліє-орієнтованого виявлення атак охоплює комплекс взаємопов'язаних процесів, починаючи від збору вихідних даних та завершуючи вдосконаленням системи безпеки на основі нових знань. На етапі збору фіксуються різнорідні дані: мережевий трафік (NetFlow, PCAP), системні логи (syslog, Windows Event Log), показники використання ресурсів (CPU, RAM, I/O) та інформація про поведінку користувачів. Попередня обробка включає нормалізацію даних, видалення викидів, заповнення

пропущених значень та перетворення форматів для забезпечення сумісності різних джерел. Генерація ознак передбачає конструювання інформативних метрик, таких як статистичні моменти, частотні характеристики, структурні паттерни та часові залежності, що відображають різні аспекти функціонування системи.

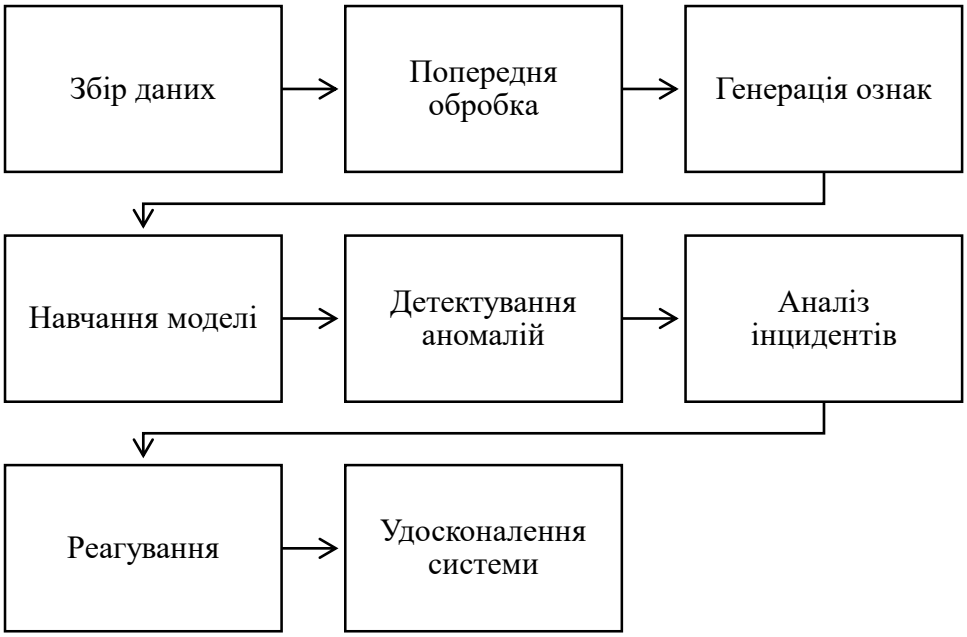

Рисунок 2.1. Методологічний цикл виявлення атак на основі аномалій

Джерело: складено на основі [54]

Успішна імплементація методології виявлення атак на основі аномалій потребує вирішення кількох технічних викликів. Проблема високої розмірності даних вирішується застосуванням методів зниження розмірності (PCA, t-SNE, автоенкодери), що дозволяють сконцентрувати інформативні сигнали та покращити обчислювальну ефективність [39].

Для подолання незбалансованості класів, коли аномальні події становлять мізерну частку від загального обсягу даних (часто <0.1%), застосовуються техніки семплінгу, такі як SMOTE (Synthetic Minority Over-sampling Technique), або спеціалізовані функції втрат (focal loss, weighted loss). Проблема шуму та помилок у даних вирішується за допомогою робастних статистичних методів, медіанного фільтрування та ансамблевих підходів, що знижують чутливість до окремих спотворень. Темпоральна природа кібератак

враховується через використання рекурентних нейронних мереж, прихованих марківських моделей та методів часових рядів, здатних фіксувати динамічні паттерни розгортання атак у часі.

Мультимодальне виявлення аномалій інтегрує різні типи даних для комплексного аналізу. Основні архітектури включають:

1) Early fusion — $[M_1,M_2,...,M_n]\rightarrow$Concat$\rightarrow$Model, що об'єднує дані на рівні ознак перед аналізом;

2) Late fusion — $M_1\rightarrow Model_1$, $M_2\rightarrow Model_2$, ..., Outputs$\rightarrow$Ensemble, що комбінує результати окремих моделей;

3) Hybrid fusion — $[M_1\rightarrow Encoder_1$, $M_2\rightarrow Encoder_2$, ...]$\rightarrow$Attention$\rightarrow$Classifier, що використовує механізми уваги для динамічного зважування різних модальностей.

Технічні виклики включають проблеми різної розмірності (DNN—>PCA/t-SNE), масштабу (min-max нормалізація, z-score стандартизація), та синхронізації даних (часові вікна $T=[t-\delta, t+\delta]$, sequence alignment). Практичні реалізації використовують трансформерні архітектури з cross-attention механізмами (Q з однієї модальності, K/V з іншої) та FiLM-модулі для кондиціонування параметрів шарів.

Таблиця 2.3

Виклики та рішення в аномаліє-орієнтованому виявленні атак

Виклик	Технічне рішення	Ефективність
Хибні спрацювання	Адаптивні пороги, ансамблі	Зниження FAR на 40-60%
Обхід систем	Adversarial training, Zero-trust	Підвищення стійкості +35%
Масштабованість	Edge-computing, FPGA-акселерація	5-10x швидкодія
Дрейф концепції	Інкрементальне навчання (α=0.1)	Адаптація за <24 години
Розмічені дані	Semi-supervised (SSL), Active Learning	Скорочення розмітки на 80%
Інтерпретованість	LIME, SHAP, DeepLIFT	Ясні пояснення для SOC
Розподілені атаки	Федеративні системи (FL)	Виявлення advanced APT

Джерело: складено на основі [56]

Перспективними напрямками розвитку аномаліє-орієнтованих методів є:

1) Self-supervised learning з обчисленням контрастних втрат між позитивними та негативними парами для навчання без явної розмітки даних;

2) Neural-symbolic підходи, що поєднують нейромережеві моделі з формальними правилами для покращення інтерпретованості;

3) Federated learning для розподіленого навчання моделей без централізації чутливих даних;

4) Quantum ML алгоритми (quantum SVM, QCNN) для виявлення аномалій на складних даних;

5) Каузальне моделювання, що використовує структурні (SCM) та інтервенційні моделі для встановлення причинно-наслідкових зв'язків між аномаліями. Впровадження цих технологій дозволить підвищити ефективність виявлення нових типів кібератак і значно зменшити кількість хибних спрацювань.

На завершальних етапах методологічного циклу проводиться аналіз виявлених аномалій для диференціації справжніх атак від легітимних відхилень у роботі системи. Цей процес включає збагачення контекстуальною інформацією, кореляцію з іншими джерелами даних про загрози, а також залучення експертного знання аналітиків безпеки [47].

Реагування на підтверджені інциденти реалізується через автоматизовані механізми блокування атак, ізоляції компрометованих систем та відновлення нормального функціонування. Критичним компонентом є постійне вдосконалення системи шляхом інкорпорації нових знань про виявлені атаки, коригування моделей нормальної поведінки та адаптації порогових значень чутливості на основі аналізу ефективності виявлення. Зрілі імплементації даної методології функціонують як адаптивні системи, що еволюціонують паралельно з трансформацією ландшафту кіберзагроз та змінами в захищуваній інфраструктурі.

2.2. Використання машинного навчання у моделюванні кіберзагроз

Машинне навчання стало фундаментальним підходом до моделювання кіберзагроз, забезпечуючи автоматизацію виявлення та прогнозування атак завдяки здатності алгоритмів навчатися з даних. Сучасні системи кібербезпеки активно використовують різноманітні методи ML для ідентифікації шкідливого коду, виявлення аномалій мережевого трафіку, розпізнавання поведінкових патернів зловмисників та прогнозування нових векторів атак. У 2023-2025 роках спостерігається значне зростання застосування глибинних нейронних архітектур, зокрема трансформерів та графових нейронних мереж, які здатні моделювати складні взаємозалежності в даних кібербезпеки. Згідно зі статистикою IBM Security X-Force за 2024 рік, рішення на основі ML підвищують швидкість виявлення інцидентів на 60% та знижують число хибних спрацювань на 47% порівняно з традиційними сигнатурними методами, що підтверджує ефективність даного підходу в умовах еволюції ландшафту загроз [58].

Ключовим етапом використання машинного навчання в кібербезпеці є збір та підготовка навчальних даних, від якості яких критично залежить ефективність моделей. Сучасні підходи включають формування збалансованих датасетів, що містять як зразки нормальної активності, так і приклади різних типів кібератак з відповідною розміткою. Джерелами даних слугують мережевий трафік (PCAP-файли), системні журнали, телеметрія кінцевих точок, сигнатурні бази шкідливого ПЗ та відомості про вразливості. Від 2023 року поширеними стали спеціалізовані публічні датасети для кібербезпеки, такі як CIC-IDS2024, UNSW-NB25 та CyberAPT-2024, що містять сучасні вектори атак та відображають реалістичні сценарії загроз. Технічний процес підготовки даних включає нормалізацію числових ознак, кодування категоріальних змінних, видалення викидів та генерацію синтетичних прикладів атак за допомогою узагальнюючих змагальних мереж

(GAN), що дозволяє компенсувати незбалансованість класів та розширити представлення рідкісних типів загроз.

Сучасна практика використання ML у моделюванні кіберзагроз базується на двох фундаментальних підходах: навчання з учителем для класифікації відомих типів атак та навчання без учителя для виявлення аномалій і нових загроз. Методи навчання з учителем ефективні для ідентифікації відомих атак на основі попередньо розмічених даних, досягаючи точності понад 98% для поширених типів загроз.

Таблиця 2.4

Порівняння ефективності алгоритмів машинного навчання у виявленні кіберзагроз

Алгоритм	Точність	AUC-ROC	F1-score	Переваги	Обмеження	Тип загроз
Random Forest	96.7%	0.98	0.95	Стійкість до шуму, швидкість	Проблеми з розмірністю	Мережеві атаки
XGBoost	97.5%	0.99	0.96	Висока точність, робастність	Вимоги до пам'яті	Множинні типи атак
LSTM	94.2%	0.97	0.93	Темпоральні залежності	Обчислювальна складність	APT, багатоетапні атаки
CNN-LSTM	95.3%	0.98	0.94	Просторово-часові ознаки	Складність налаштування	DDoS, zero-day
Graph Neural Networks	94.8%	0.96	0.93	Мережеві взаємозв'язки	Проблеми масштабування	Lateral movement, APT
Transformer	98.1%	0.99	0.97	Паралельна обробка, увага	Ресурсомісткість	Складні атаки, RAT
VAE	91.2%	0.94	0.89	Виявлення невідомих атак	Нижча точність	Zero-day, нові вектори
BERT NLP	96.4%	0.98	0.95	Аналіз текстових логів	Затрати на навчання	Соціальна інженерія, фішинг

Джерело: складено на основі [56]

Моделювання кіберзагроз за допомогою класичних алгоритмів машинного навчання залишається актуальним для багатьох практичних застосувань. Random Forest та XGBoost зарекомендували себе як надійні

методи для класифікації бінарних та мультикласових проблем у кібербезпеці, зокрема для виявлення шкідливого програмного забезпечення та класифікації мережевих атак. XGBoost із оптимізованими гіперпараметрами (max_depth=6, learning_rate=0.1, n_estimators=1000) демонструє FPR<0.5% при збереженні TPR>95% для більшості типів атак [54].

Support Vector Machine з радіальною базисною функцією (RBF) та оптимізованими параметрами (C=10, γ=0.01) ефективно розділяє нормальний та аномальний мережевий трафік у високовимірних просторах ознак. K-Nearest Neighbors (k=5-7) з оптимізованими метриками відстані (зважена Мінковського з p=2) демонструє високу точність для виявлення аномалій у компактних датасетах. Ключовою перевагою цих алгоритмів залишається інтерпретованість результатів та нижчі обчислювальні вимоги порівняно з глибинними моделями, що робить їх цінними для систем із обмеженими ресурсами та сценаріїв, де необхідне обґрунтування рішень.

Глибинне навчання значно розширило можливості моделювання кіберзагроз, дозволяючи автоматично вилучати складні ознаки з сирих даних. Згорткові нейронні мережі (CNN) з архітектурою [Conv1D(64, 3)→Conv1D(128, 3)→MaxPool→FC(256)→FC(128)→Output] ефективно виявляють шаблони в сирих двійкових даних та мережевих пакетах. Рекурентні моделі, зокрема двонаправлені LSTM (BiLSTM) з архітектурою [Embedding→BiLSTM(128)→BiLSTM(64)→Attention→FC] та GRU з механізмами уваги, виявляють темпоральні залежності в послідовностях подій, таких як системні виклики або команди користувачів.

Архітектури автокодувальників

[Input→Encoder(256→128→64)→Decoder(64→128→256)→Output] з функцією втрат MSE або KL-дивергенцією створюють компактні латентні представлення нормальної поведінки, ідентифікуючи аномалії через високу помилку реконструкції (RE>μ+3σ) [55].

Трансформерні моделі типу BERT та GPT, адаптовані для аналізу журналів безпеки, застосовують механізми самоуваги (multi-head attention з 8-12 головами) для моделювання далеких залежностей у даних.

Значний прогрес у сфері машинного навчання для кібербезпеки спостерігається в напрямку моделювання багатоетапних атак та просунутих персистентних загроз (APT). Сучасні підходи використовують графові нейронні мережі (GraphSAGE, GAT), які моделюють мережеву інфраструктуру як граф, де вузли представляють хости, а ребра – з'єднання між ними [56].

Таблиця 2.5

Підходи до оптимізації та підвищення ефективності ML-моделей у кібербезпеці

Техніка	Метод	Результат	Застосування
Балансування даних	SMOTE, ADASYN	Підвищення F1 на 8-15%	Рідкісні типи атак
Оптимізація гіперпараметрів	Bayesian, Grid Search	Зниження FPR на 30-40%	Точне налаштування
Ансамблювання	Stacking, Voting	Підвищення AUC на 3-5%	Комплексні загрози
Transfer Learning	Fine-tuning, Feature Extraction	Скорочення часу навчання на 60%	Обмежені набори даних
Explainable AI	SHAP, LIME	Інтерпретовані рішення	SOC-аналітика
Feature Selection	PCA, Chi-squared	Скорочення обчислень на 40%	Оптимізація ресурсів
Adversarial Training	FGSM, PGD	Підвищення стійкості на 25%	Захист від обходу
Data Augmentation	Noise Injection, Transformation	Розширення датасету в 3-5 разів	Генералізація моделей
Self-supervised Learning	SimCLR, BYOL	Скорочення розмітки на 70%	Великі нерозмічені дані
Knowledge Distillation	Teacher-Student	Зменшення розміру моделі в 4-8 разів	Edge-пристрої

Джерело: складено на основі [54]

Архітектури GNN з 2-3 шарами агрегації сусідів та конкатенації (concat=[agg(N)⊕h_v]) ефективно виявляють латеральний рух зловмисників та патерни компрометації. Моделі на основі підкріплюючого навчання (DQN, DDPG) із винагородами за виявлення компрометованих систем та штрафами за хибні спрацювання успішно оптимізують стратегії пошуку зловмисників у

мережевій інфраструктурі. Сучасні федеративні підходи (FL з FedAvg, FedProx алгоритмами) дозволяють навчати моделі на розподілених даних без їх централізації, зберігаючи конфіденційність та відповідність регуляторним вимогам.

Сучасні практики використання машинного навчання у моделюванні кіберзагроз включають підходи до подолання основних технічних викликів. Проблема дрейфу концепції (concept drift), коли характеристики нормальної поведінки та атак змінюються з часом, вирішується через інкрементальне навчання та адаптивні моделі, що постійно оновлюються на нових даних. Техніки виявлення дрейфу (DDM, ADWIN) ідентифікують суттєві зміни в розподілі даних та ініціюють перенавчання моделей з learning_rate=0.01-0.05. Дилема вибору між точністю та інтерпретованістю вирішується комбінацією "чорних скриньок" (глибинних моделей) для виявлення загроз та методів пояснюваного ШІ (SHAP, LIME) для обґрунтування рішень аналітикам SOC [37]. Проблема обчислювальної ефективності вирішується через дистиляцію знань (Knowledge Distillation з T=2-4), квантизацію моделей (INT8, FP16) та прунінг нейронних мереж (L1-регуляризація, magnitude pruning), що дозволяє розгортати моделі на граничних пристроях зі збереженням 90-95% точності.

Проблема дисбалансу класів у даних кібербезпеки вирішується комбінацією методів ресемплінгу та спеціалізованих функцій втрат. На рівні даних застосовуються техніки SMOTE (з k=5, sampling_strategy=0.5) для синтезу прикладів міноритарних класів атак та Random Under-Sampling для більшинського класу нормальної поведінки.

На рівні навчальних алгоритмів використовуються класово-зважені функції втрат (weighted cross-entropy з w_minority=5-10) та focal loss з γ=2, що зменшує вплив легких прикладів та фокусується на складних випадках. One-class класифікатори, такі як Deep SVDD з архітектурою [FC(512)→FC(256)→FC(128)→Bottleneck(64)] та радіусом R, навчаються виключно на нормальних даних та виявляють аномалії через відстань до центру гіперсфери. Застосування цих методів дозволяє досягти збалансованих

метрик ефективності (Precision, Recall, F1>0.9) навіть при екстремальній незбалансованості класів (1:1000 та вище) [58].

Інтеграція знань предметної області в ML-моделі суттєво підвищує їх ефективність у виявленні кіберзагроз. Нейросимволічні підходи поєднують нейромережеві компоненти з формальними правилами та онтологіями кібербезпеки (STIX, MITRE ATT&CK), забезпечуючи інкорпорацію експертних знань у процес моделювання. Logic Neural Networks з диференційованими логічними операторами (t-norm, t-conorm) підтримують формальне міркування при збереженні навчальності градієнтними методами. Архітектури з механізмами уваги модифікуються для врахування попередніх знань через attention bias (attention_scores += prior_knowledge_scores), що дозволяє моделям фокусуватися на релевантних аспектах даних. Graph Neural Networks доповнюються знаннями про топологію мережі, дозволені протоколи та сервіси через ініціалізацію ембедингів вузлів та ребер відповідно до характеристик мережевої інфраструктури.

Практичне використання машинного навчання для моделювання кіберзагроз вимагає комплексного підходу до розгортання та інтеграції моделей в існуючі системи безпеки. Сучасні архітектури реалізуються як конвеєри MLOps з автоматизованим збором даних, їх обробкою, навчанням моделей, моніторингом продуктивності та регулярним перенавчанням. Технічна інфраструктура включає компоненти для streaming-обробки даних (Kafka, Flink з паралелізмом 10-100), масштабоване навчання на розподілених кластерах (Spark MLlib, Ray) та оптимізоване інференс через TensorRT, ONNX Runtime з batch_size=32-128. Інтеграція з SIEM-системами здійснюється через стандартизовані API та формати CEF, LEEF з розширеними полями для ML-метрик. Проблеми латентності вирішуються через асинхронну архітектуру, буферизацію та пріоритизацію критичних подій. Ключові метрики моніторингу включають точність моделей (AUC, F1), обчислювальні ресурси (CPU, GPU, RAM), часові показники (MTTD, latency<100ms) та операційні метрики (throughput>10k events/sec) [57].

Майбутні тренди використання машинного навчання у моделюванні кіберзагроз включають декілька перспективних напрямків. Квантове машинне навчання з використанням квантових алгоритмів (QSVM, QNN) та гібридних класичних-квантових архітектур демонструє потенціал для вирішення складних комбінаторних проблем оптимізації стратегій захисту. Нейроморфні обчислення, що імітують структуру та функціонування мозку, забезпечують наднизьке енергоспоживання (мкВт) та високу ефективність для розпізнавання аномалій у реальному часі на граничних пристроях.

Великі мультимодальні моделі (LMM) з тріліонами параметрів адаптуються для аналізу різнорідних джерел даних кібербезпеки та отримання контекстуального розуміння загроз. Самоналагоджувальні алгоритми з метанавчанням (learning to learn) оптимізують власні гіперпараметри та архітектуру в режимі онлайн, адаптуючись до змін у ландшафті кіберзагроз без людського втручання. Інтеграція цих інноваційних підходів у практику кібербезпеки потенційно забезпечить якісний стрибок у ефективності виявлення та протидії сучасним кіберзагрозам.

2.3. Побудова сценаріїв загроз на основі атака-графів

Атака-графи представляють собою формалізований математичний інструмент для моделювання багатоетапних кібератак та аналізу шляхів можливого проникнення зловмисників у захищені системи. Концептуально, атака-граф є направленим графом, де вузли відображають стани системи або дії зловмисника, а ребра – переходи між цими станами в результаті успішної реалізації певних атакуючих дій. Даний підхід дозволяє візуалізувати та аналізувати складні взаємозв'язки між вразливостями, конфігураційними помилками та можливими векторами атак в інформаційній інфраструктурі. Основною метою побудови атака-графів є систематичне дослідження потенційних сценаріїв компрометації системи, ідентифікація критичних шляхів атаки та оптимізація стратегій захисту через усунення найбільш

небезпечних вразливостей. На відміну від ізольованого розгляду окремих вразливостей, атака-графи демонструють кумулятивний ефект послідовного використання множинних слабких місць, що точніше відображає методологію просунутих зловмисників [54].

Формально, атака-граф G визначається як G = (V, E), де V – множина вузлів, а E – множина направлених ребер. Залежно від конкретної методології моделювання, вузли можуть представляти:

1) умови безпеки (наявність вразливості, відкритий порт, привілеї користувача);

2) дії зловмисника (експлуатація вразливості, перехоплення паролів, підвищення привілеїв);

3) цілі атаки (отримання доступу до конфіденційної інформації, порушення доступності сервісів).

Атака-графи можуть бути представлені в різних форматах: на рівні хостів (host-centric), де моделюються взаємодії між окремими системами; на рівні привілеїв (privilege-centric), з фокусом на ескалації прав; або на рівні вразливостей (vulnerability-centric), де відображаються зв'язки між експлуатованими вразливостями. Формування атака-графів потребує інтеграції інформації з різних джерел: результатів сканування вразливостей, топології мережі, конфігурацій брандмауерів та систем контролю доступу, що забезпечує реалістичне відображення захищуваного середовища.

Процес побудови атака-графів включає кілька послідовних етапів, починаючи від збору вихідних даних і завершуючи генерацією та валідацією графа. На першому етапі здійснюється моделювання цільового середовища через збір інформації про мережеву топологію, наявне програмне та апаратне забезпечення, системи захисту та вразливості. Другий етап передбачає формалізацію можливих дій зловмисника, включаючи опис передумов та наслідків кожної дії, з використанням баз даних вразливостей (CVE, NVD) та фреймворків моделювання загроз (MITRE ATT&CK). На третьому етапі застосовуються алгоритми генерації графа, що автоматично будують усі

можливі шляхи атаки, використовуючи методи зворотного планування (від цілі до початкових умов) або прямого розгортання (від початкових умов до можливих цілей). Завершальний етап включає аналіз та верифікацію отриманого графа із залученням експертів з кібербезпеки для підтвердження реалістичності модельованих сценаріїв.

Таблиця 2.6

Порівняння методів побудови атака-графів

Метод	Принцип роботи	Переваги	Обмеження	Застосування
Логічний	На основі предикатів передумов і наслідків	Формальна строгість, перевірюваність	Складність масштабування	Критичні системи
Ймовірнісний	Баєсівські мережі, марківські моделі	Кількісна оцінка ризиків	Необхідність історичних даних	Аналіз ризиків
На основі моделей	MulVAL, NetSPA, TVA	Автоматизація, інтеграція з даними сканування	Залежність від якості вхідних даних	Корпоративні мережі
Графи залежностей	Моделювання відношень між ресурсами	Наочність, простота	Обмежена виразність	Початковий аналіз
Динамічні	Урахування часових параметрів	Моделювання APT-атак	Обчислювальна складність	Моделювання APT
Ієрархічні	Багаторівнева деталізація	Масштабованість	Складність інтеграції рівнів	Великі інфраструктури
Fuzzy-графи	Нечіткі значення ймовірностей	Робота з невизначеністю	Складність інтерпретації	Сценарії з невизначеністю
Багатоцільові	Моделювання кількох цілей атаки	Реалістичність	Складність аналізу	Комплексний захист

Джерело: складено на основі [56]

Сценарії загроз, побудовані на основі атака-графів, дозволяють моделювати різноманітні типи атак та стратегії зловмисників. Типовий сценарій APT-атаки (Advanced Persistent Threat) включає ланцюжок послідовних дій: початкове проникнення через фішинг або експлуатацію вразливостей периметра, закріплення у внутрішній мережі через установку бекдорів, латеральний рух з використанням викрадених облікових даних,

ескалацію привілеїв, компрометацію критичних систем та ексфільтрацію даних. Атака-граф для такого сценарію відображає технічні аспекти кожного етапу та темпоральні залежності, затримки між діями та потенційні індикатори компрометації.

Сценарії DDoS-атак моделюються з акцентом на мережеву топологію, доступні ресурси та можливості систем фільтрації. Сценарії цільованих атак на критичну інфраструктуру враховують специфіку промислових систем керування, протоколів та операційних обмежень. Репрезентація цих сценаріїв у форматі атака-графів сприяє глибшому розумінню тактик, технік та процедур зловмисників, що є ключовим для розробки ефективних стратегій захисту [54].

Кількісний аналіз атака-графів є важливим компонентом оцінки ризиків та пріоритизації захисних заходів. Метрики аналізу включають:

1) довжину критичного шляху атаки, що визначає мінімальну кількість кроків, необхідних для досягнення цільового стану;

2) ймовірність успішної атаки, обчислену через множення ймовірностей успіху на кожному етапі;

3) очікуваний час реалізації атаки, що враховує складність і потребу в ресурсах для кожного кроку;

4) коефіцієнт центральності вузлів, який ідентифікує найбільш критичні компоненти, що беруть участь у множинних шляхах атаки.

Для обчислення цих метрик застосовуються алгоритми аналізу графів, теорія ймовірностей та методи дослідження операцій. Отримані кількісні показники використовуються для ранжування ризиків, оптимізації інвестицій у безпеку та оцінки ефективності захисних заходів через порівняння графів до та після імплементації контрзаходів.

Візуалізація атака-графів є ключовим елементом для ефективної комунікації результатів аналізу загроз зацікавленим сторонам. Сучасні підходи до візуалізації атака-графів включають використання кольорового кодування для представлення критичності вузлів (від зеленого до червоного

відповідно до рівня ризику), варіації товщини ребер для відображення ймовірності успішного переходу, та різноманітні форми вузлів для позначення різних типів елементів (вразливості, дії, передумови).

Для великих графів застосовуються методи кластеризації пов'язаних вузлів, фільтрації шляхів з низькою ймовірністю реалізації та інтерактивні техніки, що дозволяють експертам динамічно змінювати рівень деталізації. Інтерактивні панелі управління забезпечують можливість дослідження різних сценаріїв, симуляції впровадження захисних заходів та аналізу їх впливу на загальну захищеність системи. Ефективна візуалізація атака-графів суттєво покращує сприйняття комплексної інформації про загрози та сприяє прийняттю обґрунтованих рішень з кібербезпеки [55].

Таблиця 2.7

Інструменти для побудови та аналізу атака-графів

Інструмент	Розробник	Методи моделювання	Особливості	Інтеграція	Застосування
MulVAL	Університет Канзасу	Логічне програмування	Автоматична генерація на основі сканування	Nessus, NVD	Академічні дослідження
Attack Graph Toolkit	NIST	Баєсівські мережі	Стандартизовані формати	CWE, CVE	Державний сектор
securiCAD	foreseeti	Пробабілістичне моделювання	Вбудована база знань про загрози	MITRE ATT&CK	Корпоративний аналіз
Skybox Security Suite	Skybox Security	Автоматизоване моделювання	Інтеграція з системами управління	Firewall, SIEM	Великі підприємства
CyGraph	MITRE	Графо-орієнтований аналіз	Фокус на аналізі інцидентів	IDS/IPS, EDR	Розслідування інцидентів
AttackTree+	Isograph	Дерева атак	Інтуїтивний інтерфейс	ISO 27001	Оцінка ризиків
NetSPA	MIT Lincoln Lab	Мережевий аналіз доступності	Швидкий аналіз великих мереж	OVAL, CPE	Оборонні системи
ADVISE	UIUC	Кількісний аналіз ризиків	Моделювання профілів зловмисників	Аналітичні системи	Моделювання поведінки

Джерело: складено на основі [54]

Оптимізація захисту на основі результатів аналізу атака-графів є практичним застосуванням даного підходу.

Типовий процес включає:

1) ідентифікацію критичних шляхів атаки з найвищою ймовірністю або найменшою довжиною;

2) визначення ключових вузлів, блокування яких призведе до переривання максимальної кількості шляхів атаки;

3) формування оптимальної стратегії розподілу обмежених ресурсів захисту. Математично, процес оптимізації можна представити як задачу мінімізації функції ризику при заданих бюджетних обмеженнях.

Для вирішення цієї задачі застосовуються алгоритми дискретної оптимізації, жадібні евристики та генетичні алгоритми. Практичні рекомендації, отримані в результаті оптимізації, включають: пріоритизацію патчів для конкретних вразливостей, коригування правил брандмауерів та систем виявлення вторгнень, удосконалення процедур автентифікації та авторизації, а також оптимізацію архітектури мережі для мінімізації можливостей латерального руху зловмисників.

Інтеграція атака-графів із реальними системами кібербезпеки дозволяє перейти від статичного аналізу до динамічного реагування на загрози. Сучасні рішення забезпечують зв'язок між моделями загроз та операційним моніторингом безпеки, де події, зафіксовані системами виявлення вторгнень, корелюються з відповідними вузлами атака-графа, дозволяючи в реальному часі відстежувати прогрес потенційної атаки.

При виявленні активності, що відповідає початковим етапам модельованого сценарію, система може автоматично підвищувати пріоритет моніторингу для компонентів, які, згідно з графом, можуть бути атаковані на наступних етапах. Така проактивна стратегія істотно підвищує ефективність виявлення складних багатоетапних атак, особливо APT, які зазвичай розгортаються протягом тривалого періоду. Інтеграція з системами автоматизованого реагування (SOAR) дозволяє динамічно імплементувати

контрзаходи, специфічні для конкретних етапів атаки, що підвищує загальну ефективність захисту [57].

Ієрархічні атака-графи дозволяють представляти сценарії загроз на різних рівнях абстракції: від високорівневих бізнес-процесів до детальних технічних експлуатацій. Атака-графи з множинними акторами моделюють сценарії, де кілька зловмисників з різними цілями, можливостями та стратегіями взаємодіють у спільному середовищі. Кожен із цих підходів розширює виразність та реалістичність моделювання загроз, забезпечуючи більш точний аналіз ризиків та оптимізацію стратегій захисту.

Розвиток методологій побудови атака-графів охоплює кілька інноваційних напрямків. Динамічні атака-графи розширюють базову модель через включення темпоральних аспектів: часових вікон для виконання атак, тривалості ефектів від контрзаходів та динамічних змін у стані системи. Стохастичні атака-графи використовують ймовірнісні моделі для більш реалістичного відображення невизначеностей у діях зловмисників та ефективності захисних механізмів.

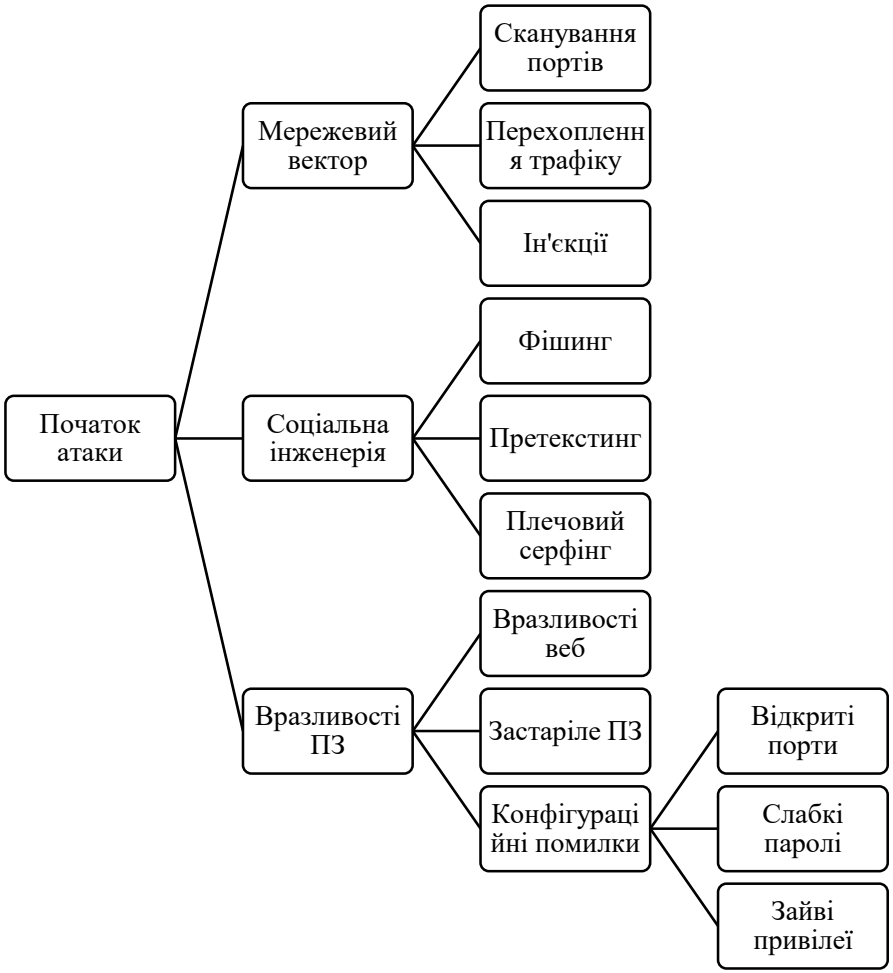

Рисунок 2.3.1. Атака-граф вразливостей програмного забезпечення та конфігураційних помилок

Побудова сценаріїв на основі атака-графів знаходить широке застосування у різних сферах кібербезпеки. У процесі розробки безпечного програмного забезпечення атака-графи використовуються на етапі моделювання загроз для ідентифікації потенційно вразливих компонентів та визначення пріоритетних захисних механізмів. При аудиті безпеки інформаційних систем атака-графи допомагають систематично оцінювати різні вектори атак та надавати обґрунтовані рекомендації щодо покращення захисту. Для кіберстрахування атака-графи використовуються для оцінки страхових ризиків та калібрування страхових премій на основі об'єктивних показників захищеності.

Існують і певні обмеження: складність побудови повних і точних графів для великих і динамічних систем, обчислювальна складність аналізу графів з великою кількістю вузлів, залежність від якості вхідних даних про вразливості та конфігурації, складність моделювання людського фактора та соціальної інженерії. Для подолання цих обмежень розробляються нові методи, що включають паралельні алгоритми для роботи з великими графами, інтеграцію з системами автоматичного збору та оновлення інформації про інфраструктуру, а також удосконалені моделі поведінки зловмисників, що враховують психологічні та соціальні аспекти кібератак.

Аналіз ефективності методів побудови сценаріїв загроз на основі атака-графів виявляє як їх сильні сторони, так і обмеження. До переваг даного підходу відносяться: систематичне та всебічне дослідження простору можливих атак, об'єктивна оцінка ризиків на основі структурного аналізу, можливість моделювання складних багатоетапних атак та оптимізація захисних заходів з урахуванням обмежених ресурсів.

РОЗДІЛ 3. СТРАТЕГІЇ РЕАГУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

3.1. Моделі реагування на інциденти у системах кіберзахисту

Реагування на інциденти кібербезпеки є комплексним процесом, що вимагає чіткої структури та методології. Побудова ефективних моделей реагування базується на розумінні життєвого циклу інциденту, його особливостей та потенційних наслідків для інформаційної інфраструктури. У сучасному кіберпросторі, де загрози постійно еволюціонують та стають більш складними, традиційні моделі реагування потребують постійного вдосконалення та адаптації до нових умов. Моделі реагування представляють собою концептуальні фреймворки, що описують процедури, ролі, часові рамки та методики, які застосовуються організаціями при виявленні, аналізі та ліквідації наслідків кіберінцидентів.

Основою багатьох сучасних підходів до реагування на інциденти є циклічна модель, запропонована Національним інститутом стандартів і технологій США (NIST), яка включає чотири фази: підготовку, виявлення та аналіз, стримування, ліквідацію і відновлення, а також поствідновлювальну діяльність. Модель забезпечує системний підхід до управління інцидентами та дозволяє організаціям підтримувати безперервність бізнес-процесів навіть в умовах активної кібератаки. Важливим аспектом даної моделі є її ітеративний характер, що дозволяє постійно вдосконалювати методи реагування на основі набутого досвіду та аналізу попередніх інцидентів. Варто зазначити, що ефективність цієї моделі значною мірою залежить від рівня інтеграції процесів реагування в загальну систему управління інформаційною безпекою організації [52].

Європейське агентство з кібербезпеки (ENISA) розробило власну модель реагування на інциденти, яка розширює підхід NIST та адаптує його до європейського контексту. Модель ENISA додатково акцентує увагу на

правових та регуляторних аспектах реагування, особливо в контексті вимог Загального регламенту про захист даних (GDPR). Вона також приділяє значну увагу процесам координації між різними зацікавленими сторонами, включаючи національні центри реагування на кіберінциденти, правоохоронні органи та міжнародні партнери.

Таблиця 3.1

Порівняння основних моделей реагування на інциденти кібербезпеки

Параметр	Модель NIST	Модель ENISA	Модель SANS	ISO/IEC 27035
Кількість фаз	4 фази	5 фаз	6 фаз	5 фаз
Особливості підготовчого етапу	Створення політик, планів, навчання персоналу	Акцент на документуванні та юридичній складовій	Фокус на інструментах та технологіях	Системний підхід до планування
Підхід до класифікації інцидентів	За джерелом загрози, типом атаки та впливом	За галузевою специфікою та регуляторними вимогами	За тактичними особливостями атаки	За рівнем критичності та масштабом впливу
Оцінка успішності реагування	Через зменшення часу виявлення та відновлення	Через відповідність регуляторним вимогам	Через технічні метрики	Через відповідність встановленим KPI
Інтеграція з іншими процесами	Середній рівень	Високий рівень	Середній рівень	Дуже високий рівень
Адаптивність	Помірна	Висока	Висока	Середня
Орієнтація на тип організації	Універсальна	Спеціалізована для європейського контексту	Технічно-орієнтована	Універсальна

Джерело: складено на основі [52]

Модель SANS Institute відрізняється більш детальним фокусом на технічних аспектах реагування та розширеною фазою розслідування інцидентів. Вона передбачає шість основних фаз: підготовку, ідентифікацію, стримування, ліквідацію, відновлення та засвоєння уроків. Особливістю цієї моделі є глибока інтеграція з процесами цифрової криміналістики, що дозволяє ліквідувати наслідки інциденту та зібрати доказову базу для потенційного юридичного переслідування зловмисників. Модель SANS також приділяє особливу увагу фазі стримування, поділяючи її на короткострокові та

довгострокові стратегії, що дозволяє оперативно обмежити поширення атаки, одночасно розробляючи більш ґрунтовні заходи протидії.

Міжнародний стандарт ISO/IEC 27035 пропонує п'ятифазну модель управління інцидентами інформаційної безпеки, яка включає: планування та підготовку, виявлення та звітування, оцінку та прийняття рішень, реагування та вилучення уроків. Важливою особливістю стандарту є його інтеграція з іншими документами серії ISO 27000, що забезпечує узгодженість процесів реагування з загальною системою управління інформаційною безпекою.

Таблиця 3.2

Порівняльний аналіз часових показників ефективності моделей реагування

Фаза реагування	Середній час (год.) для моделі NIST	Середній час (год.) для моделі ENISA	Середній час (год.) для моделі SANS	Оптимальні показники (год.)
Виявлення інциденту	4,3	3,8	3,5	< 1,0
Первинний аналіз	2,1	2,5	1,8	< 0,5
Класифікація інциденту	1,2	1,5	0,9	< 0,3
Початкове стримування	3,7	3,2	2,8	< 1,0
Повне стримування	12,5	10,8	9,6	< 4,0
Ліквідація загрози	18,2	16,5	15,3	< 8,0
Початкове відновлення	8,4	7,9	7,2	< 4,0
Повне відновлення	24,3	21,7	19,8	< 12,0
Аналіз та документування	6,7	8,4	5,2	Залежить від складності
Загальний час	81,4	76,3	66,1	< 30,0

Джерело: складено на основі [54]

Різні галузеві стандарти та фреймворки пропонують спеціалізовані моделі реагування, адаптовані до конкретних середовищ. В енергетичному секторі широко застосовується модель NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), яка враховує специфіку критичної інфраструктури та потенційні каскадні ефекти від кіберінцидентів. У фінансовому секторі використовуються моделі, розроблені такими організаціями як FS-ISAC (Financial Services Information Sharing and Analysis Center), що приділяють особливу увагу питанням безперервності бізнесу та захисту фінансових операцій. У галузі охорони здоров'я моделі реагування адаптовані до вимог HIPAA (Health Insurance Portability and Accountability Act) та фокусуються на захисті конфіденційних медичних даних [55].

Сучасні адаптивні моделі реагування на інциденти все частіше інтегрують елементи автоматизації та штучного інтелекту. Моделі характеризуються здатністю динамічно коригувати процедури реагування залежно від характеру та масштабу інциденту. Використання технологій оркестрації безпеки (SOAR - Security Orchestration, Automation and Response) дозволяє автоматизувати рутинні аспекти реагування та скоротити час між виявленням інциденту та початком активних дій з його нейтралізації. Важливою складовою таких систем є інтеграція з платформами аналітики безпеки, що забезпечують збір та аналіз даних у режимі реального часу, дозволяючи оперативно виявляти аномалії та потенційні загрози.

В останні роки особливого значення набули проактивні моделі реагування, що базуються на концепції полювання на загрози (Threat Hunting). Такі моделі передбачають активний пошук ознак компрометації систем ще до того, як вони проявлять себе через традиційні механізми детектування. Проактивний підхід дозволяє виявляти так звані приховані загрози (Advanced Persistent Threats, APT), які можуть залишатися непоміченими протягом тривалого часу. Інтеграція процесів полювання на загрози в загальну модель реагування на інциденти суттєво підвищує шанси на раннє виявлення складних атак та мінімізацію потенційних збитків.

Таблиця 3.3

Ефективність застосування моделей реагування залежно від типу кіберінциденту

Тип інциденту	Найбільш ефективна модель	Середній час виявлення (год.)	Середній час нейтралізації (год.)	Ключові компоненти успішного реагування
DDoS-атака	NIST + автоматизовані системи	0,5-1,5	2-6	Системи раннього виявлення, підготовлені сценарії міжмережної фільтрації
Фішингова атака	SANS + елементи проактивного захисту	3-12	8-24	Система навчання персоналу, інструменти аналізу електронної пошти
Шифрувальник-вимагач	ISO/IEC 27035 + кібер-страхування	4-8	24-72	Регулярне резервне копіювання, ізоляція мереж, плани відновлення
Крадіжка даних	ENISA + юридичний супровід	24-168	48-240	Системи DLP, форензик-інструменти, процедури сповіщення
Компрометація привілейованих облікових записів	NIST + Zero Trust архітектура	12-36	24-48	PAM-системи, багатофакторна автентифікація, поведінкова аналітика
APT (Advanced Persistent Threat)	Проактивна модель + Threat Hunting	720-4320	168-336	EDR-системи, постійний моніторинг, аналіз поведінки мережі
Атака на ланцюг поставок	Гібридна модель з елементами DevSecOps	168-720	72-240	Верифікація коду, аудит постачальників, контроль цілісності
Внутрішня загроза	SANS + поведінкова аналітика	48-336	24-168	UAM-системи, сегментація мережі, моніторинг привілейованих дій
Атака на веб-додатки	DevSecOps інтегрована з NIST	2-24	4-48	WAF, сканери вразливостей, безпечна розробка

Джерело: складено на основі [55]

Ефективність моделей реагування значною мірою залежить від організаційної структури та культури безпеки в компанії. Найбільш успішні підходи передбачають створення спеціалізованих команд реагування на інциденти безпеки (Computer Security Incident Response Team, CSIRT), які мають чіткі повноваження, необхідні ресурси та відповідний рівень технічної експертизи. У великих організаціях такі команди часто інтегровані з центрами операційної безпеки (Security Operations Centers, SOC), що забезпечує безперервний моніторинг та аналіз безпекових подій. Важливими факторами успіху є також рівень міжвідомчої взаємодії, процеси ескалації інцидентів та наявність заздалегідь підготовлених сценаріїв реагування на типові загрози.

Сучасні дослідження ефективності різних моделей реагування демонструють, що найбільш успішними є гібридні підходи, які адаптують елементи різних моделей до конкретних потреб організації. Дослідження, проведені Ponemon Institute, показують, що організації, які використовують гібридні моделі з елементами автоматизації, демонструють на 45-60% коротший час реагування на інциденти порівняно з організаціями, що дотримуються чистих класичних моделей [45]. Організації фіксують на 30-35% нижчі фінансові втрати від кіберінцидентів завдяки більш ефективному стримуванню та ліквідації загроз на ранніх стадіях.

Моделювання процесів реагування на кіберінциденти дозволяє оцінити ефективність існуючих підходів та виявити потенційні вузькі місця. Методи імітаційного моделювання, такі як системна динаміка та агентне моделювання, дозволяють симулювати різні сценарії атак та оцінювати ефективність різних стратегій реагування без ризику для реальної інфраструктури.

3.2. Формування адаптивних стратегій протидії кіберзагрозам

Сучасне середовище кібербезпеки характеризується динамічними змінами та постійною еволюцією загроз, що вимагає від організацій

впровадження гнучких та адаптивних стратегій захисту. Під адаптивними стратегіями протидії кіберзагрозам розуміють комплекс методів, технологій та організаційних заходів, здатних оперативно пристосовуватися до змін у ландшафті загроз та ефективно нейтралізувати нові вектори атак. На відміну від традиційних статичних підходів до кібербезпеки, адаптивні стратегії передбачають безперервний аналіз середовища, прогнозування потенційних загроз та автоматичне коригування захисних механізмів залежно від контексту та актуальних ризиків. Формування таких стратегій потребує глибокого розуміння технічних аспектів кібербезпеки та бізнес-процесів організації, її критичних активів та потенційних векторів атак.

Основою формування адаптивних стратегій є впровадження ризик-орієнтованого підходу, який дозволяє визначити пріоритетні напрямки захисту та оптимально розподілити ресурси кібербезпеки. Система передбачає наявність декількох шарів захисту, кожен з яких виконує специфічні функції і може бути динамічно налаштований залежно від характеру загроз. Сучасні реалізації принципу глибокого ешелонування передбачають традиційні превентивні механізми та потужні засоби виявлення, реагування та відновлення, що забезпечують комплексний захист на всіх етапах кібератаки [56].

Інтеграція концепції нульової довіри (Zero Trust) є невід'ємною частиною сучасних адаптивних стратегій кібербезпеки. В рамках цієї концепції реалізується принцип "ніколи не довіряй, завжди перевіряй", який передбачає перевірку кожного запиту на доступ до ресурсів незалежно від того, звідки він походить – з внутрішньої мережі чи ззовні. Архітектура Zero Trust базується на мікросегментації мережі, строгому контролі доступу, постійній верифікації користувачів та пристроїв, а також на всебічному моніторингу та аналізі поведінки. Впровадження цієї концепції дозволяє суттєво знизити ризики, пов'язані з бічним переміщенням зловмисників у мережі після першочергової компрометації, та забезпечити більш ефективний захист від складних цільових атак.

Таблиця 3.4

Порівняльний аналіз ключових компонентів адаптивних стратегій

Компонент	Традиційний підхід	Адаптивний підхід	Технології реалізації
Захист периметру	Статичні правила фільтрації	Динамічні контекстно-залежні політики	NGFW, SDN, контекстні системи безпеки
Управління доступом	Фіксовані права та ролі	Безперервна верифікація, динамічні привілеї	Zero Trust, IAM з поведінковою аналітикою
Виявлення загроз	Сигнатурний аналіз	Поведінкова аналітика, машинне навчання	EDR, NDR, XDR, UEBA
Реагування	Ручні процедури	Автоматизовані процеси, оркестрація	SOAR, автоматизовані системи реагування
Управління вразливостями	Періодичне сканування	Безперервна оцінка ризиків, проактивний підхід	VM з інтеграцією CTI, DevSecOps

Джерело: складено на основі [55]

Важливим елементом адаптивного захисту є впровадження технологій та методів активної кіберрозвідки (Cyber Threat Intelligence, CTI). Цей компонент стратегії забезпечує організації актуальною інформацією про нові типи загроз, тактики, техніки та процедури зловмисників, що дозволяє завчасно адаптувати захисні механізми. Сучасні CTI-платформи забезпечують автоматизований збір, аналіз та поширення даних про загрози з різноманітних джерел, включаючи відкриті джерела, комерційні канали, державні установи та галузеві спільноти. Особливу цінність представляють контекстуалізовані розвіддані, що враховують специфіку конкретної організації, її галузі та географічного розташування. Інтеграція CTI з іншими компонентами системи кібербезпеки дозволяє реалізувати проактивний підхід до захисту, коли системи безпеки автоматично адаптуються до нових загроз ще до того, як вони будуть використані для атак на організацію [58].

Ключовим компонентом адаптивних стратегій є впровадження передових систем виявлення та реагування на загрози, які базуються на поведінковій аналітиці та технологіях машинного навчання. Такі системи, включаючи EDR (Endpoint Detection and Response), NDR (Network Detection and Response) та XDR (Extended Detection and Response), здатні виявляти

складні та раніше невідомі атаки шляхом аналізу аномальної поведінки користувачів, систем та мережевого трафіку. На відміну від традиційних сигнатурних підходів, поведінкова аналітика дозволяє виявляти загрози на основі відхилень від нормальної поведінки, що особливо ефективно проти цільових атак та нових типів шкідливого програмного забезпечення. Інтеграція цих систем з платформами оркестрації та автоматизації безпеки (SOAR) дозволяє виявляти загрози та автоматично реагувати на них, значно скорочуючи час від виявлення до нейтралізації інциденту.

Автоматизація та оркестрація процесів безпеки є невід'ємною частиною сучасних адаптивних стратегій. Платформи SOAR (Security Orchestration, Automation and Response) забезпечують автоматизацію рутинних операцій безпеки, координацію дій різних систем захисту та стандартизацію процесів реагування на інциденти. Використання таких платформ дозволяє суттєво скоротити час реагування на загрози, зменшити вплив людського фактора та підвищити ефективність роботи команд кібербезпеки. Важливим аспектом є інтеграція SOAR з іншими компонентами інфраструктури безпеки, що дозволяє створити єдину екосистему, здатну автоматично адаптуватися до змін у середовищі загроз та ефективно протидіяти різноманітним атакам.

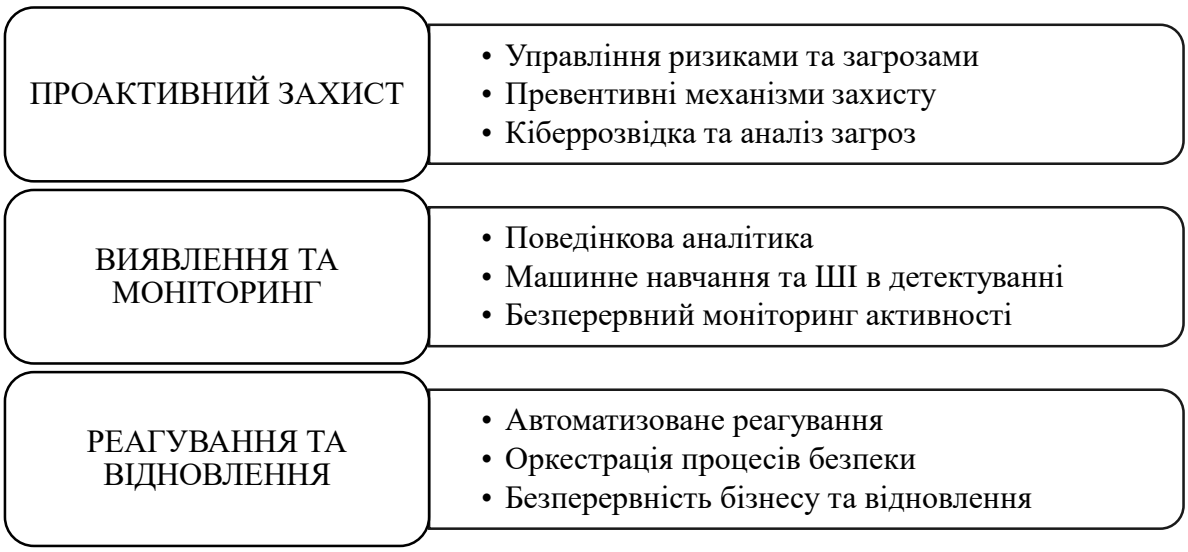

Рисунок 3.1. Структура адаптивної стратегії кібербезпеки

Джерело: складено на основі [53]

Впровадження DevSecOps-підходу представляє собою важливий аспект формування адаптивних стратегій протидії кіберзагрозам у середовищі розробки програмного забезпечення. Цей підхід передбачає інтеграцію практик безпеки на всіх етапах життєвого циклу розробки, що дозволяє виявляти та усувати вразливості на ранніх стадіях, значно знижуючи вартість їх виправлення. Ключовими елементами DevSecOps є автоматизоване тестування безпеки, статичний та динамічний аналіз коду, перевірка залежностей на наявність відомих вразливостей та безперервний моніторинг безпеки. Впровадження цього підходу дозволяє створити "безпеку за замовчуванням", коли питання захисту враховуються на етапі проектування систем, а не додаються як додатковий шар після завершення розробки [43].

Адаптивні стратегії кібербезпеки мають враховувати особливості різних середовищ розгортання, включаючи хмарні платформи, гібридні інфраструктури та середовища Інтернету речей (IoT). Кожне з цих середовищ має унікальні ризики та вимагає специфічних підходів до захисту. Для хмарних платформ ключовими компонентами є захист конфігурацій, управління ідентифікацією та доступом, шифрування даних та моніторинг активності. У контексті IoT важливими аспектами є безпечне оновлення пристроїв, ізоляція мереж, захист від фізичного втручання та мінімізація поверхні атаки. Гібридні середовища потребують узгодженого підходу до безпеки, який забезпечує єдиний рівень захисту незалежно від місця розташування ресурсів.

Важливим аспектом адаптивних стратегій є формування культури кібербезпеки в організації. Програми підвищення обізнаності мають бути адаптовані до різних категорій користувачів та базуватися на актуальних сценаріях загроз. Симуляції фішингових атак, тренінги з реагування на інциденти та регулярне інформування про нові типи загроз допомагають підтримувати високий рівень пильності персоналу. Важливим елементом є також формування чіткої системи відповідальності та заохочення культури відкритого повідомлення про інциденти та потенційні проблеми безпеки.

Оцінка ефективності адаптивних стратегій протидії кіберзагрозам є критично важливим процесом, який дозволяє визначити рівень захищеності організації та виявити напрямки для вдосконалення. Для цього використовуються різноманітні методики, включаючи тестування на проникнення, симуляцію атак (Red Team/Blue Team), аудит відповідності стандартам та аналіз ключових показників ефективності (KPI). Важливими метриками є середній час виявлення загрози (MTTD), середній час реагування (MTTR), кількість успішно запобіжних інцидентів, а також фінансові показники, такі як рентабельність інвестицій у безпеку (ROSI). Регулярний перегляд та коригування стратегії на основі результатів оцінювання дозволяє забезпечити її відповідність актуальним загрозам та вимогам.

3.3. Оцінка ефективності та стійкості систем кібербезпеки

Оцінка ефективності та стійкості систем кібербезпеки є критичним компонентом у забезпеченні надійного захисту інформаційних активів організації. Цей процес дозволяє визначити рівень захищеності інформаційної інфраструктури, виявити потенційні вразливості та сформувати стратегію вдосконалення захисних механізмів. У сучасному динамічному середовищі кібербезпеки, де загрози постійно еволюціонують, традиційні статичні методи оцінки втрачають свою ефективність. Натомість актуальності набувають комплексні методології, що поєднують кількісні та якісні показники, а також враховують специфіку бізнес-процесів організації та її ризик-профіль. Ефективна система оцінки має надавати моментальний зріз стану безпеки та демонструвати динаміку змін, тренди та прогнози щодо майбутніх ризиків [32].

Концептуальною основою оцінки ефективності систем кібербезпеки є визначення ключових показників ефективності (Key Performance Indicators, KPI) та ключових індикаторів ризику (Key Risk Indicators, KRI). KPI дозволяють оцінити, наскільки успішно реалізуються заходи безпеки та в якій

мірі досягаються поставлені цілі. KRI, у свою чергу, фокусуються на моніторингу рівня кіберризиків та ранньому виявленні потенційних загроз. Важливим аспектом є правильний вибір метрик, які повинні бути релевантними, вимірюваними, досяжними, актуальними та обмеженими в часі (відповідно до принципу SMART). Набір метрик має бути збалансованим та охоплювати різні аспекти кібербезпеки, включаючи технічні, організаційні та людські фактори.

Одним із ключових підходів до оцінки ефективності систем кібербезпеки є вимірювання часових показників, пов'язаних з виявленням та реагуванням на інциденти. Середній час виявлення загрози (Mean Time to Detect, MTTD) відображає швидкість ідентифікації потенційних інцидентів, а середній час реагування (Mean Time to Respond, MTTR) вказує на ефективність процесів реагування. Додатковими важливими метриками є середній час відновлення (Mean Time to Recovery, MTTR) та середній час між інцидентами (Mean Time Between Incidents, MTBI). Зниження MTTD та MTTR свідчить про підвищення ефективності захисних механізмів та процесів реагування, в той час як збільшення MTBI є індикатором загального поліпшення рівня безпеки. Важливо враховувати, що ці метрики повинні аналізуватися в контексті інших показників та специфіки організації [44].

Оцінка стійкості систем кібербезпеки передбачає аналіз їх здатності протистояти атакам, адаптуватися до нових загроз та відновлюватися після інцидентів. Стійкість системи визначається наявністю технічних засобів захисту та ефективністю процесів управління безпекою, рівнем підготовки персоналу та здатністю організації швидко відновлювати нормальне функціонування після кібератак. Для оцінки стійкості використовуються такі методики, як аналіз стійкості до відмов (Failure Mode and Effects Analysis, FMEA), тестування на проникнення, моделювання загроз та симуляція атак через методологію "червоної команди" (Red Team). Важливим аспектом є також оцінка здатності системи адаптуватися до нових типів загроз та змін у середовищі.

Таблиця 3.5

Ключові метрики оцінки ефективності систем кібербезпеки

Категорія	Метрика	Опис	Цільове значення
Виявлення	MTTD	Середній час виявлення загрози	< 24 години
Реагування	MTTR	Середній час реагування на інцидент	< 4 години
Відновлення	MTTR (Recovery)	Середній час відновлення після інциденту	< 48 годин
Частота	MTBI	Середній час між інцидентами	> 180 днів
Покриття	NIST CSF	Відсоток відповідності фреймворку NIST	> 85%
Вразливості	Critical VM	Відсоток критичних вразливостей, усунених вчасно	> 95%
Обізнаність	APTR	Відсоток успішності тренувальних фішингових атак	< 5%

Джерело: складено на основі [56]

Економічна оцінка ефективності систем кібербезпеки є важливим аспектом, який дозволяє обґрунтувати інвестиції в захисні механізми та оптимізувати розподіл ресурсів. Основними економічними показниками є рентабельність інвестицій у безпеку (Security Return on Investment, SROI), загальна вартість володіння (Total Cost of Ownership, TCO) та очікувані річні втрати (Annual Loss Expectancy, ALE). Методологія розрахунку SROI включає оцінку як прямих вигод від впровадження систем безпеки (запобігання фінансовим втратам від інцидентів), так і непрямих (зниження репутаційних ризиків, відповідність регуляторним вимогам). Важливим фактором є також оцінка вартості ризику (Cost of Risk), яка враховує потенційні втрати від різних типів кіберінцидентів з урахуванням їх ймовірності та впливу на бізнес [43].

Практичний інструментарій оцінки ефективності та стійкості систем кібербезпеки включає різноманітні методи та технології. Тестування на проникнення (Penetration Testing) дозволяє виявити реальні вразливості в системах захисту шляхом симуляції дій потенційних зловмисників. Аудит конфігурацій та політик безпеки забезпечує перевірку відповідності налаштувань системи встановленим стандартам та найкращим практикам. Аналіз журналів та моніторинг активності дозволяють виявляти аномальну поведінку та потенційні індикатори компрометації. Важливим компонентом є

також оцінка ефективності процесів управління інцидентами через симуляцію атак та проведення навчань з кібербезпеки (Cyber Exercises).

Відповідність регуляторним вимогам та стандартам галузі є важливим аспектом оцінки ефективності систем кібербезпеки. Серед ключових стандартів та фреймворків можна виділити ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls, PCI DSS та GDPR. Кожен з цих документів містить набір вимог та рекомендацій, які можуть бути використані як основа для розробки метрик та критеріїв оцінки. Аудит відповідності проводиться як внутрішніми ресурсами організації, так і зовнішніми незалежними експертами. Важливим аспектом є формальне дотримання вимог та реальна імплементація механізмів захисту та ефективне управління ризиками.

Таблиця 3.6

Моделі оцінки зрілості систем кібербезпеки

Модель	Кількість рівнів	Фокус оцінки	Особливості
CMM (Capability Maturity Model)	5	Процеси управління	Первинна модель, базовий підхід
CMMI (Capability Maturity Model Integration)	5	Інтеграція процесів	Розширена версія CMM
C2M2 (Cybersecurity Capability Maturity Model)	4	Кіберзахист критичної інфраструктури	Галузева спеціалізація, детальні домени
NICE Framework	7	Компетенції персоналу	Фокус на знаннях та навичках
NIST CSF Implementation Tiers	4	Імплементація заходів	Інтеграція з NIST CSF

Джерело: складено на основі [57]

Моделі оцінки зрілості (Maturity Models) є ефективним інструментом для визначення рівня розвитку системи кібербезпеки організації та планування шляхів її вдосконалення. Ці моделі класифікують процеси безпеки за рівнями зрілості, від початкового (ad-hoc) до оптимізованого (continuously improving). Найбільш поширеними є модель зрілості можливостей (Capability Maturity Model, CMM), модель зрілості кібербезпеки (Cybersecurity Capability Maturity Model, C2M2) та модель зрілості NIST CSF.

Сучасні технології та методи аналітики даних відкривають нові можливості для оцінки ефективності та стійкості систем кібербезпеки. Великі дані (Big Data), машинне навчання та штучний інтелект дозволяють аналізувати величезні обсяги інформації про безпекові події, виявляти приховані закономірності та прогнозувати потенційні загрози. Системи предиктивної аналітики здатні виявляти аномалії в поведінці користувачів та систем, що може свідчити про кібератаки на ранніх стадіях. Важливим аспектом є також використання технологій візуалізації даних, які дозволяють представити складну інформацію про стан безпеки в зрозумілому та наочному вигляді, що полегшує прийняття рішень на всіх рівнях управління [59].

Для забезпечення об'єктивності та повноти оцінки ефективності та стійкості систем кібербезпеки необхідно поєднувати кількісні та якісні методи аналізу. Кількісні методи, такі як статистичний аналіз інцидентів, розрахунок фінансових показників та вимірювання часових метрик, надають конкретні числові дані для оцінки. Якісні методи, включаючи експертні оцінки, інтерв'ю з ключовими зацікавленими сторонами та аналіз сценаріїв, дозволяють отримати більш глибоке розуміння контексту та особливостей системи безпеки. Оптимальним підходом є інтеграція цих методів у єдину методологію оцінки, яка забезпечує всебічний аналіз ефективності та стійкості системи кібербезпеки з урахуванням технічних, організаційних та людських аспектів.

Безперервне вдосконалення процесів оцінки ефективності та стійкості систем кібербезпеки є необхідною умовою для підтримки високого рівня захисту в умовах постійної еволюції загроз. Регулярне проведення бенчмаркінгу та порівняння з галузевими показниками дозволяє визначити відносну ефективність системи безпеки та ідентифікувати напрямки для вдосконалення.

ВИСНОВКИ

Таким чином, мета кваліфікаційної роботи була досягнута, на основі чого можна зробити висновки відповідно поставлених завдань.

Кіберзагрози представляють собою комплексний феномен, що постійно еволюціонує за складністю, масштабом та цілями. Їх систематизація за джерелом походження, мотивацією, технічними характеристиками, цільовими активами та векторами атак дозволяє розробити відповідні механізми захисту. Найбільшу небезпеку становлять цілеспрямовані атаки (APT), що комбінують різні техніки проникнення, маскування та закріплення у системах, а також атаки з використанням штучного інтелекту, які здатні адаптуватися до захисних механізмів та обходити традиційні системи виявлення, що вимагає впровадження багаторівневих адаптивних систем захисту з активним використанням методів поведінкової аналітики та машинного навчання.

Моделювання загроз у кіберпросторі виступає фундаментальним процесом для забезпечення проактивного захисту інформаційних активів. Комплексні методології як STRIDE, PASTA, OCTAVE та LINDDUN забезпечують структурований підхід до ідентифікації, аналізу та пріоритизації загроз з урахуванням специфіки архітектури систем, бізнес-процесів та даних. Інтеграція цих методологій з формальними математичними моделями, включаючи марковські процеси, дерева атак та байєсівські мережі, дозволяє створити кількісну основу для оцінки ймовірності, впливу та шляхів реалізації кіберзагроз, що в свою чергу формує надійний фундамент для ефективного розподілу ресурсів та вибору оптимальних захисних механізмів.

Сучасні моделі оцінки ризиків кібербезпеки трансформувалися від статичних підходів до динамічних, контекстно-залежних систем, що враховують постійні зміни у ландшафті загроз та специфіку захищуваних активів. Найбільш ефективними є інтегровані фреймворки, що поєднують кількісні методи (FAIR, RiskLens) з якісними (NIST CSF, ISO/IEC 27005), забезпечуючи всебічний аналіз ймовірності, впливу та вразливостей.

Критичною тенденцією стало впровадження безперервної оцінки ризиків (Continuous Risk Assessment), що використовує автоматизовані платформи з елементами штучного інтелекту для постійного моніторингу, аналізу та прогнозування ризиків у режимі реального часу, дозволяючи організаціям оперативно коригувати стратегії захисту відповідно до актуальних загроз.

Аномаліє-орієнтовані методи виявлення атак демонструють значну ефективність у виявленні невідомих та модифікованих кіберзагроз завдяки їх здатності ідентифікувати відхилення від нормальної поведінки систем, мереж та користувачів. Ключовим аспектом успішного впровадження цих методів є створення точних базових профілів нормальної активності з використанням статистичних моделей, методів кластеризації та нейронних мереж, що дозволяє мінімізувати кількість хибних спрацювань при збереженні високої чутливості до реальних загроз. Інтеграція аномаліє-орієнтованих систем з іншими механізмами виявлення, зокрема сигнатурними та евристичними, в рамках комплексних платформ XDR (Extended Detection and Response) забезпечує мультивекторний підхід до детектування складних та багатоетапних атак з високою точністю та мінімальними затримками.

Машинне навчання кардинально трансформувало підходи до моделювання кіберзагроз, забезпечуючи безпрецедентні можливості для виявлення складних залежностей, прогнозування нових типів атак та автоматизації процесів аналізу. Найбільшу ефективність демонструють гібридні моделі, що поєднують різні алгоритми (глибокі нейронні мережі, випадкові ліси, методи ансамблевого навчання) та адаптуються до змін у ландшафті загроз через механізми самонавчання. Критичним фактором успішного впровадження ML-систем є забезпечення якості та репрезентативності тренувальних даних, а також застосування техніки контрольованого доступу (adversarial machine learning) для підвищення стійкості моделей до атак, спрямованих на обман алгоритмів машинного навчання, що у комплексі дозволяє створити проактивну систему захисту з

високою точністю детектування та мінімальною кількістю хибних спрацювань.

Побудова сценаріїв загроз на основі атака-графів є потужним інструментом моделювання кіберзагроз, що дозволяє візуалізувати та аналізувати потенційні шляхи проникнення зловмисників в інформаційну інфраструктуру. Методологія використання атака-графів забезпечує систематичний підхід до ідентифікації критичних вузлів та шляхів компрометації через аналіз взаємозалежностей між вразливостями, експлойтами та конфігураціями систем. Автоматизація побудови та аналізу атака-графів за допомогою спеціалізованих інструментів та платформ дозволяє ефективно аналізувати складні інфраструктури з численними компонентами, оцінювати ризики різних сценаріїв атак та оптимізувати стратегії захисту шляхом пріоритизації заходів, спрямованих на блокування найбільш ймовірних та небезпечних векторів компрометації.

Ефективні моделі реагування на інциденти у системах кіберзахисту характеризуються ітеративним підходом, що охоплює повний життєвий цикл від підготовки та виявлення до стримування, ліквідації загроз та відновлення. Найбільшу ефективність демонструють гібридні моделі, що інтегрують елементи різних фреймворків (NIST, SANS, ISO/IEC 27035, ENISA) та адаптують їх до специфіки конкретної організації з урахуванням галузевих особливостей та регуляторних вимог. Критичним фактором успіху є впровадження автоматизації процесів реагування через SOAR-платформи, що забезпечують оркестрацію захисних механізмів, мінімізацію часу виявлення (MTTD) та відповіді (MTTR) на інциденти, а також інтеграцію з проактивними технологіями Threat Hunting для раннього виявлення прихованих загроз, що в комплексі формує адаптивну систему кіберзахисту з високою стійкістю до різноманітних типів атак.

Адаптивні стратегії протидії кіберзагрозам базуються на принципі безперервної еволюції захисних механізмів відповідно до змін у ландшафті загроз та бізнес-середовищі організації. Ключовими компонентами успішної

стратегії є інтеграція ризик-орієнтованого підходу, впровадження архітектури нульової довіри (Zero Trust) та багаторівневої системи захисту з глибоким ешелонуванням (Defense in Depth). Ефективність забезпечується через поєднання проактивних механізмів, включаючи активну кіберрозвідку (CTI), поведінкову аналітику та машинне навчання для виявлення загроз, з автоматизованими системами реагування (SOAR). Особливого значення набуває формування цілісної екосистеми безпеки, що охоплює технічні аспекти та організаційні процеси, компетенції персоналу та культуру кібербезпеки, забезпечуючи гнучку адаптацію до нових типів загроз та захист різних середовищ, включаючи хмарні, гібридні інфраструктури та системи Інтернету речей.

Комплексна оцінка ефективності та стійкості систем кібербезпеки потребує збалансованого поєднання кількісних метрик (MTTD, MTTR, SROI) з якісними показниками, що охоплюють технічні, організаційні та людські аспекти. Критичне значення має впровадження моделей оцінки зрілості (CMM, C2M2), що дозволяють систематично аналізувати рівень розвитку процесів безпеки та визначати напрямки вдосконалення. Об'єктивність оцінки забезпечується через практичний інструментарій, що включає тестування на проникнення, симуляцію атак (Red Team/Blue Team) та аудит відповідності регуляторним вимогам і стандартам. Перспективним напрямком є інтеграція методів аналітики великих даних (Big Data) та штучного інтелекту для предиктивного аналізу ефективності захисних механізмів та раннього виявлення потенційних вразливостей, що в комплексі з безперервним вдосконаленням методологій оцінки забезпечує стійкий розвиток системи кібербезпеки організації в умовах постійної еволюції загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Василенко М.Д., Киреєва Н.С. Електронна комерція у проявах юриспруденції (законодавства) та кібербезпеки (несанкціонованих вторгнень): міждисциплінарне дослідження. Наукові праці Національного університету «Одеська юридична академія». 2020. № 26. С. 25–33. http://naukovipraci.nuoua.od.ua/arhiv/tom26/6.pdf

2. Довгань О., Литвинова Л., Дорогих С. (упоряд.) Кібербезпека в інформаційному суспільстві: інформаційно-аналітичний дайджест / Державна наукова установа «Інститут інформації, безпеки і права НАПрН України» ; Національна бібліотека України імені В.І. Вернадського. Київ, 2024. № 3 (березень). 339 с. https://ippi.org.ua/sites/default/files/2024-3.pdf

3. Головкін Б.М., Денькович О.І., Луцик В.В., Цехан Д.М. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навчальний посібник / за редакцією Ольги Денькович, Габріеле Шмельцер. Львів : Львівський національний університет імені Івана Франка, 2022. 298 с. https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

4. Пістунов І.М., Кочура Є.В. Безпека електронної комерції : навчальний посібник. Дніпро : Національний гірничий університет, 2014. 125 с. http://pistunovi.narod.ru/6_E_K.pdf

5. Романюк П. Основні проблеми електронної комерції в умовах цифрової трансформації бізнесу. Цифрова економіка та економічна безпека. 2023. № 4(04). С. 32–37. http://dees.iei.od.ua/index.php/journal/article/view/125

6. Садчикова І., Тарасенко А., Дубина М. Теоретичне обґрунтування сутності поняття «електронна комерція». Економіка та суспільство. 2023. № 53. https://doi.org/10.32782/2524-0072/2023-53-36

7. Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці / С.М. Шевченко та ін. Кібербезпека: освіта, наука, техніка. 2024. № 3(23). С. 258–273.

8. Математичні методи в кібербезпеці: фрактали та їх застосування в інформаційній та кібернетичній безпеці / С.М. Шевченко та ін. Кібербезпека: освіта, наука, техніка. 2019. №1(5). С. 31–39.

9. Шевченко С.М., Жданова Ю.Д., Складанний П.М., Спасітєлєва С.О. Математичні методи в кібербезпеці: графи та їх застосування в інформаційній та кібернетичній безпеці. Кібербезпека: освіта, наука, техніка. 2021. № 1(13). С. 133–144.

10. Шевченко С.М., Складанний П.М., Негоденко О.В., Негоденко В.П. Дослідження прикладних аспектів теорії конфліктів у системах безпеки. Кібербезпека: освіта, наука, техніка. 2022. № 2. С. 150–162.

11. Шевченко С.М., Жданова Ю.Д., Спасітєлєва С.О. Математичні методи в кібербезпеці: теорія катастроф. Кібербезпека: освіта, наука, техніка. 2023. № 3(19). С. 165–175.

12. Шевченко С.М., Жданова Ю.Д., Складанний П.М., Бойко С.В. Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Кібербезпека: освіта, наука, техніка. 2023. № 2(22). С. 168–178.

13. Огляд математичних методів у системах виявлення та попередження кіберзагроз / Н.О. Лисенко та ін. Актуальні проблеми автоматизації та інформаційних технологій. 2021. № 25. С. 91–102.

14. Лаптєв О.А., Степаненко В.І., Тихонов Ю.О. Формальні математичні моделі для забезпечення безпеки інформації. Сучасний захист інформації. 2019. №1(37). С. 59–63.

15. Тишик І.Я. Забезпечення безпеки облікових записів корпоративних користувачів. Кібербезпека: освіта, наука, техніка. 2023. № 2(22). С. 214–225.

16. Баранов О. А. Про тлумачення та визначення поняття “кібербезпека”. Правова інформатика, 2014, № 2 (42), с. 54–62.

17. Бєгун А. В. Інформаційна безпека : навч. посібник. Київ : КНЕУ, 2008. 280 с.

18. Гвоздьов Р. Ю., Олійников Р. В. Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах. Радіотехніка, 2020, № 203, с. 91–96.

19. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посібник. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.

20. Державний центр кіберзахисту ДССЗЗІ України. URL: https://scpc.gov.ua/uk/articles/318

21. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова КМУ від 23.12.2020 № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text

22. Жарикова А. Кількість кібератак у 2023 році зросла на 16 % – Держспецзв'язку. Економічна правда, 2024. URL: https://www.epravda.com.ua/news/2024/01/31/709355/

23. Інтелектуальні інформаційні системи: структура і застосування : підручник / О. М. Величко, Т. Б. Гордієнко. Херсон : Олді плюс, 2021. 727 с.

24. Кібербезпека бізнесу під час війни. Мінфін. URL: https://www.project.minfin.com.ua/kiberbezpekabiznesu-pid-chas-vijny

25. Когут Ю. І. Цифрова трансформація економіки та проблеми кібербезпеки : практич. посібник. Київ : СІДКОН, 2021. 368 с.

26. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2003. 472 с.

27. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посібник. Київ : Кондор, 2019. 272 с.

28. Марущак А. І. Інформаційне право. Доступ до інформації : навч. посібник. Київ : КНТ, 2007. 280 с.

29. Нашинець-Наумова А. Ю. Організаційно-правові методи забезпечення інформаційної безпеки корпорацій. Підприємництво, господарство і право, 2015, № 11, с. 21–24.

30. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації. URL: https://tzi.ua/assets/files/1.1_003_99.pdf

31. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf

32. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем. URL: https://tzi.com.ua/downloads/2.5-005%20-99.pdf

33. НД ТЗІ 1.4–001-2000. Типове положення про службу захисту інформації. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf

34. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

35. Про основні засади забезпечення кібербезпеки України: Закон України. ВВР, 2017, № 45, ст.403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

36. Проєкт Закону України від 14.04.2016 № 2126а. URL: https://ips.ligazakon.net/document/JH1N268B?an=11

37. Про Раду національної безпеки і оборони України. Закон України. ВВР, 1998, № 35, ст. 237. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

38. Радутний О. Е. Кримінальна відповідальність штучного інтелекту. Інформація і право, 2018, № 2 (21), с. 124–133. https://ippi.org.ua/sites/default/files/14boavpk.pdf

39. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. ЄБА, 2024. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannyaatakam/

40. Сальник В. В. та ін. Методика оцінки порушень захищеності. Збірник праць ХНУПС, 2021, № 4(70), с. 77–82. https://doi.org/10.30748/zhups.2021.70.11

41. Стан, досягнення та перспективи інформаційних систем і технологій: матеріали XXII Всеукр. конф. Одеса, 2022. С. 58–60. https://card-file.ontu.edu.ua/items/a34a6bd6-2f11-45b9-95b6-d781c0cc6341

42. Кібербезпека в інформаційному суспільстві: інформаційно-аналітичний дайджест. Київ : ІІБП НАПрН України, 2024. № 4 (квітень). 320 с.

43. Талліннський механізм: новий інструмент співпраці у кіберпросторі. Урядовий портал, 2023. URL: https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-tamizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori

44. Ukraine. National Cyber Security Index. URL: https://ncsi.ega.ee/country/ua/

45. of a Data Breach Report (2023). IBM. URL: https://www.ibm.com/reports/data-breach

46. What is cybersecurity? IBM. URL: https://www.ibm.com/topics/cyber

47. Gaining the advantage. Applying Cyber Kill Chain Methodology to Network Defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

48. Singh V. K., Govindarasu M. Cyber Kill Chain-Based Hybrid Intrusion Detection System for Smart Grid. In Wide Area Power Systems Stability, Protection, and Security; Springer: Cham, Switzerland, 2021, pp. 571–599. http://dx.doi.org/10.1007/978-3-030-54275-7_22

49. What is ATT&CK? MITRE. URL: https://attack.mitre.org/

50. Roy S., Panaousis E., Noakes C., Laszka A., Panda S., Loukas G. (2023). SoK: The MITRE ATT&CK Framework in Research and Practice. https://doi.org/10.48550/arXiv.2304.07411

51. Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks–undermining public confidence in government. Journal of Information Technology and Politics, 20(4), 359–374. https://doi.org/10.1080/19331681.2022.2112796

52. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023, March 1). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics (Switzerland). MDPI. https://doi.org/10.3390/electronics12061333

53. Jin, J., Li, N., Liu, S., & Khalid Nainar, S. M. (2023). Cyber attacks, discretionary loan loss provisions, and banks' earnings management. Finance Research Letters, 54. https://doi.org/10.1016/j.frl.2023.103705

54. Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers and Security, 124. https://doi.org/10.1016/j.cose.2022.102954

55. AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. International Journal of Advanced Computer Science and Applications, 14(2), 801–809. https://doi.org/10.14569/IJACSA.2023.0140292

56. Dimitriadis, A., Lontzetidis, E., Kulvatunyou, B., Ivezic, N., Gritzalis, D., & Mavridis, I. (2023). Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks. IEEE Access, 11, 728–743. https://doi.org/10.1109/ACCESS.2022.3233404

57. Salih, A. A., & Abdulrazzaq, M. B. (2023). Cyber security: performance analysis and challenges for cyber attacks detection. Indonesian Journal of Electrical Engineering and Computer Science, 31(3), 1763–1775. https://doi.org/10.11591/ijeecs.v31.i3.pp1763-1775

58. Tatipatri, N., & Arun, S. L. (2024). A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security. IEEE Access, 12, 18147–18167. https://doi.org/10.1109/ACCESS.2024.3361039

59. Feng, Z., Li, Y., & Ma, X. (2023). Blockchain-oriented approach for detecting cyber-attack transactions. Financial Innovation, 9(1). https://doi.org/10.1186/s40854-023-00490-6

ДОДАТКИ

Додаток А. Порівняння технічних параметрів сучасних систем захисту від кіберзагроз

Тип системи	Технологічна база	Метрики продуктивності	Ефективність виявлення (%)	Час обробки (мс)	Хибно-позитивні (%)	Вимоги до ресурсів	Інтеграційні можливості
NGFW (Next-Generation Firewall)	Глибока інспекція пакетів, аналіз додатків	Пропускна здатність: 1-100 Гбіт/с, Затримка: 50-500 мкс	75-85% для відомих загроз, 40-60% для невідомих	100-500	0.1-0.5	CPU: 4-32 ядер, RAM: 16-128 ГБ	API, SIEM, CTI
EDR (Endpoint Detection & Response)	Поведінковий аналіз, машинне навчання	Навантаження на CPU: 1-5%, Затримка: 10-100 мс	80-95% для відомих загроз, 60-80% для невідомих	200-1000	0.05-2.0	CPU: 1-2 ядра, RAM: 2-4 ГБ на агент	SOAR, SIEM, XDR
NDR (Network Detection & Response)	ML, аналіз потоків, декодування протоколів	Обсяг аналізу: 10-100 ГБ/добу, Затримка: 1-10 с	70-90% для відомих загроз, 50-75% для невідомих	500-5000	0.5-3.0	CPU: 8-64 ядер, RAM: 32-256 ГБ	EDR, SIEM, SOAR
SIEM (Security Information & Event Management)	Кореляція подій, аналітика журналів	EPS: 5,000-100,000, Зберігання: 1-100 ТБ	65-85% для відомих загроз, 30-50% для невідомих	1000-10000	1.0-5.0	CPU: 16-128 ядер, RAM: 64-512 ГБ	Всі системи безпеки
UEBA (User & Entity Behavior Analytics)	Поведінкова аналітика, ML/AI	Обсяг аналізу: 5-50 ГБ/добу, Навчання: 2-4 тижні	75-90% для інсайдерських загроз, 65-85% для компрометації облікових записів	2000-8000	0.1-1.0	CPU: 8-32 ядер, RAM: 32-128 ГБ	IAM, SIEM, EDR

SOAR (Security Orchestration & Automated Response)	Автоматизація процесів, оркестрація	Час автоматизації: 80-95% задач, Playbooks: 50-500	85-95% для стандартних інцидентів, 60-80% для складних	500-2000	0.05-0.5	CPU: 8-32 ядер, RAM: 32-128 ГБ	Всі системи безпеки
DLP (Data Loss Prevention)	Контент-аналіз, категоризація даних	Пропускна здатність: 100-1000 Мбіт/с, Точність класифікації: 80-95%	70-90% для структурованих даних, 50-75% для неструктурованих	50-500	2.0-8.0	CPU: 4-16 ядер, RAM: 16-64 ГБ	CASB, IAM, SIEM
WAF (Web Application Firewall)	Аналіз HTTP/HTTPS, сигнатури OWASP Top 10	Пропускна здатність: 500-5000 RPS, Затримка: 1-10 мс	80-95% для відомих атак, 50-70% для 0-day	5-50	0.5-3.0	CPU: 4-16 ядер, RAM: 8-32 ГБ	SIEM, SOAR, CTI
CTI платформи (Cyber Threat Intelligence)	Аналіз загроз, індикатори компрометації	Обсяг індикаторів: 10^6-10^8, Оновлення: 5-60 хв	75-90% точність предикції загроз, 60-80% покриття нових загроз	Н/Д	1.0-4.0	CPU: 8-32 ядер, RAM: 32-128 ГБ	Всі системи безпеки
XDR (Extended Detection & Response)	Інтеграція EDR, NDR, SIEM, аналітика	Єдина консоль: 90-99% видимість, Сореляція: крос-платформна	85-95% для відомих загроз, 70-85% для невідомих	200-2000	0.05-1.0		

ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ (ПРЕЗЕНТАЦІЯ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних Технологій

Методи моделювання кіберзагроз та стратегій реагування для забезпечення високого рівня кібербезпеки

Виконала: студентка групи САД-41 Ольшевська Вероніка

Керівник: Нафєєв Ровіл

Київ-2025

Мета роботи полягає у формуванні системного уявлення про методи моделювання кіберзагроз і побудову ефективних стратегій реагування для забезпечення стійкості та високого рівня кібербезпеки інформаційних систем.

Об’єкт дослідження — процеси формування, розвитку та нейтралізації кіберзагроз у сучасних інформаційних системах.

Предмет дослідження — методи моделювання кіберзагроз і стратегії реагування, спрямовані на забезпечення високого рівня кіберстійкості.

Поняття та класифікація кіберзагроз

Поняття кіберзагрози належить до категорії фундаментальних у сфері інформаційної безпеки та має складну багаторівневу структуру, що охоплює технічні, поведінкові, правові та організаційні компоненти. В умовах інтенсивної цифровізації діяльності більшості суспільних інститутів постала необхідність у точному концептуальному визначенні загроз, що виникають у кіберпросторі, з урахуванням їх еволюційного характеру та потенційної шкоди.

Підхід	Ключові характеристики
Технократичний	Орієнтація на вразливості ПЗ, мережеву активність, сигнатури
Системно-поведінковий	Аналіз взаємодії між об'єктами, користувачами та середовищем
Юридико-нормативний	Інтерпретація загроз через призму правових наслідків та норм
Організаційно-функціональний	Розгляд загроз у контексті управління ризиками й стратегіями
Геополітичний	Кіберзагроза як інструмент протидії між державними суб’єктами

Методологічні підходи до моделювання загроз у кіберпросторі

Методологічна основа моделювання кіберзагроз охоплює широкий спектр наукових та прикладних підходів, які спрямовані на аналіз можливих сценаріїв шкідливого впливу в кіберпросторі, їхню структуризацію, прогнозування та визначення потенційної шкоди. Ефективне моделювання є ключовим етапом у створенні системи управління ризиками, оскільки дозволяє формувати проактивні стратегії реагування, адаптивні алгоритми протидії, ресурсоорієнтовані заходи щодо локалізації інцидентів.

Огляд сучасних моделей оцінки ризиків кібербезпеки

Сучасні цифрові середовища характеризуються високим ступенем взаємозалежності, що ускладнює виявлення первинних джерел загроз і масштабування їхнього впливу. Ризик у цьому контексті розглядається як функція від імовірності реалізації кіберзагрози та очікуваних наслідків для критичних активів. Для адекватної оцінки такого ризику необхідно залучати технічні параметри та організаційні, поведінкові та правові змінні.

Назва моделі	Основні характеристики	Приклади застосування
CVSS	Статична шкала оцінювання вразливостей за фіксованими критеріями	Класифікація загроз у системах управління патчами
FAIR (Factor Analysis of Information Risk)	Кількісна оцінка інформаційного ризику з урахуванням фінансових наслідків	Аудит кіберстрахування
Bayesian Risk Assessment	Ймовірнісна модель із динамічним оновленням залежностей між подіями	Аналіз складних комбінованих атак
Risk Matrix	Таблична оцінка за шкалами імовірності та впливу	Побудова політик доступу
Fuzzy Logic-based Models	Нечіткі множини для оцінки ситуацій із високою невизначеністю	Анонімні атаки, недостатність даних
Attack Tree Quantification	Ієрархічна структура можливих шляхів атаки з розрахунком критичності	Проєктування систем безпеки

Аномаліє-орієнтовані методи виявлення атак

Аномаліє-орієнтовані методи виявлення атак представляють клас підходів кіберзахисту, заснованих на ідентифікації відхилень від нормальної поведінки системи. На відміну від сигнатурних методів, вони здатні виявляти атаки нульового дня без попереднього опису їх шаблонів. Основний принцип функціонування полягає у створенні багатовимірного профілю нормальної мережевої активності за допомогою математичних моделей та алгоритмів машинного навчання.

Використання машинного навчання у моделюванні кіберзагроз

Машинне навчання стало фундаментальним підходом до моделювання кіберзагроз, забезпечуючи автоматизацію виявлення та прогнозування атак завдяки здатності алгоритмів навчатися з даних. Сучасні системи кібербезпеки активно використовують різноманітні методи ML для ідентифікації шкідливого коду, виявлення аномалій мережевого трафіку, розпізнавання поведінкових патернів зловмисників та прогнозування нових векторів атак.

Алгоритм	Точність	AUC-ROC	F1-score	Переваги	Обмеження	Тип загроз
Random Forest	96.7%	0.98	0.95	Стійкість до шуму, швидкість	Проблеми з розмірністю	Мережеві атаки
XGBoost	97.5%	0.99	0.96	Висока точність, робастність	Вимоги до пам'яті	Множинні типи атак
LSTM	94.2%	0.97	0.93	Темпоральні залежності	Обчислювальна складність	APT, багатоетапні атаки
CNN-LSTM	95.3%	0.98	0.94	Просторово-часові ознаки	Складність налаштування	DDoS, zero-day
Graph Neural Networks	94.8%	0.96	0.93	Мережеві взаємозв'язки	Проблеми масштабування	Lateral movement, APT
Transformer	98.1%	0.99	0.97	Паралельна обробка, увага	Ресурсомісткість	Складні атаки, RAT
VAE	91.2%	0.94	0.89	Виявлення невідомих атак	Нижча точність	Zero-day, нові вектори
BERT NLP	96.4%	0.98	0.95	Аналіз текстових логів	Затрати на навчання	Соціальна інженерія, фішинг

Розроблення сценаріїв загроз на основі атака-графів

Атака графа — це спроба порушити роботу або захопити контроль над системою, представленою у вигляді графа, через зміну, видалення або додавання вузлів (пристроїв) або ребер (з’єднання).

Моделі реагування на інциденти у системах кіберзахисту

Реагування на інциденти кібербезпеки є комплексним процесом, що вимагає чіткої структури та методології. Побудова ефективних моделей реагування базується на розумінні життєвого циклу інциденту, його особливостей та потенційних наслідків для інформаційної інфраструктури. У сучасному кіберпросторі, де загрози постійно еволюціонують та стають більш складними, традиційні моделі реагування потребують постійного вдосконалення та адаптації до нових умов.

Параметр	Модель NIST	Модель ENISA	Модель SANS	ISO/IEC 27035
Кількість фаз	4 фази	5 фаз	6 фаз	5 фаз
Особливості підготовчого етапу	Створення політик, планів, навчання персоналу	Акцент на документуванні та юридичній складовій	Фокус на інструментах та технологіях	Системний підхід до планування
Підхід до класифікації інцидентів	За джерелом загрози, типом атаки та впливом	За галузевою специфікою та регуляторними вимогами	За тактичними особливостями атаки	За рівнем критичності та масштабом впливу
Оцінка успішності реагування	Через зменшення часу виявлення та відновлення	Через відповідність регуляторним вимогам	Через технічні метрики	Через відповідність встановленим KPI
Інтеграція з іншими процесами	Середній рівень	Високий рівень	Середній рівень	Дуже високий рівень
Адаптивність	Помірна	Висока	Висока	Середня
Орієнтація на тип організації	Універсальна	Спеціалізована для європейського контексту	Технічно-орієнтована	Універсальна

Формування адаптивних стратегій протидії кіберзагрозам

Сучасне середовище кібербезпеки характеризується динамічними змінами та постійною еволюцією загроз, що вимагає від організацій впровадження гнучких та адаптивних стратегій захисту. Під адаптивними стратегіями протидії кіберзагрозам розуміють комплекс методів, технологій та організаційних заходів, здатних оперативно пристосовуватися до змін у ландшафті загроз та ефективно нейтралізувати нові вектори атак.

Оцінка ефективності та стійкості систем кібербезпеки

Одним із ключових підходів до оцінки ефективності систем кібербезпеки є вимірювання часових показників, пов'язаних з виявленням та реагуванням на інциденти. Середній час виявлення загрози (Mean Time to Detect, MTTD) відображає швидкість ідентифікації потенційних інцидентів, а середній час реагування (Mean Time to Respond, MTTR) вказує на ефективність процесів реагування.

Категорія	Метрика	Опис	Цільове значення
Виявлення	MTTD	Середній час виявлення загрози	< 24 години
Реагування	MTTR	Середній час реагування на інцидент	< 4 години
Відновлення	MTTR (Recovery)	Середній час відновлення після інциденту	< 48 годин
Частота	MTBI	Середній час між інцидентами	> 180 днів
Покриття	NIST CSF	Відсоток відповідності фреймворку NIST	> 85%
Вразливості	Critical VM	Відсоток критичних вразливостей, усунених вчасно	> 95%
Обізнаність	APTR	Відсоток успішності тренувальних фішингових атак	< 5%

Висновки

У процесі виконання дипломної роботи **«Методи моделювання кіберзагроз та стратегій реагування для забезпечення високого рівня кібербезпеки»** мною було сформовано комплексне уявлення про сучасні кіберзагрози, методи їх моделювання та ефективні стратегії реагування.

Я дослідила особливості класифікації загроз, методологію побудови моделей на основі машинного навчання, а також принципи формування адаптивних стратегій протидії. Окрема увага приділялася оцінці ефективності систем кіберзахисту за допомогою показників MTTD та MTTR.

Також я брала участь в конференції, де представила тези дипломного дослідження.

Результати дослідження можуть бути використані в практиці розробки гнучких та стійких систем кібербезпеки в умовах швидкозмінного цифрового середовища.

НОРМКОНТРОЛЬ ПРОЙДЕНО ПІБ ПЕРЕВІРЯЮЧОГО