МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ПОДІЙ БЕЗПЕКИ ДЛЯ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Ірина Наріжна
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Ірина НАРІЖНА
Ім’я, ПРІЗВИЩЕ

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

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

Київ 2026

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз джерел, нормативної й технічної бази	30.03.2026	
3.	Аналіз теоретичних основ забезпечення кіберстійкості об’єктів критичної інформаційної інфраструктури	21.02.2026	
4.	Аналіз методів інтелектуального аналізу подій інформаційної безпеки	15.03.2026	
5.	Розробка підходу до інтелектуального аналізу подій безпеки і оцінювання ефективності запропонованого підходу	17.03.2026	
6.	Формування висновків, списку джерел, додатків	20.04.2026	
7.	Остаточне редагування, перевірка та підготовка до захисту	10.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	05.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Ірина НАРІЖНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

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

Направляється здобувачка Наріжна І.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Методи інтелектуального аналізу подій безпеки для підвищення кіберстійкості об'єктів критичної інформаційної інфраструктури ”
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка НАРІЖНА Ірина у кваліфікаційній роботі дослідила теоретичні основи забезпечення кібербезпеки об’єктів критичної інфраструктури, проаналізувала існуючі методи інтелектуального аналізу подій безпеки, розробила алгоритм моделі інтелектуального аналізу подій безпеки та пропозиції по його застосуванню.

НАРІЖНА Ірина показала розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довела володіння методами наукового дослідження, проявила себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки НАРІЖНОЇ І.В. на оцінку “добре” та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

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

“___“_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Наріжна І.В,. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти Наріжної Ірини
на тему “ Методи інтелектуального аналізу подій безпеки для підвищення кіберстійкості об'єктів критичної інформаційної інфраструктури ”

Актуальність обраної теми обумовлена зростанням кількості та складності кіберзагроз, спрямованих на об'єкти критичної інформаційної інфраструктури, функціонування яких безпосередньо впливає на національну безпеку, економічну стабільність та безперервність надання суспільно важливих послуг. У таких умовах особливого значення набувають засоби автоматизованого виявлення аномалій та прихованих закономірностей у великих масивах подій безпеки

Позитивні сторони.

1. У роботі розглянуто сучасні підходи до формування кіберстійкості, основні категорії загроз, принципи функціонування систем моніторингу безпеки та особливості захисту критичних інформаційних ресурсів, визначено основні вимоги до систем виявлення та аналізу кіберінцидентів. Проведено порівняльний аналіз існуючих підходів, визначено їх переваги, недоліки та перспективи застосування для задач забезпечення кіберстійкості критичної інфраструктури
2. Кваліфікаційна робота оформлена відповідно до встановлених вимог. Матеріал викладено послідовно та логічно, сформульовано обґрунтовані висновки. Основні положення роботи представлено у вигляді таблиць і рисунків.

Недоліки.

Разом із позитивними сторонами роботи доцільно відзначити окремі зауваження. Зокрема, результати експериментального оцінювання могли б бути додатково підтверджені на більшому обсязі реальних даних кібермоніторингу, а також доцільним було б розширення порівняльного аналізу запропонованого підходу з сучасними рішеннями, що використовуються в комерційних системах управління подіями безпеки (SIEM). Проте зазначені зауваження не мають принципового характеру та не знижують загальної позитивної оцінки виконаної роботи

Разом із позитивними сторонами роботи доцільно відзначити окремі зауваження. Зокрема, результати порівняння могли б бути додатково підтверджені на більшому обсязі реальних даних кібермоніторингу, а також доцільним було б розширення порівняльного аналізу запропонованого підходу з сучасними рішеннями, що використовуються в комерційних системах управління подіями безпеки (SIEM). Проте зазначені зауваження не мають принципового характеру та не знижують загальної позитивної оцінки виконаної роботи

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “добре”, а здобувачка НАРІЖНА Ірина заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

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

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів інтелектуального аналізу подій безпеки для підвищення кіберстійкості об’єктів критичної інформаційної інфраструктури. Робота складається зі вступу, чотирьох розділів, що містять 6 рисунків, 13 таблиць, висновків, списку використаних джерел із 39 найменувань та 2 додатків. Загальний обсяг роботи становить 102 аркуші, з яких 5 аркушів займає список використаних джерел.

Метою роботи є дослідження сучасних методів інтелектуального аналізу подій інформаційної безпеки, аналіз їх застосування для моніторингу та виявлення кіберзагроз, а також розробка рекомендацій підвищення кіберстійкості об’єктів критичної інформаційної інфраструктури.

Об’єктом дослідження процеси моніторингу, аналізу та обробки подій інформаційної безпеки в інформаційно-комунікаційних системах об’єктів критичної інформаційної інфраструктури.

Предмет дослідження – методи інтелектуального аналізу подій безпеки (методи машинного навчання, аналізу аномалій та кореляції подій), що застосовуються для підвищення кіберстійкості інформаційних систем критичної інфраструктури.

Методи дослідження. Для вирішення поставлених завдань у роботі використано методи аналізу та узагальнення наукових і нормативних джерел, системного та порівняльного аналізу, моделювання загроз, методи інтелектуального аналізу даних, машинного навчання, виявлення аномалій, а також експериментальне оцінювання ефективності запропонованого підходу.

Як результат у роботі досліджено теоретичні основи забезпечення кіберстійкості об’єктів критичної інформаційної інфраструктури; проаналізовано основні джерела подій безпеки та сучасні методи їх інтелектуального аналізу; визначено особливості використання засобів моніторингу безпеки SIEM, SOC та IDS/IPS; сформовано структуру набору даних подій безпеки та підхід до їх підготовки для аналізу; розроблено модель інтелектуального аналізу подій безпеки на основі виявлення аномалій і

контекстного ранжування; виконано реалізацію алгоритму та проведено його експериментальне оцінювання; сформульовано практичні рекомендації щодо застосування запропонованого підходу для підвищення кіберстійкості критичної інформаційної інфраструктури.

Галузь застосування. Отримані результати можуть бути використані підрозділами інформаційної та кібербезпеки підприємств, установ і організацій, зокрема на об’єктах критичної інфраструктури, для вдосконалення процесів моніторингу подій безпеки, виявлення кіберінцидентів, зниження кількості хибнопозитивних спрацювань, підвищення ефективності реагування на загрози та підтримки кіберстійкості інформаційно-комунікаційних систем.

Ключові слова: КРИТИЧНА ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА, КІБЕРСТІЙКІСТЬ, ПОДІЇ БЕЗПЕКИ, МОНІТОРИНГ БЕЗПЕКИ, ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ, МАШИННЕ НАВЧАННЯ, ВИЯВЛЕННЯ АНОМАЛІЙ, КОРЕЛЯЦІЯ ПОДІЙ, SIEM, SOC, IDS/IPS, PYTHON.

ABSTRACT

The qualification work is devoted to the study of the impact of the human factor on the effectiveness of the information security management system. The work consists of an introduction, three chapters containing 5 figures, 1 table, conclusions and the list of references containing 42 items. The total volume of the work is 69 pages, of which 4 pages is occupied by the list of references.

The purpose of the study is to investigate modern methods of intelligent analysis of information security events, analyse their application for monitoring and detecting cyber threats, and develop recommendations for improving the cyber resilience of critical information infrastructure objects.

The object the study is the processes of monitoring, analysing and processing information security events in information and communication systems of critical information infrastructure objects.

The subject of the study is the methods of intelligent analysis of security events, including machine learning methods, anomaly detection and event correlation, used to improve the cyber resilience of information systems of critical infrastructure.

Research methods. To solve the tasks set in the work, methods of analysis and generalisation of scientific and regulatory sources, system and comparative analysis, threat modelling, intelligent data analysis methods, machine learning, anomaly detection, as well as experimental evaluation of the effectiveness of the proposed approach were used.

As a result**,** the work investigates the theoretical foundations of ensuring the cyber resilience of critical information infrastructure objects; analyses the main sources of security events and modern methods of their intelligent analysis; identifies the specific features of using security monitoring tools such as SIEM, SOC and IDS/IPS; forms the structure of a security event dataset and an approach to its preparation for analysis; develops a model for intelligent analysis of security events based on anomaly detection and context-aware ranking; implements the algorithm and carries out its experimental evaluation; and formulates practical recommendations for applying the

proposed approach to improve the cyber resilience of critical information infrastructure.

Field of application. The results obtained can be used to improve the cybersecurity management systems of enterprises, institutions and organisations, as well as to automate the processes of threat analysis, risk assessment and decision support in the context of modern cyber threats.

The purpose of the study is to investigate and develop a decision-support model in the field of cybersecurity based on artificial intelligence technologies, with a view to improving the effectiveness of cyber-threat detection, risk assessment and response to security incidents.

The object the study is the decision-support process in cybersecurity management systems.

The subject of the study is the models, methods and algorithms of artificial intelligence used to support decision-making in the field of cybersecurity.

Research methods. To address the objectives set out in this work, methods of analysis and synthesis, comparison, classification, modelling, risk assessment, statistical analysis and machine learning were employed, as well as a systematic approach to constructing decision support models in the field of cybersecurity.

As a result, this study examines the theoretical foundations of decision support systems and artificial intelligence technologies in cybersecurity; analyses modern decision support methods and machine learning algorithms for detecting security incidents; identifies the main shortcomings and limitations of existing approaches; an architecture for an artificial intelligence-based decision support model has been developed; it has been implemented and tested using the analysis of cyber incidents as an example; recommendations have been formulated for the implementation of the model into a cybersecurity management system.

Field of application. The obtained results can be used by information and cybersecurity units of enterprises, institutions and organisations, in particular at critical infrastructure facilities, to improve security event monitoring processes, detect cyber incidents, reduce the number of false positives, increase the effectiveness of threat

response, and support the cyber resilience of information and communication systems.

***Keywords*:** CRITICAL INFORMATION INFRASTRUCTURE, CYBER RESILIENCE, SECURITY EVENTS, SECURITY MONITORING, INTELLIGENT DATA ANALYSIS, MACHINE LEARNING, ANOMALY DETECTION, EVENT CORRELATION, SIEM, SOC, IDS/IPS, PYTHON.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AI	**Artificial Intelligence (штучний інтелект)**
API	Application Programming Interface (інтерфейс прикладного програмування)
CERT-UA	Урядова команда реагування на комп'ютерні надзвичайні події України
CSF	Cybersecurity Framework
CISA	Cybersecurity and Infrastructure Security Agency
CSV	Comma-Separated Values
DMARC	Domain-based Message Authentication, Reporting & Conformance
ENISA	European Union Agency for Cybersecurity
HMI	Human-Machine Interface (людино-машинний інтерфейс)
ICS	Industrial Control Systems (промислові системи керування)
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPFIX	Internet Protocol Flow Information Export
KII	Критична інформаційна інфраструктура
ML	Machine Learning (машинне навчання)
NetFlow	Технологія експорту статистики мережевих протоколів
NIST	National Institute of Standards and Technology
OT	Operational Technology (операційні технології)
PLC	Programmable Logic Controller (програмований логічний контролер)
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operations Center
TLS	Transport Layer Security
VPN	Virtual Private Network

ВСТУП

Актуальність теми. Дослідження зумовлена тим, що критична інформаційна інфраструктура стала базовим цифровим контуром функціонування держави, економіки та суспільства. Енергетика, транспорт, зв’язок, державні реєстри, промислові та сервісні інформаційні системи працюють у режимі постійної взаємодії з великою кількістю мережевих, прикладних і технологічних компонентів. За таких умов кіберінцидент дедалі рідше проявляється як поодиноке порушення безпеки окремого вузла. Значно частіше він розгортається як складний ланцюг подій, розподілених у часі, між різними джерелами журналювання та сегментами інфраструктури. Саме це створює потребу у використанні методів інтелектуального аналізу подій безпеки, здатних виявляти слабкі сигнали загроз, аномальні патерни та приховані залежності між подіями. Для об’єктів критичної інфраструктури проблема має особливу вагу через поєднання IT- та OT-середовищ, складну архітектуру зв’язків між сервісами, обмежену можливість зупинення технологічних процесів і високу ціну помилки під час реагування. Класичні правилові механізми моніторингу залишаються необхідними, однак у 2025–2026 роках їх дедалі частіше недостатньо для раннього виявлення багатоступеневих атак, прихованого закріплення в мережі, компрометації облікових записів, зловживання довіреними сервісами та аномальної взаємодії між IT- і OT-рівнями. У зв’язку з цим науковопрактичного значення набуває розробка підходів, які поєднують збір і нормалізацію телеметрії, побудову ознакового простору, виявлення відхилень, контекстне ранжування аномалій та подальшу підтримку рішень у SOC або SIEM-середовищі.

Метою роботи є дослідження сучасних методів інтелектуального аналізу подій інформаційної безпеки, аналіз можливостей їх застосування для моніторингу та виявлення кіберзагроз, а також розробка підходу до підвищення кіберстійкості об’єктів критичної інформаційної інфраструктури.

Для досягнення поставленої мети в роботі визначено такі завдання: проаналізувати роль критичної інформаційної інфраструктури у системі забезпечення національної безпеки та визначити основні кіберзагрози для її інформаційних систем; дослідити сучасні підходи до моніторингу подій інформаційної безпеки в інформаційних системах і мережах; провести аналіз методів інтелектуального аналізу даних, що застосовуються для виявлення кіберзагроз і аномальної поведінки; дослідити можливості застосування систем моніторингу безпеки SIEM, IDS/IPS та організаційних функцій SOC для аналізу подій інформаційної безпеки; розробити модель або підхід до інтелектуального аналізу подій безпеки з використанням методів машинного навчання й аномального аналізу; провести оцінювання ефективності запропонованого підходу для виявлення кіберінцидентів; сформувати практичні рекомендації щодо підвищення кіберстійкості об’єктів критичної інформаційної інфраструктури.

Об’єктом дослідження є процеси моніторингу, аналізу та обробки подій інформаційної безпеки в інформаційно-комунікаційних системах об’єктів критичної інформаційної інфраструктури.

Предметом дослідження є методи інтелектуального аналізу подій безпеки, зокрема методи машинного навчання, виявлення аномалій і кореляції подій, що застосовуються для підвищення кіберстійкості інформаційних систем критичної інфраструктури.

Методи дослідження охоплюють аналіз і узагальнення наукових та нормативних джерел, системний аналіз інформаційних і технологічних контурів КІІ, порівняльний аналіз методів обробки подій безпеки, моделювання загроз, методи інтелектуального аналізу даних, а також експериментальне оцінювання роботи запропонованого алгоритму на тестовому наборі подій безпеки. 17 Наукова новизна одержаних результатів полягає у формуванні гібридного підходу до інтелектуального аналізу подій безпеки, який поєднує аномальне виявлення, побудову ознакового простору для багаторівневої телеметрії, контекстне ранжування подій з урахуванням критичності активу та придатність

до інтеграції із сучасними системами моніторингу безпеки. Запропонований підхід орієнтовано на умови гібридного IT/OT-середовища та на раннє виявлення сценаріїв, що становлять підвищений ризик для критичних функцій об’єкта.

Практичне значення отриманих результатів полягає у можливості використання розробленої логіки формування набору даних, побудови ознак, виявлення аномалій і контекстного ранжування в навчальних, тестових та наближених до експлуатаційних середовищах моніторингу безпеки. Запропоновані таблиці, схеми, алгоритмічна модель і рекомендації можуть бути використані під час підготовки організаційних рішень щодо модернізації SIEM/SOC-контуру, удосконалення процедур тріажу, зниження рівня хибнопозитивних спрацювань і підвищення кіберстійкості критичної інфраструктури.

Структура роботи складається з переліку умовних позначень та скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. У першому розділі розглянуто теоретичні основи забезпечення кіберстійкості об’єктів критичної інформаційної інфраструктури. У другому розділі проаналізовано методи інтелектуального аналізу подій інформаційної безпеки. У третьому розділі розроблено підхід до інтелектуального аналізу подій безпеки та описано його реалізацію. У четвертому розділі наведено методику оцінювання ефективності, результати експериментального дослідження, порівняння з існуючими підходами та практичні рекомендації щодо застосування результатів дослідження.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

1.1. Поняття та значення критичної інформаційної інфраструктури у системі національної безпеки

У сучасній системі національної безпеки критична інформаційна інфраструктура посідає особливе місце, оскільки саме через неї забезпечується безперервність функціонування базових державних, економічних і суспільних процесів. Українське законодавство розглядає захист критичної інфраструктури як складову законодавства у сфері національної безпеки, а критичну інформаційну інфраструктуру – як сукупність об'єктів, кібератака на які здатна безпосередньо вплинути на стале функціонування критично важливих об'єктів. Після законодавчих змін 2025 року поняття об'єкта критичної інформаційної інфраструктури було конкретизовано: ним визнається інформаційна, електронна комунікаційна, інформаційно-комунікаційна або технологічна система, необхідна для стійкого та безперервного функціонування об'єкта критичної інфраструктури, яка істотно впливає на безперервність надання життєво важливих функцій і не має повноцінної альтернативи. Такий підхід фіксує принципово важливу тезу: предметом захисту є не лише фізичний об'єкт, а й його цифрове середовище керування, зв'язку, збору телеметрії та прийняття рішень. Значення критичної інформаційної інфраструктури визначається не стільки її вартістю чи масштабом, скільки наслідками порушення її роботи.

Закон України «Про критичну інфраструктуру» прямо пов'язує безпеку таких об'єктів із забезпеченням життєво важливих функцій та послуг, порушення яких тягне негативні наслідки для національної безпеки [1]. До них віднесено, зокрема, енергозабезпечення, інформаційні послуги, транспорт, водопостачання, охорону здоров'я та інші сфери, без яких неможливі ані повсякденне функціонування держави, ані її стійкість у кризовий період. Звідси

випливає, що критична інформаційна інфраструктура є не допоміжним технологічним контуром, а функціональним ядром сучасної державності: через неї проходять сигнали управління, маршрути обміну даними, телеметрія, диспетчерські команди, механізми ідентифікації, взаємодія між операторами та суб'єктами реагування. У науковому розумінні критичну інформаційну інфраструктуру доцільно трактувати як сукупність цифрових, комунікаційних і технологічних систем, за допомогою яких об'єкт критичної інфраструктури підтримує свій штатний режим роботи, переходить у режим готовності, реагує на загрозу та відновлює функціонування після інциденту [2-3]. Йдеться про серверні комплекси, системи диспетчеризації, промислові мережі, SCADA- та ICS-середовища, центри обробки даних, телекомунікаційні вузли, засоби електронної ідентифікації, журнали подій, канали резервного зв'язку та інші компоненти, які забезпечують керованість об'єкта.

Така інфраструктура має подвійну природу. Вона є носієм інформації та середовищем автоматизованого управління, але водночас сама стає самостійною ціллю для противника, оскільки вплив на неї дає можливість без прямого фізичного втручання змінити режими роботи обладнання, порушити зв'язок, спотворити дані моніторингу або зупинити критичний сервіс. Саме цим пояснюється перехід від традиційного захисту інформації до моделі забезпечення стійкості технологічних процесів. Найбільш наочно роль критичної інформаційної інфраструктури проявляється в енергетичному секторі.

Українська модель секторизації критичної інфраструктури охоплює в межах паливно-енергетичного сектору електроенергетику, газову промисловість, нафтову промисловість, ядерну енергетику та енергетичне машинобудування [4]. До критичних послуг віднесено виробництво електроенергії, управління системами передачі та енергопостачання, розподіл електричної енергії, експлуатацію газотранспортної системи, атомних електростанцій та сховищ відпрацьованого палива. Нормативно закріплено й масштаб можливих наслідків: порушення функціонування енергетичного об'єкта оцінюється, зокрема, за кількістю населення, що залишиться без

електропостачання, та за часом відновлення штатного режиму. Така деталізація показує, що для енергетики цифровий контур уже давно не є другорядним: без нього неможливі диспетчерське керування, балансування навантажень, обмін технологічними параметрами, аварійна автоматика та координація відновлювальних робіт. Енергетика є особливо чутливою до сучасних кіберзагроз через поєднання кількох факторів: широкого використання операційних технологій, високої вартості помилки, залежності від суміжних мереж і обмеженої можливості зупиняти процес для технічного обслуговування.

У табл. 1.1 наведено секторальні особливості критичної інформаційної інфраструктури.

Таблиця 1.1

Секторальні особливості критичної інформаційної інфраструктури

Сектор	Ключові цифрові функції	Типові наслідки порушення
Енергетика	Диспетчеризація, телеметрія, автоматизоване керування	Порушення енергопостачання, втрата видимості процесу
Транспорт	Сервіси координації руху, логістика, диспетчеризація	Каскадні затримки, блокування вузлів, порушення перевезень
Зв'язок	Маршрутизація, сигнальний обмін, мережеве керування	Деградація сервісів, втрата координації між секторами

Європейський контекст підтверджує цю вразливість [5-6]: ENISA повідомляла, що лише у 2023 році було зафіксовано понад 200 кіберінцидентів, націлених на енергетичний сектор, причому більш як половина з них стосувалася Європи; окремо зазначалося, що 32 % операторів енергетики не мають жодного критичного OT-процесу, який моніторився б центром SOC. У 2025–2026 роках акцент ще більше змістився до проблеми безпеки OT та ICS-середовищ, ланцюгів постачання та захисту енергетичних мереж від дій угруповань, що демонструють інтерес саме до енергетичної інфраструктури й здатність впливати на операційні технології. Для України це не абстрактний сценарій: CERT-UA у 2024 році публічно повідомляла про плани угруповання Sandworm щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України.

Транспортний сектор має іншу, але не менш складну архітектуру залежностей.

До нього належать авіаційний транспорт, управління повітряним рухом, автомобільний і міський електричний транспорт, метрополітен, залізниця, морський та внутрішній водний транспорт, а також інтелектуальні транспортні системи, що забезпечують управління рухом і взаємодію між різними видами перевезень.

Специфіка транспортної критичної інформаційної інфраструктури полягає в тому, що її відмова має одночасно просторовий і часовий ефект: інцидент може швидко поширюватися ланцюгом маршрутів, створювати каскадні затримки, блокувати вузлові станції, аеропорти, логістичні центри, прикордонні пункти пропуску. Українська методика категоризації прямо фіксує як критичний сценарій неможливість надання послуг авіаційним транспортом стратегічно важливим аеропортом протягом понад 24 годин без альтернативи, а також блокування ключових транспортних вузлів і сервісів. У практичному вимірі це означає, що інформаційна інфраструктура транспорту має забезпечувати не просто облік чи диспетчеризацію, а безперервність мобільності, логістики, евакуації, військових і гуманітарних перевезень. У безпековому середовищі 2025–2026 років транспорт став однією з найуразливіших ланок через поєднання цифровізації, геополітичної напруженості та великої кількості зовнішніх інтерфейсів. ENISA у звіті Threat Landscape 2025 зафіксувала, що кіберкримінальні інциденти проти транспортного сектору становили 8,4 % усіх інцидентів, причому 83,9 % з них були пов’язані з програмами-вимагачами, а 16,1 % –з витоками даних.

У тому самому звіті зазначено, що активність проти транспорту, логістики і вантажоперевезень у ряді країн ЄС узгоджується з ширшою стратегією тиску на критичну інфраструктуру держав, пов’язаних із підтримкою України. Для транспортної критичної інформаційної інфраструктури це означає, що загрози більше не обмежуються окремими інцидентами зловмисного ПЗ: до них додаються кампанії типу відмови в обслуговуванні, втручання в логістичні сервіси, компрометація підрядників, атаки на мережеву периферію та спроби

порушення координації між IT- і OT-контурами. Не менш значущим є сектор зв'язку та цифрової інфраструктури.

Українське регулювання відносить до критично важливих підсекторів електронні комунікації, електронні довірчі послуги, електронну ідентифікацію, адміністрування адресного простору українського сегмента Інтернету, а також функціонування державних інформаційно-комунікаційних систем і реєстрів. У 2026 році європейський безпековий порядок денний для телекомунікаційного сектору концентрувався на кібератаках на телеком-мережі, стійкості мереж із урахуванням залежностей від енергоживлення, загрозах шпигунства в телеком-мережах та стійкості підводних кабелів.

Така постановка питання є показовою: зв'язок сьогодні виступає не лише сервісом передачі даних, а опорною інфраструктурою для управління енергетикою, транспортом, обороною, державними реєстрами і кризовими комунікаціями. Втрата телекомунікаційного сегмента або його деградація не лише ускладнює обмін інформацією, а й руйнує координацію між усіма іншими секторами критичної інфраструктури. Функціонування критичної інформаційної інфраструктури у сучасній системі національної безпеки визначає її роль як цифрового каркаса, без якого неможливі ані стале надання базових послуг, ані збереження керованості держави в умовах кризи. Її особливість полягає в міжсекторальному характері: інформаційний контур енергетики залежить від зв'язку, транспорт – від енергоживлення і телеметрії, зв'язок – від електропостачання і захищених центрів керування. Саме тому будь-яке дослідження кіберстійкості об'єктів критичної інформаційної інфраструктури має виходити з того, що їх захист зводиться не до ізольованого посилення окремого сервера чи мережевого сегмента, а до побудови здатності системи вчасно виявляти події безпеки, корелювати їх між різними джерелами, локалізувати вплив інциденту та відновлювати штатне функціонування без втрати життєво важливих послуг. Саме ця логіка робить інтелектуальний аналіз подій безпеки ключовим інструментом підвищення кіберстійкості критичної інформаційної інфраструктури.

У табл. 1.2 наведено порівняння секторних наслідків порушення інформаційної інфраструктури.

Таблиця 1.2

Порівняння секторних наслідків порушення інформаційної інфраструктури

Сектор	**Критична функція**	**Основні цифрові залежності**	**Типовий наслідок інциденту**
Енергетика	Передача та розподіл енергії	SCADA, HMI, телеметрія, технологічні шлюзи	Втрата керованості та видимості
Транспорт	Координація руху й логістика	Диспетчерські системи, API, центри керування	Каскадні затримки та блокування вузлів
Зв'язок	Передача даних і сигналізація	Мережеве ядро, OSS/BSS, маршрутизація	Деградація міжсекторальної взаємодії

1.2. Основні кіберзагрози та атаки на об'єкти критичної інформаційної інфраструктури

Станом на 2026 рік характер кіберзагроз для об'єктів критичної інформаційної інфраструктури визначається не лише зростанням кількості інцидентів, а насамперед зміною їхньої логіки. Якщо раніше значна частина атак була орієнтована на викрадення інформації або порушення роботи окремих інформаційних систем, то нині основною метою дедалі частіше стає вплив на безперервність критичних послуг, дестабілізація керування технологічними процесами, виснаження ресурсів реагування та створення довготривалого операційного тиску на державу й економіку. ENISA у звіті NIS360 2026 зазначає, що кіберзрілість секторів високої критичності в ЄС зростає, проте рівень їхньої критичності залишається стабільно високим, а це означає, що навіть за наявності прогресу в захисті наслідки успішного інциденту залишаються системно небезпечними. Для України така оцінка має особливе значення, оскільки кіберпростір давно став частиною ширшого безпекового протистояння, а об'єкти

енергетики, транспорту та зв’язку розглядаються противником як цілі, ураження яких дає непрямий, але масштабний ефект. Специфіка кіберзагроз для критичної інформаційної інфраструктури зумовлена тим, що вона функціонує на стику IT- та OT-середовищ.

У звичайних корпоративних мережах інцидент часто обмежується компрометацією даних, сервісів або облікових записів. На об’єктах критичної інфраструктури компрометація цифрового контуру може призводити до зміни режимів роботи обладнання, втрати телеметрії, порушення диспетчерського керування, блокування процедур аварійного реагування або руйнування довіри до показників системи. Через це ключовими стають загрози, пов’язані з операційними технологіями, системами промислового керування, вузлами віддаленого доступу, периферійними мережевими пристроями та критичними серверами, які зв’язують технологічний процес із корпоративною мережею. CISA у 2026 році прямо звертала увагу на випадки компрометації інтернет-доступних автоматизованих систем у критичній інфраструктурі та на інциденти, що демонструють реальні прогалини в безпеці OT та ICS-середовищ. Це підтверджує, що сучасна атака на критичний об’єкт часто починається не з фізичного впливу, а з проникнення в допоміжний або неправильно сегментований цифровий контур.

Однією з найбільш небезпечних категорій залишаються деструктивні та підривні атаки на енергетичні об’єкти. Для енергетики характерна висока залежність від телеметрії, автоматизованого керування, каналів диспетчерського зв’язку та синхронізації між сегментами мережі. Саме тому атака на цифровий контур тут може бути спрямована не лише на викрадення інформації, а на зміну фактичної поведінки інфраструктури: відключення підстанцій, порушення режимів передавання електроенергії, втручання в процеси балансування, блокування відновлювальних дій або спотворення показників моніторингу. CERT-UA ще раніше фіксувала наміри угруповання Sandworm здійснити кібератаку з виведенням з ладу елементів високовольтної інфраструктури, а CISA у 2026 році вже аналізувала інцидент в енергетичному секторі Польщі,

який продемонстрував прогалини в безпеці OT та ICS. На цьому тлі загроза для енергетики у 2026 році полягає не в окремому класі шкідливого коду, а в комбінації технік: проникнення через IT-контур, закріплення, рух до технологічного сегмента, порушення видимості для операторів і спроби вплинути на фізичний процес через цифрові інтерфейси.

Другою системною загрозою для критичної інфраструктури є атаки із застосуванням програм-вимагачів та пов'язані з ними моделі подвійного або потрійного вимагання. Для корпоративного сектору атаки із застосуванням програм-вимагачів часто означають тимчасову втрату доступу до даних і сервісів. Для об'єктів критичної інфраструктури наслідки ширші, оскільки блокування IT-компонентів майже завжди порушує технологічне планування, логістику, диспетчеризацію, обслуговування абонентів, аварійні процедури й документообіг. У сучасному європейському кіберпросторі програми-вимагачі залишаються загрозою з одним із найвищих рівнів впливу, а для транспортного сектору цей клас інцидентів є особливо показовим. Це вказує на зміну логіки зловмисників: вони дедалі частіше атакують не лише дані, а вузли організаційної координації – розклади, системи управління перевезеннями, внутрішні логістичні сервіси, електронний документообіг, системи бронювання, доступу та управління ланцюгами постачання.

Для критичної інфраструктури це означає, що шифрування навіть допоміжної частини інформаційного середовища здатне непрямо вивести з ладу весь сервісний контур. Для транспортної інфраструктури окрему роль відіграють атак типу відмови в обслуговуванніи та кампанії, які мають демонстративно-дестабілізаційний характер. Транспорт є публічно видимим сектором, де навіть короткочасне порушення доступності цифрових сервісів одразу створює суспільний резонанс, впливає на пасажирів, перевізників, вантажовідправників і суміжні галузі. Транспортний сектор у 2025 році значною мірою зазнавав саме атак типу відмови в обслуговуванні; активність окремих угруповань при цьому прямо пов'язувалася з політичними подіями та підтримкою України. У практичному вимірі такі атаки не завжди спричиняють фізичне зупинення

перевезень, але вони підривають доступність вебпорталів аеропортів, портів, операторів перевезень, інформаційних табло, сервісів бронювання та систем взаємодії з клієнтами.

У поєднанні з іншими техніками, зокрема фішинговими кампаніями, компрометацією підрядників або шкідливою активністю в мережі, атака типу відмови в обслуговуванні стає не просто шумовим інструментом, а засобом відволікання й розсіювання уваги захисників. Для сектора зв'язку та цифрової інфраструктури головною ознакою сучасних загроз є поєднання шпигунського інтересу, залежності від постачальників і високої ціни компрометації мережевого ядра. ENISA у 2025–2026 роках неодноразово виокремлювала для телекомунікаційного середовища такі проблеми, як шпигунство в телекомунікаційних мережах, стійкість підводних кабелів, захист високошвидкісних і супутникових мереж, а також ризики, пов'язані з обладнанням і технологічною залежністю від високоризикових постачальників. Одночасно CISA у спільних консультативних матеріалах попереджала, що державні актори прагнуть закріплюватися в мережах критичної інфраструктури для майбутніх підривних або руйнівних дій, а ENISA відзначала інтенсифікацію тривалих кампаній кіберрозвідки проти телекомунікаційних та логістичних мереж. Для сектора зв'язку це означає зміну акценту: загрозою стає не лише відмова сервісу, а прихована присутність у мережі, збір службових даних, компрометація міжоператорської взаємодії, вплив на сигнальний обмін і використання телеком-інфраструктури як плацдарму для подальших атак на енергетику, державні системи та транспорт.

Суттєве місце в сучасному ландшафті загроз займає експлуатація вразливостей і компрометація ланцюгів постачання. Критична інфраструктура має складну архітектуру залежностей: вона спирається на програмне забезпечення, мережеве обладнання, спеціалізовані контролери, віддалене адміністрування, хмарні сервіси, оновлення постачальників та інтеграторів. Через це атакувальник дедалі частіше обирає не прямий штурм добре захищеного ядра, а проникнення через периферійний сервіс, застаріле мережеве

обладнання, систему віддаленого доступу або сторонній компонент. ENISA вказує, що експлуатація вразливостей залишається одним із ключових векторів початкового доступу, а в NIS Investments 2025 зазначено, що вразливості залишаються другим за поширеністю початковим вектором інцидентів, часто озброюються протягом кількох днів після розкриття і становлять близько п'ятої частини вторгнень. Для об'єктів критичної інфраструктури ця тенденція є особливо небезпечною, оскільки цикли оновлення в OT-середовищах повільніші, а вікно між появою експлойта і встановленням виправлення часто перевищує допустимий рівень ризику.

Помітно трансформується і соціотехнічний компонент атак. Якщо раніше фішинг у критичній інфраструктурі сприймався переважно як шлях компрометації пошти окремих працівників, то у 2025–2026 роках він дедалі частіше використовується як стартова точка для входу в мережі операторів, підрядників, сервісних компаній і технічного персоналу, який має віддалений доступ до критичних систем. ENISA у Threat Landscape 2025 вказує, що на початку 2025 року понад 80 % спостережуваної активності соціальної інженерії вже пов'язувалося з фішинговими кампаніями, підтриманими засобами штучного інтелекту. Для критичної інфраструктури це особливо небезпечно, оскільки такі кампанії точніше імітують службову комунікацію, технічні листи, внутрішні доручення й повідомлення від постачальників, а в разі компрометації облікових даних відкривають шлях до VPN, поштових сервісів, систем віддаленого адміністрування та хмарних панелей керування. У секторі енергетики це створює ризик руху від офісної мережі до технологічного сегмента; у транспорті – ризик компрометації диспетчерських або логістичних сервісів; у зв'язку – ризик доступу до мережевого адміністрування й критичних сервісних платформ.

Характерною ознакою загроз 2026 року є також зближення різних типів акторів і технік. ENISA прямо вказує, що європейська цифрова інфраструктура зазнає впливу від різнорідних, але дедалі більш конвергентних угруповань, які повторно використовують інструменти, спільно експлуатують вразливості й

комбінують моделі шпигунства, ідеологічного тиску та кримінального зиску. Для критичної інформаційної інфраструктури це означає, що межа між «звичайною» кампанією типу відмови в обслуговуванні, шпигунською операцією, інцидентом із застосуванням програм-вимагачів і диверсійною підготовкою стає менш чіткою. Один і той самий інцидент може починатися зі збору розвідувальної інформації, продовжуватися компрометацією облікових даних, переходити у втручання в роботу допоміжних сервісів, а далі використовуватися як інструмент політичного або економічного тиску. Через це основні кіберзагрози для об'єктів критичної інформаційної інфраструктури доцільно розглядати не як ізольовані категорії, а як взаємопов'язаний набір сценаріїв впливу на стійкість. Для енергетики домінують ризики OT та ICSкомпрометації та підриву технологічних процесів, для транспорту – програмивимагачі, атаки на доступність і атаки на логістичний контур, для зв'язку – шпигунство, компрометація мережевого ядра та атаки через залежності від постачальників. Саме ця складна структура загроз зумовлює необхідність переходу від реактивного захисту до системного моніторингу, кореляції подій та інтелектуального аналізу ознак інцидентів у різних секторах критичної інфраструктури.

1.3. Поняття кіберстійкості інформаційних систем та підходи до її забезпечення

Поняття кіберстійкості інформаційних систем у сучасній науковій і нормативній площині виходить за межі традиційного розуміння кіберзахисту як сукупності превентивних заходів. NIST визначає кіберстійкість як здатність передбачати, витримувати, відновлюватися та адаптуватися до несприятливих умов, стресів, атак або компрометацій систем, що використовують кіберресурси або функціонують завдяки їм. У спеціалізованих настановах NIST також підкреслюється, що кіберстійкість покликана забезпечити досягнення місійних і бізнес-цілей у змагальному кіберсередовищі, тобто за умов, коли сам факт

спроби компрометації вже вважається нормальним елементом операційної реальності [7-12]. За такого підходу центр ваги зміщується з абсолютного недопущення інциденту на збереження працездатності системи, локалізацію наслідків порушення, контрольоване відновлення та удосконалення архітектури після інциденту. Саме тому кіберстійкість доцільно розглядати як інтегральну характеристику інформаційної системи, яка об’єднує безпеку, надійність, безперервність функціонування та керованість у кризових умовах.

Для об’єктів критичної інформаційної інфраструктури кіберстійкість має більш вузький і водночас більш вимогливий зміст, ніж для звичайних корпоративних систем. Якщо в комерційному секторі припустимим може бути тимчасове обмеження окремих цифрових сервісів, то в енергетиці, транспорті та зв’язку навіть короткочасне порушення інформаційного контуру здатне створити непропорційно великі наслідки для суспільства, економіки та державного управління. Українське законодавство виходить із того, що об’єкт критичної інформаційної інфраструктури є системою, необхідною для сталого та безперервного функціонування об’єкта критичної інфраструктури, а це означає, що її оцінювання не може обмежуватися лише показниками конфіденційності чи цілісності даних. Визначальним стає питання, чи здатна система зберігати керованість, підтримувати життєво важливу функцію та переходити в режим відновлення без втрати критичного сервісу. У цьому сенсі кіберстійкість для критичної інфраструктури є властивістю не окремого програмного або мережевого компонента, а всієї операційної системи управління сектором [13].

Підходи до забезпечення кіберстійкості інформаційних систем ґрунтуються на системній логіці життєвого циклу. NIST SP 800-160 Vol. 2 Rev. 1 розглядає кіберстійкість як результат цілеспрямованого архітектурного та інженерного проєктування, а не як сукупність додаткових захисних механізмів, приєднаних до вже створеної системи [10]. Такий підхід є принциповим для критичної інфраструктури, оскільки системи енергетики, транспорту і зв’язку мають складну багаторівневу архітектуру, включають застарілі компоненти, залежать від сторонніх постачальників і не можуть вільно виводитися з

експлуатації для модернізації.

Кіберстійкість у цьому контексті означає, що вимоги до сегментації, резервування, безпечного віддаленого доступу, журналювання, процедур аварійного перемикання, пріоритетів відновлення та ручного керування повинні закладатися ще на етапі проєктування або модернізації. Її не можна забезпечити виключно засобами мережевого екранування чи антивірусного контролю, якщо сама архітектура системи не передбачає функціонування в умовах часткової деградації, втрати окремих вузлів або компрометації довірених компонентів.

Один із базових підходів до забезпечення кіберстійкості полягає у побудові стійкої архітектури з урахуванням особливостей OT- і ICS-середовищ. NIST у настанові щодо захисту операційних технологій прямо підкреслює, що безпека OT-систем має впроваджуватися з урахуванням їхніх унікальних вимог до продуктивності, надійності та безпеки фізичного процесу [14]. Це означає, що для об'єктів енергетики, транспорту та зв'язку традиційні IT-практики не можуть переноситися механічно.

Наприклад, для енергетичних систем визначальними є контрольованість технологічних режимів, збереження видимості телеметрії та недопущення небезпечних команд у мережі керування. Для транспортних інформаційних систем критичною є синхронізація між диспетчерськими, логістичними та комунікаційними підсистемами. Для телекомунікаційних середовищ – безперервність маршрутизації, стійкість сигнального обміну та здатність мережі працювати за умов часткової втрати вузлів або каналів. Звідси випливає, що кіберстійкість у КІІ спирається на сегментацію середовищ, ізоляцію критичних зон, мінімізацію точок довіри, контроль міжсистемних шлюзів, використання компенсуючих засобів там, де неможливо змінити застарілий компонент, та наявність процедур переходу до безпечного режиму роботи. Другим засадничим підходом є забезпечення постійної видимості подій і стану системи.

Кіберстійкість неможлива без своєчасного виявлення відхилень, розуміння нормального режиму функціонування та здатності швидко ідентифікувати межі інциденту. Саме тому сучасні рамки для критичної інфраструктури дедалі більше

поєднують архітектурну стійкість із розвиненим моніторингом. ENISA у матеріалах 2026 року для секторів високої критичності наголошує, що навіть за зростання загальної кіберзрілості рівень критичності секторів залишається високим, а це означає потребу в безперервній оцінці стану безпеки та зрілості процесів. Для енергетики це означає моніторинг не лише IT-подій, а й OT-телеметрії, аномалій у взаємодії між сегментами, подій віддаленого доступу та відхилень у технологічних командах. Для транспорту – кореляцію інцидентів між логістичними системами, системами бронювання, диспетчерськими платформами, периферійними сервісами та каналами зв'язку.

Для сектора зв'язку – спостереження за сигнальними аномаліями, міжоператорськими інтерфейсами, подіями у маршрутизації та атиповою активністю у мережевому ядрі. У цьому аспекті кіберстійкість безпосередньо пов'язана з якістю аналітики подій безпеки. Третім напрямом є реалізація принципу контрольованого відновлення. У сучасному безпековому середовищі питання полягає не в тому, чи станеться інцидент, а в тому, чи зможе організація відновити критичну функцію в допустимий час і без переходу інциденту в системну аварію. CISA у своїх міжсекторальних рекомендаціях для критичної інфраструктури виділяє резервне копіювання, тестування відновлення, реагування на інциденти, управління комунікаціями під час кризи та мінімізацію ризиків від постачальників як практики базового рівня, необхідні для зниження найбільш значущих ризиків.

Для критичної інформаційної інфраструктури це означає, що резервування повинне стосуватися не лише даних, а й каналів зв'язку, конфігурацій, серверів управління, опорних служб автентифікації та планів переходу на спрощений або ручний режим. В енергетиці це набуває форми резервних диспетчерських і ручних процедур. У транспорті – альтернативних сценаріїв координації перевезень, локального управління вузлами та пріоритетного відновлення маршрутно-критичних сервісів. У телекомунікаціях – дублювання вузлів, резервування маршрутів, автономних джерел живлення та планів швидкого переналаштування мережевої топології. Кіберстійкість у такій моделі є мірою

готовності системи продовжувати роботу навіть у деградованому стані.

Четвертий підхід пов’язаний з управлінням довірою та зменшенням латерального поширення інциденту. У 2025–2026 роках у міжнародних рекомендаціях посилився акцент на принципах нульової довіри, мінімізації привілеїв та ризиках, пов’язаних із постачальниками, що відображено, зокрема, в оновлених міжсекторальних цілях CISA 2.0. Значення цього підходу для критичної інфраструктури є особливо високим, оскільки об’єкти КІІ зазвичай залежать від інтеграторів, сервісних компаній, виробників обладнання й операторів віддаленого супроводу. Компрометація постачальника або надмірні привілеї технічного персоналу можуть стати шляхом обходу зовнішнього периметра. Для енергетики це означає суворий контроль віддаленого доступу до підстанцій, центрів керування та OT-шлюзів.

Для транспорту – обмеження доступу до систем управління рухом, сервісів технічної підтримки, платформ квиткування і логістичних баз. Для зв’язку – жорстке розмежування доступу до мережевого ядра, систем білінгу, сигнальних платформ і адміністративних консолей. забезпечення кіберстійкості вимагає не стільки формального впровадження модних концепцій, скільки перегляду самої моделі довіри, на якій побудована система. П’ятий підхід пов’язаний із секторною адаптацією моделей стійкості. Кіберстійкість не може бути однаково реалізована у всіх секторах, оскільки критична функція в енергетиці, транспорті та зв’язку має різну природу. В енергетичному секторі домінують вимоги до стабільності технологічного процесу, безпечності фізичного обладнання та пріоритетності OT-видимості.

У транспорті на перший план виходить синхронізація між вузлами, доступність цифрових сервісів координації та здатність уникати каскадного ефекту відмов. У секторі зв’язку ключовими стають стійкість мережевої інфраструктури, захист маршрутизації, цілісність сигнального обміну, готовність до шпигунських кампаній та врахування взаємозалежності з енергетикою. ENISA у 2026 році спеціально акцентувала на взаємозалежностях між телекомунікаціями й енергетикою, на питаннях безпеки підводних кабелів,

супутникових комунікацій, маршрутизації, 5G і архітектурах нульової довіри. Це означає, що забезпечення кіберстійкості КІІ має будуватися як поєднання загальних принципів і секторно-специфічних рішень, а не як універсальний набір однакових заходів для всіх об’єктів. Аналіз підходів дозволяє визначити кіберстійкість інформаційних систем як здатність системи зберігати керованість і виконання критичних функцій в умовах кібератак, збоїв і компрометацій, відновлювати працездатність у прийнятні строки та адаптуватися до нових умов загроз.

Для об’єктів критичної інформаційної інфраструктури таке розуміння є базовим, оскільки їхня безпека оцінюється не за відсутністю інцидентів, а за здатністю не допустити втрати життєво важливого сервісу. Основні підходи до її забезпечення охоплюють стійке архітектурне проєктування, сегментацію IT- та OT-середовищ, мінімізацію довіри, постійний моніторинг, кореляцію подій, резервування, підготовленість до відновлення та секторно орієнтовані сценарії реагування. У цій логіці інтелектуальний аналіз подій безпеки набуває методологічного значення, оскільки саме він дає змогу перетворити розрізнені сигнали з критичних систем на основу для своєчасного виявлення інциденту, оцінки його впливу та вибору рішень, що підтримують кіберстійкість об’єкта.

1.4. Роль моніторингу та аналізу подій безпеки у забезпеченні кіберстійкості

Моніторинг та аналіз подій безпеки є одним із ключових функціональних механізмів забезпечення кіберстійкості інформаційних систем, оскільки саме вони перетворюють захист із сукупності статичних налаштувань на безперервний процес спостереження, інтерпретації та реагування. У сучасному розумінні кіберстійкості важливою є не лише наявність бар’єрів на периметрі або засобів автентифікації, а здатність системи своєчасно виявляти відхилення від нормального режиму, оцінювати характер інциденту, локалізувати його вплив і підтримувати функціонування критичного сервісу в умовах атаки. NIST пов’язує

інцидент-респонс із ширшим контуром кіберризик-менеджменту та прямо зазначає, що ефективне виявлення, реагування і відновлення зменшують кількість і наслідки інцидентів. У логіці критичної інформаційної інфраструктури це означає, що моніторинг не є допоміжною технічною функцією, а входить до ядра операційної стійкості об'єкта. Для об'єктів критичної інформаційної інфраструктури роль моніторингу істотно зростає через неможливість покладатися виключно на превентивний захист.

Енергетика, транспорт і зв'язок працюють у середовищі постійної загрози, мають складні міжсистемні залежності, використовують змішані IT- та OT-архітектури, а також часто спираються на обладнання й програмні компоненти з тривалим життєвим циклом. За таких умов питання полягає не в тому, чи буде здійснено спробу компрометації, а в тому, як швидко організація зможе її побачити, зрозуміти і зупинити розвиток інциденту до рівня, на якому він почне впливати на життєво важливу функцію. ENISA у звіті NIS360 2026 підкреслює, що електроенергетика, телекомунікації та банківський сектор залишаються водночас і найбільш зрілими, і найбільш критичними секторами; це означає, що навіть за високої зрілості захисту вимога до постійної видимості та моніторингу не зменшується, а навпаки посилюється. Моніторинг подій безпеки в сучасній практиці слід розуміти як безперервне збирання, централізацію, нормалізацію та аналіз даних із різнорідних джерел: мережевого обладнання, серверів, кінцевих точок, контролерів, засобів захисту, систем віддаленого доступу, журналів автентифікації та телеметрії прикладних сервісів. Класичне виявлення вторгнень розглядається як процес спостереження за подіями в комп'ютерній системі або мережі з подальшим аналізом ознак інциденту, а сучасні рекомендації для критичної інфраструктури наголошують на необхідності агрегувати журнали подій у централізованому, відокремленому середовищі, де порушник не може легко ними маніпулювати.

На рис. 1.1 наведено схема взаємозалежності секторів критичної інформаційної інфраструктури.

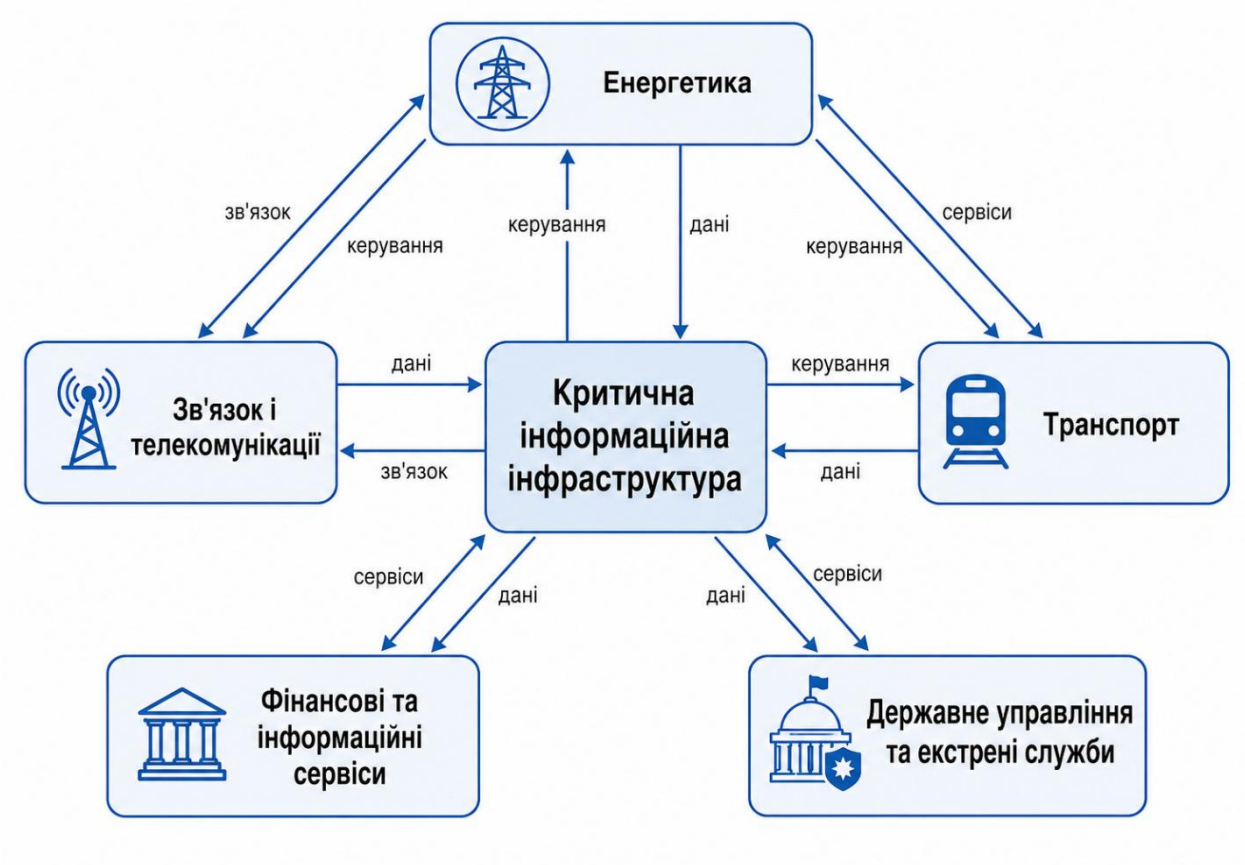

Рис. 1.1. Схема взаємозалежності секторів критичної інформаційної інфраструктури

Така централізація є принциповою, оскільки саме вона робить можливою кореляцію сигналів між різними сегментами інфраструктури та дозволяє виявляти не окрему подію, а сценарій атаки. У забезпеченні кіберстійкості вирішальним є не сам факт збирання журналів, а здатність побудувати на їх основі операційну картину стану системи. Це особливо важливо для критичної інфраструктури, де інцидент рідко обмежується єдиним джерелом даних. Початкова компрометація може проявитися як фішинговий вхід у корпоративну пошту, продовжитися підозрілою VPN-сесією, потім перейти в зміну конфігурації мережевого шлюзу або сервера адміністрування, а завершитися спробою взаємодії з OT-сегментом. Якщо кожен з цих сигналів розглядати ізольовано, система захисту реагуватиме фрагментарно.

Якщо ж події поєднуються в єдиному аналітичному контурі, організація отримує можливість виявляти атаку ще до того, як вона досягне технологічно критичного рівня. У цьому полягає пряма залежність між зрілістю моніторингу

й кіберстійкістю: чим повнішою є видимість і чим якіснішим є аналіз зв’язків між подіями, тим менший шанс, що інцидент перейде в операційну кризу. В енергетичному секторі моніторинг виконує не лише охоронну, а й стабілізуючу функцію. Для енергетичних об’єктів критично важливо підтримувати видимість мережевих взаємодій між IT- та OT-компонентами, спостерігати за типовими потоками телеметрії, контролювати віддалений доступ до інженерних станцій, серверів керування та мережевих шлюзів, а також вчасно виявляти нетипові команди або зв’язки між пристроями, які в нормальному режимі не повинні комунікувати NIST SP 800-82 Rev [9].

3 рекомендує для OT-середовищ базування типового мережевого трафіку, даних про потоки й модель device-to-device communications, а також використання мережевого моніторингу для виявлення аномалій, помилок конфігурації й збоїв. Додатково NIST IR 8219 показує, що поведінкове виявлення аномалій у промислових системах дозволяє виявляти несанкціоновані зв’язки між ICS- пристроями, а також атипові інтернеткомунікації, які можуть свідчити про ексфільтрацію чи спробу горизонтального переміщення усередині сегмента. Показовим у цьому контексті є й аналіз CISA щодо інциденту в енергетичному секторі Польщі в 2026 році, де окремо наголошувалося на прогалинах видимості та безпеки OT та ICS-середовищ. Для енергетики моніторинг є, по суті, способом зберегти керованість технологічним процесом під час цифрового інциденту. У транспортному секторі роль моніторингу визначається високою залежністю від доступності сервісів і великою кількістю цифрових точок взаємодії.

Транспортна інфраструктура включає інформаційні системи диспетчеризації, бронювання, логістики, квиткування, керування рухом, взаємодії з постачальниками, пасажирами й суміжними операторами. У 2025 році транспортний сектор значною мірою страждав від атак типу відмови в обслуговуванні, а також від програм-вимагачів; транспортні інциденти в європейському просторі мали високу частку саме цих двох типів впливу. За таких умов моніторинг повинен охоплювати одночасно публічний цифровий контур і внутрішню операційну інфраструктуру. Для транспорту недостатньо

спостерігати лише за доступністю вебресурсів або навантаженням на мережу. Потрібна кореляція між ознаками атак типу відмови в обслуговуванні, подіями автентифікації адміністраторів, активністю в системах резервного керування, змінами в інтеграціях з підрядниками та станом ключових бекенд-сервісів.

Такий підхід дозволяє відрізняти суто демонстративну атаку на доступність від інциденту, що використовується як прикриття для глибшої компрометації. Для сектора зв'язку та цифрової інфраструктури моніторинг виконує ще одну функцію – виявлення прихованої присутності противника. ENISA окремо виокремлює для телекомунікаційного середовища теми шпигунства в телеком- мережах, стійкості підводних кабелів і захисту цифрової інфраструктури як стратегічні виклики. Крім того, CISA та партнерські агентства в попередніх консультативних матеріалах наголошували, що державні актори прагнуть заздалегідь закріплюватися в IT-мережах критичної інфраструктури для майбутніх підривних або руйнівних дій, а в 2025 році окремо звертали увагу на необхідність посиленого захисту й виявлення для телекомунікаційних організацій. Для операторів зв'язку це означає, що моніторинг не може обмежуватися традиційним рівнем традиційного SOC.

Він має включати спостереження за подіями в мережевому ядрі, аномаліями маршрутизації, нетиповими змінами конфігурацій, адміністративними входами, активністю в системах керування мережею, а також за спробами використовувати легітимні сервісні механізми як канал прихованого управління. У секторі зв'язку кіберстійкість значною мірою залежить від здатності виявляти не лише шумові інциденти, а й довготривалі малопомітні кампанії кіберрозвідки. Моніторинг і аналіз подій безпеки мають безпосереднє значення і для етапів реагування та відновлення. Під час інциденту саме дані моніторингу дозволяють визначити межі компрометації, зрозуміти початковий вектор проникнення, оцінити латеральне поширення, пріоритезувати ізоляцію сегментів і зберегти докази для подальшого аналізу NIST SP 800-61 Rev [8].

З пов'язує реагування на інциденти не лише з технічним усуненням наслідків, а й із подальшим вдосконаленням процесів виявлення, відповіді та

відновлення. Сучасні рекомендації, засновані на досвіді реагування на реальні інциденти, окремо наголошують на необхідності розгорнутого журналювання й централізованого збирання логів саме тому, що без них організація втрачає можливість відтворити розвиток інциденту та зрозуміти його повний масштаб. Для об’єктів критичної інфраструктури це має особливу вагу, оскільки від точності оцінки масштабу ураження залежить рішення про зупинення, сегментацію або збереження окремих функцій у роботі. У практичному вимірі ефективний моніторинг у КІІ потребує не лише технологічної платформи, а й організаційної зрілості. Необхідними є чітко визначені джерела телеметрії, процедури її збереження, сценарії кореляції, секторно-специфічні аналітичні сценарії, межі ескалації, взаємодія між SOC, IT-підрозділом, OT-операторами та керівництвом об’єкта.

NIS Investments 2025 показує, що впровадження NIS2 стимулює організації зосереджуватися на найбільш складних, але суттєвих напрямах кіберстійкості, серед яких прямо фігурують виявлення загроз, безперервність діяльності, управління оновленнями та ризики ланцюгів постачання. Це свідчить про те, що моніторинг більше не розглядається як окремий інструмент технічного аудиту; він стає елементом управління стійкістю, який пов’язує виявлення загроз, операційну безперервність і управління ризиками постачальників. Для енергетики, транспорту та зв’язку така інтеграція є критично необхідною, оскільки більшість значущих інцидентів розгортаються саме на межі між технічним, операційним і організаційним контурами. У системі забезпечення кіберстійкості моніторинг та аналіз подій безпеки виконують функцію раннього попередження, оперативної діагностики і післяінцидентного навчання. Саме вони дозволяють перейти від реакції на вже очевидну аварію до виявлення слабких сигналів, які свідчать про підготовку атаки, її початкову фазу або поступове закріплення порушника в інфраструктурі.

Для об’єктів критичної інформаційної інфраструктури ця здатність має безпосереднє значення для збереження життєво важливих функцій. У зв’язку з цим моніторинг подій безпеки слід розглядати не як допоміжний сервіс

кіберзахисту, а як один із базових інструментів підтримання кіберстійкості, на основі якого надалі вибудовуються методи кореляції, виявлення аномалій та інтелектуального аналізу даних подій безпеки. Висновки до розділу 1 Матеріал першого розділу показує, що критична інформаційна інфраструктура є функціональною основою сучасної держави, оскільки саме через неї забезпечуються безперервність надання базових послуг, керованість критичними процесами та стійкість суспільства до кризових впливів. Для енергетики, транспорту і зв'язку цифровий контур уже не є допоміжним елементом, а виступає середовищем керування, координації, диспетчеризації, обміну телеметрією та прийняття рішень. Це означає, що кібератака на інформаційний компонент критичного об'єкта здатна спричинити наслідки, співмірні з порушенням роботи самого фізичного об'єкта.

Аналіз сучасних кіберзагроз засвідчив, що у 2026 році для об'єктів критичної інформаційної інфраструктури найбільшу небезпеку становлять не окремі технічні інциденти, а комбіновані сценарії впливу, що поєднують компрометацію IT- та OT-середовищ, експлуатацію вразливостей, атаки на доступність, втручання в логістичні та телекомунікаційні сервіси, а також використання ланцюгів постачання і соціотехнічних засобів проникнення. Для енергетики особливо небезпечними є спроби впливу на технологічний процес і втрати видимості подій у мережі керування. Для транспорту критичними є кампанії, що порушують координацію перевезень і доступність цифрових сервісів. Для зв'язку пріоритетного значення набувають приховане закріплення в мережі, шпигунство та компрометація мережевого ядра. Розгляд поняття кіберстійкості показав, що її доцільно оцінювати як здатність інформаційної системи зберігати керованість, підтримувати критичну функцію в умовах інциденту, відновлювати працездатність у прийнятні строки та адаптуватися до змін середовища загроз.

Такий підхід передбачає поєднання стійкого архітектурного проєктування, сегментації середовищ, мінімізації довіри, резервування, підготовленості до відновлення та секторно-орієнтованих сценаріїв реагування. Центральне місце в

цій моделі займають моніторинг та аналіз подій безпеки, оскільки саме вони забезпечують своєчасне виявлення слабких сигналів інциденту, побудову цілісної картини подій і підтримку обґрунтованих рішень під час реагування. Звідси випливає, що подальше дослідження методів інтелектуального аналізу подій безпеки є логічним кроком для розроблення підходів, здатних підвищити кіберстійкість об’єктів критичної інформаційної інфраструктури.

Висновки до розділу 1

У розділі 1 обґрунтовано місце критичної інформаційної інфраструктури у системі національної безпеки та показано, що її стійкість визначається здатністю підтримувати критичні функції в умовах кібератак і збоїв. Визначено секторну специфіку енергетики, транспорту та зв’язку, узагальнено основні кіберзагрози для цих секторів і встановлено роль моніторингу та аналізу подій безпеки як базового механізму забезпечення кіберстійкості. Отримані результати створюють теоретичне підґрунтя для подальшого аналізу методів обробки подій інформаційної безпеки.

РОЗДІЛ 2 АНАЛІЗ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Класифікація подій інформаційної безпеки в інформаційних системах

У системах моніторингу інформаційної безпеки базовою аналітичною одиницею виступає подія безпеки, оскільки саме вона фіксує окремий факт зміни стану системи, мережі, прикладного сервісу або технологічного процесу, що може мати значення для оцінювання захищеності середовища. У міжнародній практиці подія безпеки трактується як спостережуване явище в інформаційній системі або мережі, яке пов'язане з виконанням дій користувачів, процесів, служб чи технічних засобів і може бути релевантним для подальшого аналізу. Таке розуміння закріплене у стандартах управління інцидентами [21-25] та у методичних документах NIST, де подія розглядається як будь-яка ідентифікована зміна в системі або мережі, а інцидент – як подія або сукупність подій, що реально порушують або створюють безпосередню загрозу порушення політики безпеки, правил прийнятного використання чи стандартних механізмів захисту. Це розмежування має не лише термінологічне, а й прикладне значення. Подія не завжди свідчить про атаку, оскільки вона може бути наслідком штатної адміністративної дії, технологічного оновлення, автоматизованого резервного копіювання або легітимної мережевої взаємодії.

Інцидент формується тоді, коли окрему подію або ланцюг подій уже можна інтерпретувати як загрозу конфіденційності, цілісності, доступності чи керованості інформаційної системи. У зв'язку з цим методологічно виправданою є систематизація та класифікація подій, оскільки вона формує підґрунтя для чіткого відокремлення нормальної активності від потенційно небезпечної. Для об'єктів критичної інформаційної інфраструктури таке завдання є особливо складним. У корпоративному середовищі значна частина подій має типовий

характер і обмежується межами офісної IT-інфраструктури. У середовищі критичної інфраструктури події генеруються на перетині мережевих, серверних, прикладних і технологічних компонентів, а наслідки хибної інтерпретації можуть виходити далеко за межі цифрового контуру.

В енергетичних об'єктах подія безпеки може бути пов'язана не лише з автентифікацією адміністратора чи зміною конфігурації міжмережевого екрана, а й з атиповою командою в SCADA-системі, несанкціонованим зверненням до програмованих логічних контролерів (PLC) або зміною параметра технологічного процесу. Для транспортної інфраструктури релевантними стають події у диспетчерських системах, сервісах координації руху, логістичних платформах, вузлах зв'язку та інтеграціях із підрядниками. У секторі зв'язку аналітичну цінність мають не лише журнали доступу до серверів, а й сигнальні події, маршрутизаційні аномалії, зміни конфігурації мережевого ядра та нетипові взаємодії між телекомунікаційними вузлами. Джерела формування подій у сучасних системах моніторингу доцільно класифікувати за трьома рівнями. Перший рівень становить мережева інфраструктура, яка формує події про маршрутизацію, фільтрацію трафіку, мережеві сесії, аномальні з'єднання та спроби несанкціонованого доступу.

У табл. 2.1 наведено джерела формування подій безпеки в інформаційних системах КІІ.

Таблиця 2.1

Джерела формування подій безпеки в інформаційних системах КІІ

Рівень	**Основні джерела**	**Аналітичне призначення**
Мережевий	Маршрутизатори, міжмережеві екрани, IDS/IPS, NetFlow/IPFIX	Виявлення сканування, латерального руху, міжсегментних аномалій
Системний та прикладний	Windows Event Logs, Syslog, вебсервери, БД, каталоги користувачів	Виявлення аномальної активності користувачів і служб
Технологічний	SCADA, PLC, HMI, інженерні станції, технологічні шлюзи	Контроль впливу на технологічний процес і ОТповедінку

До цієї групи належать журнали маршрутизаторів, міжмережевих екранів, систем виявлення та запобігання вторгненням (IDS/IPS), а також телеметрія формату NetFlow або IPFIX. Саме мережева подія найчастіше відображає первинний контакт порушника з інфраструктурою, сканування, спробу обходу політики доступу, латеральне переміщення або приховану взаємодію між сегментами. Для критичної інфраструктури мережевий рівень має підвищену цінність, оскільки він дозволяє спостерігати взаємодію між IT- та OTсередовищами, виявляти нехарактерні напрями трафіку та відстежувати появу каналів комунікації, яких не повинно існувати в нормальному режимі. Другий рівень охоплює системні та прикладні джерела подій. Йдеться про журнали системних подій Windows (Windows Event Logs), протокол Syslog операційних систем, журнали серверів застосунків, вебсерверів, баз даних, систем автентифікації, каталогів користувачів, засобів резервного копіювання та хмарних сервісів.

Ці події фіксують спроби входу, зміну облікових записів, створення або видалення служб, запуск процесів, звернення до конфігураційних файлів, доступ до баз даних, зміну прав доступу та інші дії, що мають значення для оцінки внутрішньої активності. Аналіз архітектури сучасних систем моніторингу свідчить, що саме системний та прикладний рівні генерують найбільший масив журнальних записів у більшості організацій, а також надають найширший контекст для інтерпретації поведінки користувачів і адміністраторів. Для транспортних і телекомунікаційних систем події цього рівня дозволяють виявляти спроби зміни налаштувань критичних сервісів, маніпуляції з конфігураціями маршрутизації, несанкціоноване підключення зовнішніх облікових записів, а також нетипові звернення до прикладних інтерфейсів (API), через які може здійснюватися підготовка до інциденту. Третій рівень становлять події технологічного середовища, характерні для операційних технологій (OT) та промислових систем керування (ICS). До них належать журнали промислових контролерів PLC, SCADA-систем, серверів зберігання історичних даних

(історіанів), панелей людино- машинного інтерфейсу (HMI), інженерних станцій, систем дистанційного керування та технологічних шлюзів.

Специфіка подій технологічного сегмента полягає в їхній принципово іншій семантиці порівняно з традиційними IT-журналами. Вони описують не лише інформаційну активність, а й фактичний стан технологічного процесу: запуск або зупинку обладнання, зміну режимів керування, зміну параметрів датчиків, завантаження логіки контролера, перепідключення інженерної станції, втрату зв'язку з польовими пристроями. У критичній інфраструктурі саме цей рівень найтісніше пов'язаний із фізичними наслідками. В енергетиці така подія може передувати порушенню розподілу навантаження або втраті видимості на підстанції. У транспорті –відображати втручання в системи диспетчеризації чи сигнального керування.

У секторі зв'язку аналогом технологічного рівня виступають події мережевого ядра, сигнальні журнали та події критичних елементів маршрутизації, які безпосередньо впливають на доступність послуг зв'язку. Групування подій дозволяє перейти від хаотичного потоку записів до аналітичної моделі, придатної для пріоритезації та кореляції. У сучасних системах моніторингу події класифікуються за кількома ознаками. Найпоширенішою є класифікація за рівнем критичності, де умовно виділяються низький, середній і високий рівні. Події низької критичності переважно не свідчать про безпосередню загрозу, але формують поведінковий фон і можуть використовуватися як допоміжний контекст.

Події середньої критичності потребують додаткової перевірки, оскільки відображають відхилення від норми, нетипову активність або дії, що можуть бути як легітимними, так і шкідливими. Події високої критичності безпосередньо пов'язані з порушенням політики безпеки, спробами вторгнення, змінами у критичних конфігураціях, несанкціонованим доступом або впливом на технологічний процес. Не менш важливою є класифікація за типом активності. У практиці моніторингу доцільно виокремлювати щонайменше такі класи: події автентифікації, які охоплюють успішні й неуспішні входи, зміну факторів

доступу, створення сесій і спроби ескалації привілеїв; події зміни конфігурації, що стосуються редагування правил, політик, таблиць маршрутизації, параметрів обладнання або технологічних налаштувань; події мережевої взаємодії, які відображають встановлення з'єднань, зміну напрямів трафіку, звернення до сервісів і появу атипових потоків; події доступу до об'єктів, що охоплюють роботу з файлами, записами баз даних, конфігураційними сховищами, логікою PLC-контролерів або диспетчерськими командами. Така класифікація є практично цінною, оскільки дозволяє вибудовувати сценарії кореляції: поєднання атипової автентифікації, зміни конфігурації та нетипової мережевої взаємодії має значно вищу аналітичну вагу, ніж кожна з цих подій окремо.

Окрему проблему становить масштаб великих даних (Big Data), які формуються в сучасних інформаційних системах. На об'єктах критичної інфраструктури щодобовий обсяг журналів може сягати мільйонів або десятків мільйонів записів, причому лише незначна частка з них має відношення до реальних загроз. Це породжує ефект шуму, коли аналітично цінні сигнали губляться серед великої кількості фонових подій, службових записів, повторюваних повідомлень та технічно допустимих відхилень. Результати досліджень реальних інцидентів доводять, що класичні методи фільтрації на основі жорстких детермінованих правил дедалі частіше демонструють обмежену ефективність. Ця обмеженість зумовлена спроможністю таких методів реагувати виключно на заздалегідь відомі шаблони активності.

Крім того, жорсткі правила генерують високий рівень хибнопозитивних спрацювань (хибнопозитивні спрацювання) у середовищах зі складною поведінкою, зокрема в OT- та гібридних мережах КІІ. Додатковим ускладнюючим фактором є те, що сучасні цільові атаки дедалі рідше проявляються у вигляді одиничних критичних подій, а набувають форми слабких, розподілених у часі та просторі ознак, які стають помітними лише після аналізу взаємозв'язків між подіями. У 2026 році ця проблема набула особливої гостроти через зростання кількості взаємопов'язаних систем, хмарних сервісів, компонентів віддаленого доступу та OT-телеметрії, що одночасно надходить до

систем моніторингу. Для енергетики це означає співіснування подій корпоративної IT-мережі й технологічного сегмента. Для транспорту – одночасний аналіз логістичних, мережевих, прикладних і диспетчерських журналів.

Для сектора зв'язку – обробку подій маршрутизації, сигнального обміну, адміністрування та сервісної інфраструктури. Відповідно, класифікація подій інформаційної безпеки втрачає ознаки суто формальної технічної процедури впорядкування журналів, набуваючи статусу фундаментальної методологічної передумови інтелектуального аналізу даних (інтелектуального аналізу даних). Саме потреба відокремлювати значущі закономірності від надлишкових даних, виявляти приховані зв'язки між подіями та знижувати вплив шуму створює логічний перехід до застосування методів машинного навчання та виявлення аномалій у системах кібермоніторингу.

2.2. Методи інтелектуального аналізу даних у задачах кібербезпеки

У задачах кібербезпеки інтелектуальний аналіз даних слід розглядати як сукупність методів виявлення прихованих закономірностей, відхилень, залежностей і поведінкових шаблонів у великих масивах телеметрії, журналів подій та мережевих потоків. Його практичне значення зростає в умовах, коли критична інформаційна інфраструктура генерує надлишковий обсяг різнорідних даних, а загрози дедалі частіше мають багатоступеневий, малопомітний і адаптивний характер. ENISA у Threat Landscape 2025 фіксує, що експлуатація вразливостей залишається одним із провідних векторів початкового доступу, а підтримувані штучним інтелектом фішингові кампанії стали одним із визначальних елементів сучасного ландшафту загроз. Це означає, що аналітична система має виявляти не лише вже відомі сигнатури, а й слабкі, розподілені в часі ознаки компрометації, які стають помітними тільки після обробки значного масиву даних. Для об'єктів енергетики, транспорту та зв'язку така вимога є базовою, оскільки в цих секторах цифровий інцидент безпосередньо впливає на

стійкість технологічного або сервісного процесу.

Одним із найпоширеніших напрямів інтелектуального аналізу є методи класифікації, що належать до контрольованого навчання (контрольованого навчання). Їхня сутність полягає у побудові моделі на основі попередньо розмічених даних, де кожному об'єкту відповідає певний клас: нормальна активність, підозріла активність, фішинг, шкідливе програмне забезпечення, аномальний мережевий потік, несанкціонована зміна конфігурації тощо. У практиці кібермоніторингу класифікація використовується для автоматизованого первинного сортування сповіщень, виявлення шкідливих вкладень, аналізу URL, оцінки ризикових сесій автентифікації та віднесення подій до певних таксономічних категорій. Для корпоративних середовищ такі моделі показують високу ефективність за наявності якісних датасетів і стабільного профілю активності. На об'єктах критичної інфраструктури ситуація складніша.

Енергетичні та транспортні системи мають вузькоспеціалізовані режими функціонування, а розмічених наборів даних для OT-подій значно менше, ніж для звичайної IT-безпеки. Крім того, характер нормальної поведінки в критичній інфраструктурі залежить від технологічного циклу, зміни навантаження, сезону, аварійних режимів та інтеграції з підрядниками. Через це класифікаційні моделі в середовищі КІІ потребують ретельного налаштування ознак, контролю дисбалансу класів і регулярного оновлення з урахуванням явища концептуального зсуву (концептуального зсуву). До другої великої групи належать методи кластеризації, які використовуються тоді, коли попереднє розмічення даних є неповним або відсутнім (unконтрольованого навчання). Їхнє завдання полягає в автоматичному групуванні об'єктів за подібністю ознак, що дає змогу виявляти приховану структуру масиву подій.

У табл. 2.2 наведено порівняння методів інтелектуального аналізу даних у кібербезпеці.

Таблиця 2.2

Порівняння методів інтелектуального аналізу даних у кібербезпеці

Метод	Переваги	Обмеження
Класифікація	Дає чітке віднесення до відомих класів загроз	Потребує якісних розмічених даних
Кластеризація	Працює в умовах браку розмітки	Потребує подальшої інтерпретації кластерів
Виявлення аномалій	Придатне для пошуку невідомих сценаріїв	Чутливе до якості ознак і профілю норми
Часові та графові моделі	Враховують динаміку та зв’язки між подіями	Складніші в реалізації та поясненні

У кібербезпеці кластеризація застосовується для групування схожих логів, профілів мережевих вузлів, поведінки користувачів, категорій запитів до сервісів або послідовностей подій у журнальних даних. Практична цінність цього підходу для критичної інформаційної інфраструктури визначається тим, що в реальному середовищі далеко не кожна подія або атака має готову категорію. У транспортному секторі кластеризація дозволяє відокремлювати типові потоки операційної активності від нетипових сервісних взаємодій, а у секторі зв'язку – виділяти аномальні кластери маршрутизаційних або сигнальних подій, які губляться в загальному фоні. Для енергетичних об'єктів вона корисна в задачах групування технологічних режимів, що дає змогу виявляти події, які не відповідають жодному зі звичних профілів функціонування підстанції, центру диспетчеризації або сегмента мережі керування. Методична перевага кластеризації полягає в тому, що вона підтримує аналітику в середовищах із дефіцитом розмічених даних, який є типовим саме для об'єктів КІІ.

Найбільш значущу роль у задачах кіберзахисту критичної інфраструктури відіграють методи виявлення аномалій. Їхня логіка базується на побудові моделі нормального стану системи та подальшому виявленні відхилень від цієї моделі. Саме такий підхід є особливо цінним для середовищ, де небезпечна активність не обов'язково збігається з раніше відомими сигнатурами. NIST IR 8219 присвячений поведінковому виявленню аномалій у промислових системах і

показує, що такі можливості можуть підтримувати виявлення шкідливих дій і порушень цілісності критичних операційних даних у виробничих та процесних середовищах. В енергетиці це означає виявлення несанкціонованих взаємодій між ICS-пристроями, нетипових інтернет-комунікацій, відхилень у мережевих потоках і технологічних командах.

Для транспорту –фіксацію незвичних послідовностей дій у диспетчерських і логістичних системах. Для телекомунікаційного сектора – виявлення сигнальних аномалій, нехарактерних маршрутів трафіку, змін у профілі адміністративних сесій та прихованих сценаріїв закріплення в мережевому ядрі. Перевага аномального аналізу полягає в здатності виявляти раніше невідомі сценарії атак типу zero- day або маловідомі сценарії компрометації, недоступні для чисто сигнатурного підходу. Окреме місце посідають методи аналізу часових рядів і потокових даних. Для об'єктів критичної інфраструктури інформація надходить не у вигляді ізольованих записів, а як часово впорядкований потік, у якому значення має не лише сам факт події, а й її послідовність, інтервали між подіями, сезонність, повторюваність і взаємозв'язок із режимом функціонування системи.

В енергетиці це стосується телеметрії SCADA, зміни навантаження, команд керування і стану мережевих вузлів. У транспорті – потоків диспетчерських подій, змін у графіку руху, стану вузлів автоматизованого контролю, керування доступністю сервісів і поведінки периферійних систем. У зв'язку – маршрутизаційних оновлень, сигнального обміну, переключень трафіку та керування мережею. Аналіз часових рядів дозволяє виявляти не лише разові аномалії, а й повільні дрейфи поведінки, які можуть свідчити про приховане втручання, підготовку до атаки або деградацію системи внаслідок зловмисної активності. У середовищі КІІ це має принципове значення, оскільки цільові атаки часто не створюють негайного ефекту, а розгортаються як тривалий процес поступового відхилення системи від нормального профілю.

Перспективним напрямом є графові методи аналізу, які подають інфраструктуру та події у вигляді вузлів і зв'язків між ними. Така модель є

природною для сучасних атак, оскільки вони розгортаються через взаємодію користувачів, облікових записів, пристроїв, сервісів, контролерів, мережевих сегментів і зовнішніх вузлів. Графове представлення дає змогу аналізувати не окрему подію, а маршрут поширення атаки: початковий вхід, створення нової сесії, доступ до сервера адміністрування, звернення до технологічного шлюзу, переміщення до критичного сегмента. Для енергетичних об'єктів це допомагає моделювати ланцюг від корпоративної мережі до OT-середовища. Для транспортних систем – аналізувати перехід від зовнішнього прикладного сервісу до операційного контуру.

Для зв'язку – простежувати рух між сегментами мережевого ядра, системами керування та міжоператорськими точками обміну. Цінність графових методів особливо помітна в контексті сучасних кампаній завчасного прихованого закріплення (завчасного прихованого закріплення), коли противник прагне зафіксувати присутність у мережах критичної інфраструктури задовго до активної фази деструктивного впливу. Суттєвим компонентом інтелектуального аналізу є також попередня обробка даних, побудова ознакового простору та зниження розмірності. Журнали подій у КІІ мають різний формат, неоднорідну семантику й відмінну часову гранулярність. Через це результативність будь-якої моделі значною мірою залежить від того, наскільки якісно виконано нормалізацію, агрегацію, вилучення релевантних ознак і синхронізацію часових міток.

У транспортному середовищі одні й ті самі дії можуть фіксуватися окремо в системі бронювання, прикладному сервері, мережевому обладнанні та системі автентифікації. В енергетиці подібна багатошаровість виникає між корпоративним IT-контуром, центром диспетчеризації та PLC/SCADA-компонентами. У секторі зв'язку різниця між мережевими та сервісними подіями ще виразніша. Саме тому інтелектуальний аналіз у кібербезпеці не зводиться до застосування окремого алгоритму; він охоплює повний цикл підготовки даних, що безпосередньо впливає на точність виявлення та стійкість моделі до шуму. У 2026 році окремої уваги потребує проблема надійності самих моделей

інтелектуального аналізу.

NIST у звіті з протидії навмисному спотворенню машинного навчання (adversarial machine learning) наголошує, що системи штучного інтелекту мають власні вектори вразливості: маніпуляцію тренувальними даними, ухилення від детекції, зловживання особливостями ознакового простору та інші форми атак на життєвий цикл моделі. Для критичної інфраструктури це означає, що використання ML- методів не може бути безумовною заміною експертних правил, сегментації, журналювання та людського контролю. У середовищі енергетики, транспорту й зв'язку доцільною є гібридна модель, у якій сигнатурні правила, контекст галузі, базові політики безпеки й поведінкові моделі працюють спільно. Такий підхід знижує ризик як пропуску нової атаки, так і надмірної довіри до моделі, яка може бути нестійкою до нестандартних сценаріїв або навмисного обману. Інтелектуальний аналіз даних у задачах кібербезпеки доцільно розглядати не як окремий набір алгоритмів, а як багаторівневий методичний підхід до інтерпретації подій інформаційної безпеки.

Контрольована класифікація забезпечує автоматизоване віднесення об'єктів до відомих класів загроз. Кластеризація дозволяє виявляти структури та групи в умовах браку розмічених даних. Аномальний аналіз орієнтований на виявлення невідомих або слабко формалізованих відхилень. Часові та потокові методи враховують динаміку інциденту, а графові моделі – зв'язки між елементами інфраструктури. Для об'єктів критичної інформаційної інфраструктури найбільш результативною є комбінація цих підходів, адаптована до секторної специфіки енергетики, транспорту та зв'язку. Саме така комбінація створює методологічне підґрунтя для переходу до підрозділу 2.3, де центральне місце посідатимуть методи виявлення аномалій та кореляції подій безпеки.

2.3. Методи виявлення аномалій та кореляції подій безпеки

У системах кіберзахисту критичної інформаційної інфраструктури виявлення аномалій і кореляція подій безпеки утворюють взаємопов'язаний

аналітичний контур, без якого неможливе своєчасне розпізнавання складних інцидентів. Якщо класифікація подій дозволяє впорядкувати журнальні записи та виділити їхні типові категорії, то аномальний аналіз орієнтований на фіксацію відхилень від нормального стану, а кореляція – на поєднання окремих сигналів у цілісний сценарій атаки. У сучасному середовищі кіберзагроз це має визначальне значення, оскільки значна частина цільових атак розгортається як послідовність слабких, рознесених у часі дій, кожна з яких окремо може виглядати технічно допустимою. ENISA у матеріалах 20252026 років вказує на поєднання різних векторів початкового доступу, зокрема експлуатації вразливостей та підтриманих штучним інтелектом фішингових кампаній, що ускладнює виявлення інциденту на рівні окремого правила або сигнатури. Для енергетики, транспорту і зв'язку це означає, що ефективне виявлення загрози повинне спиратися не лише на заздалегідь визначені індикатори, а й на аналіз поведінкових відхилень та міжподієвих залежностей.

Методи виявлення аномалій базуються на припущенні, що нормальний режим роботи інформаційної або технологічної системи має достатньо стійкий профіль, а суттєве відхилення від нього може бути ознакою інциденту. У базовому вимірі такий підхід реалізується через статистичне моделювання, коли для конкретних параметрів визначаються допустимі діапазони, частоти або часові закономірності. Для критичної інфраструктури цей підхід зберігає актуальність, особливо у випадках, коли об'єкт має стабільний режим функціонування. В енергетиці це можуть бути очікувані шаблони мережевої взаємодії між диспетчерськими вузлами, контролерами та інженерними станціями. У транспортному секторі – регулярність звернень до систем диспетчеризації, бронювання або внутрішніх сервісів маршрутизації.

У телекомунікаційному середовищі – типові профілі сигнального обміну, завантаження мережевих вузлів і характер міжсегментної взаємодії. Статистичні моделі мають перевагу у прозорості та чіткій інтерпретації результатів, однак їхня ефективність знижується у випадку складних, динамічних середовищ, де нормальна поведінка залежить від зовнішніх чинників, часу доби, режиму

навантаження або змін конфігурації. Більш розвиненим підходом є поведінкове виявлення аномалій, яке орієнтується не на окремі порогові значення, а на модель типової поведінки системи, користувача, пристрою або протоколу. Саме цей напрям NIST детально демонструє в NIST IR 8219 для промислових систем, де технології поведінкового аналізу (behavioral anomaly detection) застосовуються до виробничих і процесних середовищ для виявлення нетипових мережевих взаємодій, несанкціонованих модифікацій логіки HMI, нестандартних діагностичних функцій Modbus, деформованої структури трафіку (аномально сформованого трафіку), доступу до незареєстрованих адрес пам'яті та сканування ICS-пристроїв. Методологічне значення цього підходу для критичної інформаційної інфраструктури полягає в тому, що він здатний виявляти не лише відомі сценарії атак, а й атипову активність, яка не збігається з жодною сигнатурою, але порушує звичний профіль технологічного процесу.

Для енергетичних об'єктів це дає змогу фіксувати аномальні команди в OT-сегменті, появу нових напрямів трафіку або нетипову взаємодію між PLC і SCADA. Для транспорту поведінковий аналіз корисний у виявленні незвичних ланцюгів доступу до диспетчерських платформ і логістичних сервісів. У секторі зв'язку аналогічна логіка застосовується до маршрутизаційних, сигнальних і адміністративних подій, де прихована присутність порушника проявляється через нетиповий, але не обов'язково явно шкідливий шаблон активності. У практиці 2026 року значного поширення набули також методи машинного навчання для аномального виявлення, насамперед неконтрольовані та напівконтрольовані моделі. Їх застосування зумовлене тим, що для більшості середовищ КІІ відсутні повні й якісно розмічені набори даних інцидентів, натомість доступний великий масив телеметрії нормального функціонування.

За таких умов модель тренується на масивах легітимних даних і надалі фіксує відхилення від вивченого профілю. Для енергетики це дозволяє виявляти повільні дрейфи мережевої або технологічної поведінки, які можуть бути наслідком підготовки до втручання в процес керування. Для транспортної інфраструктури – розпізнавати нетипові шаблони взаємодії між інформаційними

вузлами, які передують збою або спробі компрометації. Для зв'язку – відстежувати відхилення в керуванні мережею, сигнальному обміні та поведінці адміністративних сесій. Водночас застосування машинного навчання не усуває потреби в експертному контролі, оскільки математичні моделі є вразливими до динамічного концептуального зсуву (концептуального зсуву), зміни архітектури та атак на сам життєвий цикл математичного забезпечення.

NIST у рекомендаціях щодо протидії навмисному спотворенню моделей підкреслює, що такі алгоритми можуть зазнавати маніпуляцій через дані, ознаки або механізми ухилення, а для критичної інфраструктури це робить недоцільною повну заміну прозорих і пояснюваних механізмів виявлення лише автоматизованими моделями. Кореляція подій безпеки виконує іншу, але не менш важливу функцію. Її сутність полягає в поєднанні подій із різних джерел у логічно зв'язаний ланцюг, що дозволяє переходити від окремого сповіщення до реконструкції сценарію атаки. NIST SP 800-61 Rev. 3 наголошує, що постачальник послуг або централізована аналітична служба може виявити шкідливу активність раніше, ніж окрема організація, саме завдяки можливості корелювати події між різними джерелами та інцидентами [8].

У середовищі КІІ цей принцип набуває особливої ваги, оскільки атака на критичний об'єкт майже ніколи не обмежується єдиною точкою входу чи одним логом. Вона може початися з фішингової компрометації користувача, перейти в несанкціонований VPN-доступ, далі – у зміну конфігурації шлюзу, а завершитися взаємодією з технологічним сегментом або критичним прикладним сервісом. Без кореляції кожна з цих подій виглядатиме локальною аномалією; після кореляції вони утворюють послідовність, яка вже однозначно вказує на інцидент. У сучасних системах моніторингу доцільно виокремлювати кілька основних підходів до кореляції подій безпеки. Перший підхід є правиловим і базується на заздалегідь сформульованих детермінованих умовах, серед яких збіг часових меж, джерела, адресата, типу події, ознак критичності або послідовності дій.

Такий підхід широко реалізується в SIEM-платформах і залишається

необхідним для виявлення відомих сценаріїв, зокрема неуспішної серії входів із подальшим успішним доступом, зміни конфігурації після автентифікації з нової адреси або появи мережевої взаємодії між сегментами, які не повинні комунікувати. Другий підхід є часово- послідовнісним і орієнтований на аналіз того, як саме події розгортаються у визначеному часовому вікні. Третій підхід є контекстним або топологічним, коли кореляція враховує роль вузла в архітектурі, критичність активу, сегмент мережі, тип сервісу та ймовірні шляхи латерального переміщення порушника. Для телекомунікаційного сектора саме контекстна кореляція часто дає змогу відрізнити технічну помилку від прихованої шкідливої активності, оскільки одна й та сама мережева дія має різну аналітичну вагу залежно від того, чи відбувається вона в периферійному вузлі, чи в мережевому ядрі. Для енергетики, транспорту і зв'язку кореляція подій має секторно-специфічний зміст.

В енергетичному середовищі результативною є кореляція між подіями автентифікації, зверненнями до серверів керування, мережевими потоками між IT- та OT-сегментами і технологічними діями в SCADA або PLC. Така модель дозволяє виявляти сценарії, коли цифровий інцидент переходить у площину впливу на фізичний процес. У транспорті корисною є кореляція між подіями у вебсервісах, бекенд-системах, мережевій периферії, системах резервного керування і прикладних логах диспетчеризації; це дає змогу пов'язати атаки типу DDoS або компрометацію облікового запису з подальшим порушенням операційного контуру. Для зв'язку визначальним є поєднання мережевих, сигнальних, адміністративних та сервісних подій, оскільки загрози в цьому секторі часто пов'язані не з одномоментною відмовою, а з прихованим закріпленням, шпигунством або поступовим впливом на критичні елементи цифрової інфраструктури. ENISA у 2026 році прямо вказувала на актуальність загроз шпигунства в телеком-мережах і на необхідність підвищеної уваги до стійкості цифрової інфраструктури, що підсилює вимогу саме до кореляційної аналітики, а не до ізольованого перегляду журналів [12].

Результативність аномального виявлення і кореляції подій безпеки

безпосередньо залежить від якості нормалізації даних, повноти журналювання, часової синхронізації, релевантності ознак та зрілості процедур реагування. Навіть найкраща модель не забезпечить кіберстійкості, якщо вона працює на неповних даних або не інтегрована в операційні процеси SOC, IT- та OTпідрозділів. CISA у Cross-Sector Cybersecurity Performance Goals 2.0 відносить централізоване журналювання, виявлення, реагування та відновлення до базових практик для критичної інфраструктури, що підтверджує системний статус цих механізмів у сучасному підході до захисту. Для КІІ це означає, що методи виявлення аномалій і кореляції повинні розглядатися як частина ширшої архітектури кіберстійкості, де аналітика підтримує не лише детекцію, а й пріоритезацію рішень під час інциденту, оцінку масштабу впливу та планування відновлення. Саме з цієї причини подальший аналіз систем моніторингу безпеки, зокрема SIEM, SOC та IDS/IPS, є логічним продовженням дослідження методів інтелектуального аналізу даних у кібербезпеці.

2.4. Огляд сучасних систем моніторингу безпеки та їх можливостей

У сучасній архітектурі кіберзахисту критичної інформаційної інфраструктури системи моніторингу безпеки виконують роль сполучної ланки між збиранням телеметрії, аналітикою подій, реагуванням на інциденти та підтриманням кіберстійкості. У методичних підходах NIST безперервний моніторинг розглядається як підтримання постійної обізнаності щодо стану безпеки, вразливостей і загроз для ухвалення рішень з управління ризиками, а у CSF 2.0 функція Detect прямо пов'язується зі своєчасним виявленням і аналізом атак та компрометацій. Для об'єктів критичної інфраструктури це означає, що системи моніторингу не можуть розглядатися як допоміжний IT-сервіс. У секторах енергетики, транспорту і зв'язку вони є частиною операційного механізму забезпечення стійкості, оскільки саме від швидкості виявлення та якості інтерпретації подій залежить, чи переросте цифровий інцидент у

порушення надання критичної послуги. ENISA у NIS360 2026 відносить електроенергетику й телекомунікації до секторів із водночас високою кіберзрілістю та високою критичністю, що прямо підсилює вимогу до розвинених засобів моніторингу й аналітики.

Центральне місце у сучасних засобах моніторингу займають платформи SIEM. У термінології NIST SIEM визначається як програмний засіб, що забезпечує централізовані можливості журналювання для різних типів логів, а в оновленому підході до управління журналами (log management) такі платформи розглядаються як компоненти централізованої інфраструктури, які виконують безпековий моніторинг, надають сховища для збереження, аналітичні сервіси та автоматизовані робочі процеси обробки даних. Функціонально SIEM поєднує збір журналів із різнорідних джерел, їх нормалізацію, збереження, кореляцію, побудову правил виявлення, пріоритезацію сповіщень і надання аналітику цілісної картини інциденту. Для критичної інформаційної інфраструктури цінність SIEM полягає в тому, що платформа дозволяє об'єднати в єдиному просторі мережеві журнали, системні події, телеметрію засобів захисту, події автентифікації та, за наявності інтеграції, дані з OT- або телекомунікаційного середовища. Саме ця централізація створює основу для виявлення складних сценаріїв атаки, коли окремі сигнали з різних сегментів лише в сукупності набувають значення інциденту.

На рис. 2.1 наведено узагальнена схема інтелектуального аналізу подій безпеки.

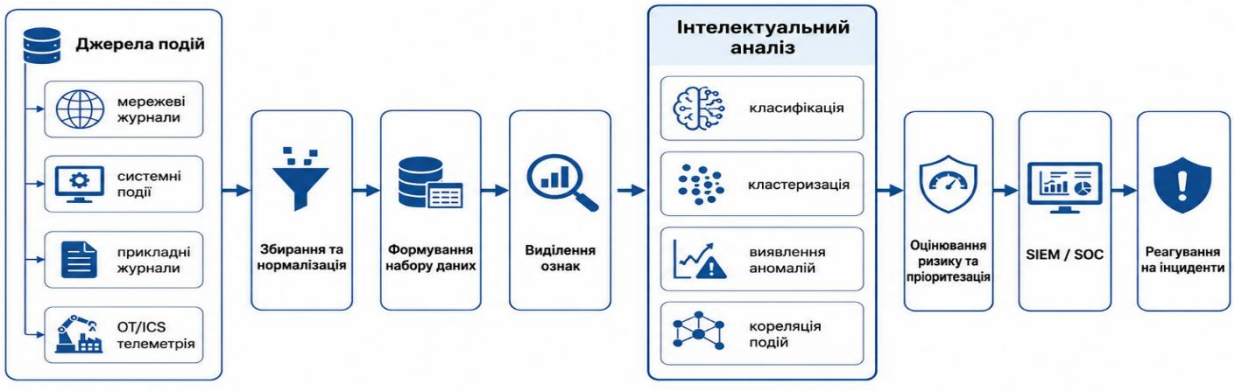

Рис. 2.1. Узагальнена схема інтелектуального аналізу подій безпеки

Практичні можливості SIEM не зводяться до централізованого зберігання логів. Для об'єктів критичної інфраструктури ключовими є саме кореляційні та контекстні механізми. В енергетичному секторі платформа SIEM має поєднувати події з міжмережевих екранів, серверів автентифікації, систем віддаленого доступу, робочих станцій операторів і, за можливості, телеметрію з SCADA або технологічних шлюзів. У транспортному середовищі SIEM набуває цінності як засіб зведення воєдино подій вебпорталів, систем бронювання, диспетчерських платформ, мережевої периферії та резервних контурів керування. У секторі зв'язку на перший план виходить кореляція між подіями мережевого ядра, адміністративних систем, журналами маршрутизації, засобами доступу та телекомунікаційними сервісними платформами.

CISA у рекомендаціях для критичної інфраструктури прямо вказувала на доцільність налаштування SIEM для моніторингу, аналізу та кореляції логів у мережах ICS, що підтверджує доцільність такого підходу і для середовищ, де цифровий контур безпосередньо впливає на фізичний процес. Водночас платформа SIEM не є самодостатньою. Її ефективність визначається повнотою джерел, якістю нормалізації, релевантністю правил і здатністю аналітиків інтерпретувати сповіщення в контексті конкретного сектора. Для критичної інфраструктури типовими проблемами залишаються надлишковість журналів, високий рівень хибнопозитивних спрацювань, складність інтеграції застарілих OT-компонентів, різна часово-логічна семантика IT- і технологічних подій, а також труднощі з тривалою ретенцією даних достатньої глибини. NIST у SP 800-92 і його оновленій редакції наголошує, що лог-менеджмент охоплює не лише генерацію, а й огляд, захист, збереження й використання журналів, а отже платформа SIEM без належної організації процесів не дає потрібного ефекту.

Для енергетики та зв'язку це означає потребу в суворій пріоритезації джерел і глибокому врахуванні того, які події реально критичні для підтримання сервісу, а які лише створюють аналітичний шум. Організаційним центром роботи з подіями безпеки виступає SOC – Security Operations Center. У

термінології NIST SOC визначається як фокальна точка для безпекових операцій і оборони мережі організації, призначена для безперервного моніторингу, виявлення, аналізу та своєчасного реагування на кіберінциденти. ENISA у настановах з побудови CSIRT і SOC також характеризує SOC як службу виявлення інцидентів, що спостерігає технічні події в мережах і системах та може відповідати за реагування і обробку інцидентів. Для критичної інфраструктури принциповим є те, що SOC – це не просто команда операторів SIEM.

Його функція охоплює тріаж, розслідування, активний пошук загроз (активний пошук загроз), взаємодію з експлуатаційними та технологічними підрозділами, ухвалення рішень про ізоляцію сегментів, ескалацію інциденту, а також накопичення й передачу досвіду, отриманого під час реагування на інциденти. У цій моделі технологія без процесу є недостатньою, а процес без аналітичної платформи – неоперативним. Для об'єктів енергетики, транспорту та зв'язку SOC має секторно- специфічну побудову. В енергетиці робота SOC потребує тісної інтеграції з OT-фахівцями та диспетчерськими службами, оскільки сповіщення про підозрілу активність можуть вимагати оцінки потенційного впливу на технологічний процес, а рішення про блокування або сегментацію не можна ухвалювати без урахування операційної безпеки. У транспортному секторі SOC має враховувати взаємозалежність між цифровими сервісами й рухомим, диспетчерським та логістичним контурами, де навіть короткочасний збій у реагуванні може створити каскадні наслідки для доступності сервісу.

У секторі зв'язку ключовим стає вміння розрізняти технічні збої, навмисні дії на рівні мережевого ядра, шпигунську активність і атаки на доступність. ENISA у 2025-2026 роках окремо підкреслювала ризики шпигунства в телекоммережах, стійкість цифрової інфраструктури та довготривалі кампанії проти телекомунікаційних і логістичних мереж, що безпосередньо підвищує значення SOC як центру аналітичного та операційного реагування. Сенсорним і частково превентивним шаром моніторингу виступають IDS/IPS – системи

виявлення та запобігання вторгненням. NIST SP 800-94 визначає їх як технології, спрямовані на ідентифікацію можливих інцидентів, журналювання відомостей про них, спробу зупинення шкідливої активності та повідомлення адміністраторів безпеки. NIST також виділяє чотири основні класи інструментів IDPS: мережеві, бездротові, засоби аналізу поведінки мережі (network behavior analysis) та хостові системи.

У структурі захисту критичної інфраструктури IDS/IPS виконують функцію первинного спостереження за трафіком, поведінкою протоколів, мережевими аномаліями, відомими сигнатурами атак і порушеннями політик доступу. Для енергетики та інших OT-середовищ це особливо важливо, оскільки мережеві IDPS можуть виявляти несанкціоновані взаємодії між сегментами, аномалії в індустріальних протоколах і спроби сканування технологічних вузлів. Для транспортних і телекомунікаційних систем IDS/IPS є важливими як засоби раннього попередження на мережевій периферії, у датацентрових сегментах, вузлах доступу та точках інтеграції з зовнішніми сервісами. Разом із цим IDS/IPS мають чіткі межі застосовності. Сигнатурна логіка таких систем добре працює проти відомих шаблонів, але поступається ефективністю там, де атака використовує легітимні інструменти середовища або тактику використання довіреного простору (використання довірених сервісів та легітимних інструментів середовища), приховану взаємодію або повільні багатоступеневі сценарії [14].

У критичній інфраструктурі додатковим обмеженням є ризик хибнопозитивного блокування: в OT-мережах невдале превентивне спрацювання IPS може порушити технологічний процес, а в телекомунікаційних або транспортних середовищах – критично вплинути на доступність сервісу. Саме тому CISA у рекомендаціях для ICS наголошує не лише на запровадженні моніторингу, а й на визначенні безпечних точок його розміщення, способів передавання даних і надійних механізмів (trusted mechanisms) для збору телеметрії. Для практики захисту КІІ це означає, що IDS/IPS найрезультативніші не як ізольований засіб, а як частина багаторівневої архітектури, де їхні

спрацьовування збагачуються контекстом SIEM і перевіряються аналітиками SOC. сучасні системи моніторингу безпеки доцільно розглядати як функціонально розподілену, але концептуально єдину систему. SIEM забезпечує централізацію, кореляцію та аналітичне осмислення подій. SOC виконує операційне управління виявленням, розслідуванням і реагуванням [15].

IDS/IPS формують мережевий і хостовий сенсорний рівень, а частково й превентивний контур захисту. Для об'єктів критичної інформаційної інфраструктури результативність цієї моделі визначається не наявністю окремих продуктів, а здатністю інтегрувати їх у секторно орієнтовану систему кіберстійкості, де враховуються OT-специфіка енергетики, сервісна й логістична чутливість транспорту, а також мережево-ядерний характер телекомунікаційного сектора. Саме така інтегрована модель створює прикладне підґрунтя для подальшого переходу до проєктування власного підходу до інтелектуального аналізу подій безпеки в межах наступного розділу роботи.

Висновки до розділу 2

У розділі 2 систематизовано події інформаційної безпеки, визначено їх основні джерела в IT- та OT-середовищах і обґрунтовано необхідність інтелектуального аналізу великих масивів телеметрії. Розглянуто сучасні методи класифікації, кластеризації, виявлення аномалій, кореляції подій і проаналізовано функціональні можливості систем SIEM, SOC та IDS/IPS. Це дозволило сформувати методичну основу для розробки власного підходу до інтелектуального аналізу подій безпеки.

РОЗДІЛ 3 РОЗРОБКА ПІДХОДУ ДО ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ПОДІЙ БЕЗПЕКИ

3.1. Постановка задачі аналізу подій інформаційної безпеки

Побудова підходу до інтелектуального аналізу подій безпеки в інформаційних системах критичної інфраструктури потребує чіткої постановки задачі, оскільки ефективність будь-якої моделі безпосередньо залежить від того, наскільки точно визначено об’єкт спостереження, аналітичну мету, перелік джерел даних, вимоги до результату та обмеження середовища. Для об’єктів енергетики, транспорту та зв’язку задача аналізу подій безпеки не зводиться до виявлення окремих шкідливих записів у журналах. Її зміст полягає у своєчасному виявленні відхилень, які можуть свідчити про підготовку, розвиток або реалізацію кіберінциденту, здатного вплинути на безперервність критичної послуги, керованість технологічного процесу або цілісність оперативних рішень. У такому формулюванні задача має не лише технічний, а й функціональний характер, оскільки кінцевою метою є не класифікація логів як така, а підтримання кіберстійкості об’єкта [16].

У середовищі критичної інформаційної інфраструктури аналітична задача ускладнюється трьома факторами. Перший пов’язаний із гетерогенністю джерел подій. У типовому середовищі КІІ одночасно існують мережеві журнали, системні події серверів і робочих станцій, телеметрія засобів автентифікації, журнали прикладних платформ, події OT-компонентів і дані про стан технологічного процесу. Другий фактор полягає в різній часовій природі подій.

Частина з них має дискретний характер, наприклад вхід користувача або зміна правила на міжмережевому екрані, тоді як інша частина є потоковою і формується безперервно, як у випадку SCADA-телеметрії, сигнального обміну чи мережевих потоків. Третій фактор зумовлений тим, що один і той самий

інцидент може проявлятися в різних сегментах інфраструктури з різною інтенсивністю та різною семантикою. Для енергетики це може бути поєднання атипового віддаленого входу, зміни конфігурації технологічного шлюзу й нетипової команди в ОТ-сегменті. Для транспорту – спроба несанкціонованого доступу до прикладного сервісу, аномальна мережева взаємодія з резервним вузлом та подальше порушення диспетчерської синхронізації [16].

Для сектора зв'язку – прихована присутність у мережевому ядрі, що спочатку проявляється лише як незначна маршрутизаційна аномалія або нетипова адміністративна сесія. У зв'язку з цим задачу аналізу подій доцільно формулювати як задачу побудови інтелектуального механізму, здатного виявляти аномальні або підозрілі патерни у великому масиві різнорідних подій інформаційної безпеки, визначати їхню можливу належність до сценаріїв кіберзагроз і формувати аналітичний висновок щодо рівня ризику для критичної функції об'єкта. Така постановка передбачає поєднання трьох компонентів: спостереження, інтерпретації та пріоритезації. Спостереження охоплює збирання й агрегування подій з усіх релевантних джерел [17].

Інтерпретація полягає у визначенні, чи є подія або група подій відхиленням від нормального профілю. Пріоритезація означає оцінку того, наскільки виявлене відхилення є небезпечним саме для конкретного сектора критичної інфраструктури. У цьому контексті одна й та сама аномалія може мати різну вагу: зміна параметра технологічного протоколу на енергетичному об'єкті потенційно небезпечніша за аналогічну дію в звичайному офісному сегменті, а нетипова сигнальна подія в мережі оператора зв'язку може мати системний ефект навіть без явного порушення доступності сервісу. Формалізація задачі потребує також визначення вхідних і вихідних параметрів моделі [18].

Вхідними даними є події безпеки, подані у вигляді структурованих записів із часовою міткою, джерелом, типом події, технічними атрибутами та, за наявності, контекстом активу. Вихідними результатами мають бути оцінка аномальності події або їх послідовності, класифікація за рівнем критичності, виявлення ланцюгів подій, що можуть формувати сценарій атаки, а також

формування аналітичного повідомлення, придатного для подальшого використання в SIEM або SOC. З практичної точки зору така модель повинна вирішувати щонайменше чотири підзадачі: зниження шуму, виявлення слабких сигналів, скорочення кількості хибнопозитивних спрацювань і підтримка раннього виявлення інциденту. У середовищі КІІ ці підзадачі є взаємозалежними, оскільки перевантаження аналітика шумом безпосередньо зменшує ймовірність своєчасного виявлення реальної загрози [19].

Обмеження задачі також мають бути визначені на етапі постановки. Для критичної інфраструктури типовими є дефіцит розмічених даних, неможливість вільного тестування на реальному виробничому середовищі, наявність застарілих компонентів, нерівномірна якість журналювання, а також висока вартість помилкового реагування. У системах енергетики й транспорту невдале автоматичне блокування або некоректна ізоляція сегмента може завдати не менше шкоди, ніж сам інцидент. Для сектора зв’язку критичним є ризик непропорційного впливу на доступність мережі [20].

Саме тому задача аналізу подій повинна орієнтуватися не на повну автоматизацію будь-якого рішення, а на формування аналітично обґрунтованих індикаторів і пріоритетів для фахівця SOC або оператора безпеки. У такому вигляді інтелектуальний аналіз виступає інструментом підтримки прийняття рішень, а не неконтрольованим механізмом автономного втручання. З методичного погляду задача аналізу подій інформаційної безпеки в межах цього дослідження може бути визначена як задача виявлення аномальних і потенційно шкідливих послідовностей подій у гібридному IT/OT-середовищі на основі попередньої підготовки даних, побудови ознакового простору, застосування алгоритму аномального аналізу та подальшої інтерпретації результату в контексті критичності активу. Таке формулювання забезпечує зв’язок між теоретичними положеннями другого розділу і прикладною частиною роботи, оскільки дозволяє перейти від загального огляду методів до розробки конкретного підходу, придатного для навчального або тестового середовища. Для енергетики, транспорту і зв’язку принципово важливо, що у фокусі

залишаються не абстрактні мережеві аномалії, а саме ті події, які можуть вплинути на цифрову підтримку критичної функції. Саме це визначає прикладний зміст подальших підрозділів, де буде сформовано набір даних, запропоновано модель аналізу та описано її реалізацію.

3.2. Формування набору даних подій безпеки та їх підготовка до аналізу

Побудова моделі інтелектуального аналізу подій безпеки неможлива без формування репрезентативного набору даних, який відображає як нормальний режим функціонування системи, так і події, що мають ознаки загроз або аномальної поведінки. У середовищі критичної інформаційної інфраструктури це завдання ускладнюється тим, що джерела телеметрії є неоднорідними, рівень деталізації подій відрізняється, а пряме використання реальних виробничих даних часто обмежується вимогами безпеки, конфіденційності та режиму експлуатації. З цієї причини в навчально- дослідницькій практиці доцільно формувати тестовий набір даних на основі поєднання відкритих логів, синтетично згенерованих подій, прикладів типових мережевих записів і змодельованих сценаріїв для IT та OT-сегментів. Такий підхід не претендує на відтворення всієї повноти реального середовища, проте дозволяє побудувати коректну методику аналізу та оцінити працездатність алгоритму без порушення етичних і правових меж [21].

Структурно набір даних подій безпеки має відображати багаторівневу природу критичної інфраструктури. Для цього до нього доцільно включати записи з мережевого, системного, прикладного і технологічного рівнів. На мережевому рівні це можуть бути події міжмережевих екранів, IDS/IPS, NetFlow/IPFIX, журнали маршрутизаторів і комутаторів. На системному рівні – журнали Windows Event Logs, Syslog, події служб автентифікації, записи про

створення процесів, зміну облікових записів і доступ до критичних об’єктів.

На прикладному рівні – журнали вебсервісів, API-звернень, баз даних, резервного копіювання, диспетчерських і логістичних платформ. На технологічному рівні – події SCADA, PLC, HMI, історіанів та інженерних станцій. Для телекомунікаційного сегмента замість класичних SCADA компонентів логічно включати події маршрутизації, сигнального обміну, мережевого ядра та систем керування мережею. Така композиція даних дозволяє надалі тестувати модель не на ізольованому класі записів, а на середовищі, яке ближче до реальної архітектури КІІ.

У табл. 3.1 наведено узагальнена структура тестового набору даних подій безпеки.

Таблиця 3.1

Узагальнена структура тестового набору даних подій безпеки

Група ознак	**Приклади атрибутів**	**Призначення**
Часові	час події, інтервал, частота	Виявлення нетипових часових патернів
Мережеві	джерело, адресат, протокол, напрям трафіку	Пошук міжсегментних відхилень
Системні	тип автентифікації, процес, зміна конфігурації	Оцінка поведінки користувачів і служб
Технологічні	команда ОТ, зміна параметра, звернення до SCADA/PLC	Контроль впливу на критичний процес

Під час формування набору даних доцільно передбачити наявність двох типів спостережень: фонових та аномальних. Фонові записи мають відображати нормальне функціонування середовища: штатні входи користувачів, типові мережеві потоки, регламентні зміни конфігурацій, технологічні телеметричні цикли, синхронізацію сервісів, резервне копіювання, передачу даних між системами. Аномальні записи мають моделювати або відображати типові загрозові сценарії: серії невдалих входів із подальшим успішним доступом, нетипові віддалені підключення, підозрілі запити до критичних сервісів,

сканування сегментів, аномальні потоки між IT- та OT-рівнями, нетипові зміни параметрів технологічного процесу, конфігураційні зміни поза регламентом, а також сигнальні або маршрутизаційні відхилення для сектора зв'язку. Групування таких записів дозволяє створити набір даних, придатний як для неконтрольованого виявлення аномалій, так і для подальшої експертної перевірки отриманих результатів.

Не менш важливим етапом є нормалізація даних. Події безпеки, отримані з різних джерел, зазвичай мають відмінну структуру, різний формат часових міток, нерівномірне наповнення полів і неоднакову семантику. Для забезпечення придатності до машинного аналізу всі записи доцільно привести до уніфікованої таблиці ознак, де кожен рядок відображає окрему подію, а кожне поле містить стандартизований атрибут: час, тип події, джерело, адресат, протокол, категорію дії, користувача, хост, рівень критичності, секторний контекст, належність до IT або OT-сегмента. У дослідницькій реалізації це може бути виконано у форматі CSV або Parquet із подальшою обробкою в Python.

Саме етап нормалізації визначає, чи зможе модель коректно порівнювати події між собою, оскільки одна й та сама дія в різних системах може позначатися різними кодами, назвами або рівнями деталізації. Після нормалізації виконується очищення даних. До цієї процедури входять видалення дублікатів, обробка пропущених значень, усунення явно некоректних записів, гармонізація часових поясів і впорядкування даних за хронологією. Для подій критичної інфраструктури особливого значення набуває часове узгодження, оскільки навіть незначне зміщення часових міток між джерелами може призвести до хибної інтерпретації послідовності подій.

Наприклад, у моделі атаки на енергетичний об'єкт різниця між фактичним моментом входу в сервер адміністрування і моментом технологічної команди в OT-сегменті є ключовою для побудови кореляції. Аналогічно в транспортному або телекомунікаційному середовищі часова неузгодженість може зруйнувати логіку переходу від зовнішнього інциденту до внутрішньої операційної аномалії. Саме тому підготовка набору даних має враховувати не лише технічну чистоту

записів, а й аналітичну цілісність часової структури. Наступним кроком є побудова ознакового простору.

Для інтелектуального аналізу подій безпеки недостатньо використовувати первинні журнальні поля в їх сирому вигляді. Необхідно сформувати похідні ознаки, що краще відображають поведінкові закономірності: кількість подій певного типу за інтервал часу, частоту звернень із конкретного вузла, кількість невдалих входів перед успішною автентифікацією, появу нових маршрутів трафіку, відстань між типовими і нетиповими часовими інтервалами, кількість змін конфігурації за добу, частоту взаємодії між IT- та OT-сегментами, коефіцієнт відхилення від нормального профілю. Для енергетики доцільними є ознаки, пов’язані з нетиповими технологічними командами, нестандартною появою зовнішніх з’єднань і змінами параметрів процесу. Для транспорту – ознаки концентрації подій на окремих сервісах координації, аномалії доступу до логістичних вузлів і порушення звичних часових патернів.

Для зв’язку – ознаки нетипових адміністративних сесій, маршрутизаційних відхилень і сигнальних подій, які не відповідають звичній мережевій поведінці. Оскільки в дослідженні передбачається застосування аномального аналізу, набір даних доцільно структурувати так, щоб основну частину становили фонові записи, а аномальні події були меншістю. Це відповідає реальній природі кібермоніторингу, де справжні інциденти трапляються значно рідше, ніж нормальна активність. У такому випадку алгоритм навчається на переважно легітимному масиві спостережень і надалі виявляє записи, які за своїми ознаками істотно відхиляються від норми.

Для підвищення аналітичної цінності моделі доцільно також позначити окремі підмножини подій як умовно аномальні для подальшої перевірки якості роботи алгоритму. Йдеться не про побудову повноцінного повністю розміченого набору даних, а про створення контрольної вибірки, за якою можна оцінити, чи модель дійсно виокремлює небезпечні патерни. Такий підхід є методично виправданим для навчально-дослідницького проєкту, де головним є не індустріальна точність, а демонстрація коректної логіки побудови рішення.

Відповідно, підготовка набору даних подій безпеки в межах цього дослідження включає чотири взаємопов’язані етапи: збирання та агрегацію даних із багаторівневих джерел, нормалізацію та очищення записів, формування ознак і створення контрольної вибірки для оцінювання результатів.

Саме така структура набору даних створює аналітичну основу для побудови моделі інтелектуального аналізу, орієнтованої на виявлення аномалій і слабких сигналів у середовищі критичної інфраструктури. Для енергетики, транспорту та зв’язку це дозволяє моделювати не абстрактний потік логів, а ситуацію, максимально наближену до реального гібридного середовища, де цифрова подія має оцінюватися через її можливий вплив на критичну функцію об’єкта. На цій основі в наступному підрозділі може бути запропонована конкретна модель або алгоритм інтелектуального аналізу подій безпеки.

3.3. Розробка моделі або алгоритму інтелектуального аналізу подій безпеки

Розробка моделі інтелектуального аналізу подій безпеки для об’єктів критичної інформаційної інфраструктури має спиратися на поєднання трьох вимог: здатності працювати з великим обсягом різнорідних даних, чутливості до малопомітних відхилень та придатності до пояснення результату в контексті кіберстійкості. Застосування складних багатошарових моделей машинного навчання саме по собі не гарантує кращого результату, якщо модель є непрозорою, важко налаштовується або вимагає великого масиву розмічених даних, які в середовищі КІІ зазвичай відсутні. З цієї причини для дослідницької реалізації доцільно обрати гібридний підхід, у якому базою виступає алгоритм аномального виявлення, а його результати додатково збагачуються правилами контекстної інтерпретації. Така модель є достатньо простою для реалізації в навчальному проєкті й водночас достатньо наближеною до реальної практики, де автоматичне виявлення рідко існує без експертного контексту або правилової

надбудови.

Як базовий алгоритм доцільно використати алгоритм Isolation Forest, який широко застосовується для задач виявлення викидів у середовищах без повного розмічення даних. Алгоритм ізолює спостереження шляхом випадкового вибору ознаки та випадкового порогу розбиття; аномальні об’єкти, як правило, ізолюються за меншу кількість кроків, ніж нормальні. Для задач кібербезпеки цей підхід є придатним з кількох причин [26-28]. По-перше, він не потребує великої кількості еталонно розмічених інцидентів.

На рис. 3.1 наведено логіка роботи запропонованого алгоритму аналізу подій безпеки.

Рис. 3.1. Логіка роботи запропонованого алгоритму аналізу подій безпеки

По-друге, він працює з багатовимірним ознаковим простором, де аномалія може виявлятися не в одному полі, а в поєднанні кількох характеристик. По-третє, алгоритм достатньо легкий з обчислювального погляду, що робить його придатним для експериментальної реалізації у Python та подальшої інтеграції з SIEM- орієнтованою логікою [29-30]. Для середовищ енергетики, транспорту і зв’язку це означає можливість виявляти атипові поєднання мережевої, системної та технологічної активності без жорсткого прив’язування до наперед заданих сигнатур. Структурно запропоновану модель можна подати як послідовність чотирьох блоків: підготовка даних, обчислення ознак, аномальне оцінювання,

контекстна інтерпретація.

У блоці підготовки даних журнальні записи нормалізуються, очищуються, синхронізуються за часом та переводяться у числовий або категоріально-кодований формат. У блоці побудови ознак формуються індикатори, що відображають частоту, повторюваність, інтенсивність, міжсегментні зв'язки, часові інтервали та появу нових патернів взаємодії. У блоці аномального оцінювання алгоритм Isolation Forest обчислює оцінку аномальності для кожної події або агрегованого вікна подій. У блоці контекстної інтерпретації цей показник коригується з урахуванням критичності активу, належності події до IT чи OT-сегмента, типу джерела, часової близькості до інших підозрілих подій та наявності відомих правил ризику.

Саме останній блок є критично важливим для КІІ, оскільки в умовах енергетики, транспорту чи зв'язку аномалія на периферійному вузлі і аномалія на критичному сегменті не можуть оцінюватися однаково. Для підвищення якості інтерпретації доцільно використовувати не окремі події, а часові вікна спостереження. Наприклад, замість того щоб оцінювати кожен запис із журналу окремо, можна агрегувати події за п'ятихвилинними або десятихвилинними інтервалами й обчислювати для кожного вікна набір ознак: кількість невдалих входів, число унікальних джерел, кількість змін конфігурації, обсяг нетипового трафіку, кількість звернень до критичних сервісів, частоту подій OT-сегмента, появу нових маршрутів або нових користувачів. Такий підхід краще відображає реальну природу інциденту, оскільки атака рідко складається з однієї події; зазвичай вона проявляється як послідовність взаємопов'язаних дій у межах певного часового інтервалу.

Для енергетичного середовища це може бути серія мережевих звернень до технологічного шлюзу, для транспорту – скупчення нетипових прикладних запитів і спроб доступу до резервного контуру, для зв'язку – серія аномальних адміністративних або маршрутизаційних подій. Оскільки аномальні алгоритми схильні виявляти не лише загрози, а й будь-які статистично нетипові стани, до моделі доцільно додати контекстно- правиловий модуль. Його функція полягає

у зменшенні кількості хибнопозитивних результатів шляхом урахування знань про архітектуру об’єкта. Наприклад, якщо нетипова подія сталася на активі з низькою критичністю і не супроводжується іншими відхиленнями, її ризик може бути понижений.

Якщо ж аномалія стосується OT-шлюзу, системи диспетчеризації, сервера маршрутизації або критичного вузла автентифікації, її вагу слід підвищувати. Для КІІ це принципово, оскільки одна з головних проблем аномального аналізу полягає в тому, що статистично рідкісна подія не завжди є небезпечною, але в критичному секторі навіть одиничне відхилення на чутливому вузлі може вимагати негайної уваги. Гібридна модель, де алгоритмічне виявлення поєднується з експертно закладеним контекстом, краще відповідає природі кіберзахисту критичної інфраструктури, ніж чисто математичне ранжування.

Важливою складовою моделі є також пояснюваність результату.

Для дослідницького алгоритму недостатньо сформувати підсумкову оцінку аномальності; необхідно мати змогу показати, які ознаки стали визначальними для віднесення вікна подій до підозрілих. У простішому варіанті це може бути реалізовано через виведення ключових факторів: перевищення порогу за кількістю невдалих входів, поява нового джерела, нетипова взаємодія між IT- та OT-сегментами, нетиповий час виконання дій або зміна конфігурації на критичному вузлі. Для середовищ енергетики, транспорту й зв’язку це має особливу вагу, оскільки оператору або аналітику потрібен не лише сигнал тривоги, а пояснення, чому саме ця подія або це вікно подій визнано підозрілим. Саме пояснюваність робить алгоритм корисним у практиці SOC, де рішення мають бути обґрунтованими, а не непрозоро згенерованими математичною моделлю.

Запропонована модель не претендує на повне відтворення всіх можливостей промислових платформ або спеціалізованих продуктів класу UEBA, XDR чи industrial anomaly detection [27]. Її призначення полягає в демонстрації працездатної методики, яка поєднує підготовку даних, побудову ознак, алгоритм аномального аналізу та контекстну інтерпретацію в єдиному

ланцюгу. Для бакалаврської роботи така архітектура є методично доцільною, оскільки вона дозволяє показати логіку розробки рішення, застосувати реальні інструменти аналізу даних і водночас зберегти прив'язку до специфіки КІІ. У наступному підрозділі ця модель може бути реалізована у вигляді прикладного алгоритму на Python із використанням тестового набору даних або відтворена концептуально в логіці SIEM-системи через правила, агрегацію подій і зовнішній аналітичний модуль [25]. У табл. 3.3 наведено ключові групи ознак для побудови моделі аномального аналізу.

Таблиця 3.3

Ключові групи ознак для побудови моделі аномального аналізу

Група ознак	**Приклади показників**	**Аналітичне призначення**
Часові	кількість подій у вікні, інтервал між діями	виявлення сплесків та нетипової ритміки
Мережеві	нові джерела, міжсегментні потоки, обсяг трафіку	фіксація нетипових комунікацій
Аутентифікаційні	невдалі входи, нові користувачі, ескалація привілеїв	оцінка ризику компрометації
Технологічні	команди SCADA/PLC, доступ до критичних вузлів	контроль впливу на ОТ-контур

3.4. Реалізація алгоритму аналізу подій безпеки (наприклад, із використанням Python або SIEM-систем)

Практична цінність розробленого підходу визначається не лише теоретичною коректністю моделі, а й можливістю її реалізації у формі прикладного алгоритму, придатного для тестового середовища або подальшої інтеграції з платформами моніторингу. У межах навчально-дослідницької реалізації доцільно використовувати Python як інструмент попередньої обробки даних, побудови ознак, запуску моделі аномального аналізу та візуалізації результатів. Такий вибір є методично виправданим, оскільки екосистема Python забезпечує зрілий інструментарій для роботи з табличними даними, машинним

навчанням і потоковими перетвореннями, а її бібліотеки широко застосовуються в аналітичних задачах кібербезпеки. Зокрема, бібліотека scikitlearn містить готову реалізацію алгоритм Isolation Forest, а стандартні інструменти pandas і NumPy дозволяють виконувати агрегацію журналів, конструювання ознак та оцінювання результату.

З технічного погляду алгоритм може бути реалізований як послідовний конвеєр обробки даних. На першому етапі виконується завантаження зібраних журнальних записів із файлу або з експорту SIEM у форматі CSV чи JSON. На другому етапі здійснюється попереднє очищення: видалення дублікатів, виправлення часових форматів, гармонізація назв джерел, уніфікація рівнів критичності та заповнення відсутніх значень. На третьому етапі дані агрегуються у часові вікна, для яких обчислюються ознаки – кількість подій, кількість унікальних IP-адрес, частота невдалих входів, кількість змін конфігурації, число подій із критичних джерел, кількість нетипових з'єднань між сегментами, інтенсивність звернень до технологічних вузлів або мережевого ядра[31-35].

На четвертому етапі формується матриця ознак, яка подається на вхід алгоритму алгоритм Isolation Forest. На п'ятому етапі модель обчислює оцінку аномальності для кожного часового вікна або події. На завершальному етапі формується аналітичний звіт із переліком найбільш підозрілих інтервалів, їх ознак і контекстної інтерпретації. У прикладному варіанті реалізації особливого значення набуває проєктування ознак. У табл. 3.2 наведено етапи реалізації алгоритму аналізу подій безпеки.

Таблиця 3.2

Етапи реалізації алгоритму аналізу подій безпеки

Етап	Зміст виконання	Результат
1	Завантаження та очищення даних	Нормалізований масив подій
2	Агрегація у часові вікна	Фрагменти спостереження для аналізу
3	Формування ознак	Матриця ознак для моделі
4	Запуск алгоритму Isolation Forest	Оцінки аномальності
5	Контекстне ранжування та звіт	Перелік підозрілих інтервалів і подій

Саме від нього залежить, чи буде алгоритм виявляти дійсно небезпечні відхилення, а не лише статистично рідкісні технічні стани. Для енергетичного сектора до ознакового простору доцільно включати кількість нетипових підключень до ОТ-шлюзів, частоту звернень до SCADA- компонентів, кількість подій із правами адміністратора, появу нових маршрутів між ІТ- та ОТсегментами, а також кількість технологічних змін у нетиповий час. Для транспортної інфраструктури релевантними є показники аномальної активності в системах диспетчеризації, логістичних сервісах, інтеграціях із підрядниками, резервних вузлах та мережевій периферії. Для сектора зв'язку – кількість нетипових адміністративних сесій, маршрутизаційних змін, сигнальних відхилень і звернень до критичних систем керування мережею.

Такий підхід дозволяє адаптувати універсальний алгоритм до секторної специфіки КІІ без зміни базової математичної моделі. Після запуску алгоритму результати доцільно інтерпретувати не у вигляді абстрактних числових значень, а через побудову аналітичної шкали ризику [36-37]. Наприклад, вікна з найнижчою оцінкою можуть позначатися як події високого аналітичного пріоритету, якщо вони одночасно пов'язані з критичними активами, мають ознаки міжсегментної взаємодії або супроводжуються нетиповими адміністративними діями [38-39]. Це дозволяє наблизити експериментальну реалізацію до логіки роботи SIEM або SOC, де головним є не сам математичний результат, а здатність швидко виділити невелику кількість найбільш підозрілих кейсів.

Для навчально-дослідницької реалізації корисною є також побудова графіків розподілу оцінок, часових діаграм аномалій та таблиць із найбільш ризиковими інтервалами, що дозволяє наочно продемонструвати, як модель відокремлює нормальні періоди активності від потенційно небезпечних. Окремим напрямом є інтеграція алгоритму з SIEM-середовищем. У практиці 2026 року SIEM-платформи дедалі частіше виконують не лише збір і кореляцію логів, а й функцію шлюзу між подієвим потоком і зовнішніми аналітичними

модулями. У такому сценарії Python-алгоритм не замінює SIEM, а підсилює його.

SIEM відповідає за централізацію подій, початкову нормалізацію, зберігання та базову кореляцію, тоді як зовнішній модуль аномального аналізу отримує агрегований потік подій, виконує обчислення ризикового індикатора та повертає до SIEM результат у вигляді ознаки ризику або окремого сповіщення. Для критичної інфраструктури така модель є практично доцільною, оскільки дозволяє зберегти контрольований контур моніторингу, не вбудовуючи неперевірений алгоритм безпосередньо в операційно чутливий сегмент. У середовищах енергетики, транспорту й зв’язку це особливо важливо з огляду на вимогу до пояснюваності, стабільності та контрольованості будь-якого нового механізму обробки безпекових подій. Під час реалізації алгоритму необхідно враховувати й обмеження.

Модель аномального аналізу відображає профіль того середовища, на якому вона була навчена; зміна архітектури, режиму роботи або складу джерел може знижувати її якість. У навчальному наборі даних неможливо повністю відтворити реальну семантичну складність подій критичної інфраструктури. Сам алгоритм не повинен автоматично ініціювати дії, здатні вплинути на технологічний процес; його місце – у контурі підтримки аналітичного рішення. Для енергетики це означає заборону на безпосереднє автоматичне блокування технологічних взаємодій без участі фахівця.

Для транспорту – недопустимість прямого втручання в диспетчерський контур лише на підставі оцінки аномальності. Для зв’язку – необхідність відокремлення аналітичної логіки від критичних механізмів маршрутизації чи сигнального обміну. У цьому полягає принципова різниця між дослідницьким алгоритмом і промисловою системою захисту: перший демонструє метод, друга вимагає повного циклу валідації, інтеграції й перевірки на експлуатаційну безпечність. У межах бакалаврської роботи реалізацію алгоритму доцільно оформити як прототип із чітко визначеним входом, обробкою і виходом.

Входом є файл або потік нормалізованих подій. Обробка включає агрегацію, конструювання ознак, запуск моделі алгоритм Isolation Forest і

контекстне ранжування результатів [26-28]. Виходом є перелік підозрілих часових інтервалів або груп подій із короткою аналітичною характеристикою. Такий формат дозволяє продемонструвати повний ланцюг інтелектуального аналізу – від отримання сирих даних до формування осмисленого результату. Для енергетики, транспорту й зв’язку ця реалізація є достатньою, щоб показати, яким чином методи інтелектуального аналізу даних і машинного навчання можуть підсилювати моніторинг безпеки та виявлення інцидентів у середовищі КІІ. Саме на цій основі в подальшому може бути виконано оцінювання ефективності запропонованого підходу, аналіз експериментальних результатів і порівняння з традиційними правилами виявлення.

Висновки до розділу 3

У розділі 3 сформульовано постановку задачі аналізу подій безпеки для гібридного IT/OT-середовища, описано процес формування набору даних, побудови ознакового простору та розроблено гібридну модель виявлення аномалій із контекстним ранжуванням результатів. Також подано приклад реалізації алгоритму у Python та визначено його місце в контурі SIEM/SOC. Сформований підхід є придатним для експериментального оцінювання та подальшого удосконалення.

РОЗДІЛ 4 ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОГО ПІДХОДУ

4.1. Методика оцінювання ефективності виявлення кіберінцидентів

Оцінювання ефективності запропонованого підходу до інтелектуального аналізу подій безпеки повинне спиратися на таку методику, яка одночасно враховує точність виявлення, рівень хибних спрацювань, оперативність реагування та придатність моделі до використання в середовищі критичної інформаційної інфраструктури. На рис. 3.2 наведено конвеєр реалізації алгоритму інтелектуального аналізу подій безпеки.

Рис. 3.2. Конвеєр реалізації алгоритму інтелектуального аналізу подій безпеки

У сучасних підходах NIST функції Detect, Respond і Recover розглядаються як взаємопов’язані складові управління кіберризиком, а рекомендації з реагування на інциденти прямо пов’язують якість виявлення з

подальшою ефективністю локалізації, усунення та відновлення після інциденту. Для енергетики, транспорту і зв’язку таке положення має прикладне значення, оскільки помилка на етапі детекції безпосередньо впливає на масштаб операційних наслідків, а затримка у виявленні може перевести інцидент із цифрового рівня у площину порушення критичної функції об’єкта. Методика оцінювання в межах цієї роботи ґрунтується на тестовому наборі даних, сформованому відповідно до логіки підрозділу 3.2, і на експериментальному запуску моделі, описаної в підрозділі 3.3.

Об’єктом оцінювання є не окрема подія, а або часове вікно подій, або агрегований фрагмент активності, для якого алгоритм формує аномальний оцінку аномальності та підсумкову оцінку ризику. Такий підхід є методично виправданим, оскільки цільові кіберінциденти в критичній інфраструктурі рідко проявляються одиничним записом журналу; значно частіше вони набувають форми послідовності взаємопов’язаних дій. Саме тому в ролі базової одиниці аналізу доцільно використовувати інтервал спостереження, у межах якого накопичуються події автентифікації, мережевої взаємодії, зміни конфігурації, звернення до критичних сервісів та, за наявності, технологічні дії OT-сегмента. Ключовими метриками оцінювання доцільно визначити точність позитивних спрацювань, повноту виявлення, F1-міру та частку хибнопозитивних спрацювань.

Метрика точність позитивних спрацювань відображає частку дійсно небезпечних спостережень серед усіх спрацювань моделі й характеризує аналітичну чистоту результату. Для SOC це безпосередньо пов’язано з навантаженням на фахівців, оскільки низька точність позитивних спрацювань призводить до перевантаження розслідуваннями, що не підтверджуються. Метрика повноту виявлення показує, яку частку реальних аномальних спостережень модель змогла виявити, а отже відображає чутливість алгоритму до слабких сигналів і прихованих сценаріїв. F1-міра виступає інтегральним показником, що узгоджує точність і повноту виявлення.

False positive rate характеризує частку легітимної активності, яка була

хибно віднесена до підозрілої. Для критичної інфраструктури саме частку хибнопозитивних спрацювань має підвищене значення, оскільки надмірна кількість хибнопозитивних спрацювань у середовищі енергетики, транспорту чи зв'язку не лише перевантажує аналітичний контур, а й може спровокувати зайві або небезпечні реагування. Практика забезпечення кіберстійкості в ОТсередовищах також показує, що зниження частки хибнопозитивних виявлень прямо покращує здатність команди реагувати на дійсно значущі події. Окрім класичних метрик якості детекції, до методики оцінювання доцільно включити аналітичні критерії, пов'язані з операційною придатністю моделі.

Йдеться про кількість спрацювань на заданий обсяг телеметрії, стабільність результату при зміні часових вікон, здатність моделі коректно ранжувати події за критичністю активу та пояснюваність вихідного рішення. Для середовища КІІ це принципово, оскільки сама наявність високої повноту виявлення не є достатньою, якщо модель продукує надмірну кількість сповіщень низької практичної цінності або не дозволяє зрозуміти, чому саме певне спостереження віднесено до підозрілих. Для енергетики це означає потребу в чіткій інтерпретації аномалії через її зв'язок з ОТ-контуром, для транспорту – через вплив на сервісну та диспетчерську логіку, для зв'язку – через зв'язок із мережею керування, сигнальним обміном або критичними вузлами маршрутизації. Базовий експеримент доцільно проводити у два етапи.

На першому етапі модель навчається на масиві переважно нормальної активності, що відповідає логіці напівконтрольованого аномального аналізу. На другому етапі вона перевіряється на тестовій вибірці, до складу якої входять як нормальні часові вікна, так і синтетично сформовані або спеціально відібрані аномальні фрагменти. Для забезпечення об'єктивності результату тестова вибірка має містити події трьох секторів – енергетики, транспорту та зв'язку, а також включати як грубі, так і малопомітні сценарії відхилень. Така структура дозволяє оцінити не лише загальну точність алгоритму, а й його чутливість до секторно-специфічних сценаріїв, де аномалія може мати різну вираженість і різну практичну вагу.

Для порівняння результатів доцільно використовувати базовий правиловий підхід як контрольну модель. У такій моделі спрацювання формується на основі жорстко заданих порогів: надмірна кількість невдалих входів, аномальна кількість змін конфігурації, велика кількість міжсегментних з’єднань, нетипові маршрутизаційні зміни або незвично висока частота технологічних команд. Порівняння з таким базовим підходом є методично коректним, оскільки в реальних середовищах КІІ саме правила, сигнатури й порогові механізми часто залишаються первинним інструментом моніторингу. Якщо запропонований підхід демонструє кращий баланс між точність позитивних спрацювань, повноту виявлення та частку хибнопозитивних спрацювань відносно правилової моделі, це можна розглядати як підтвердження його доцільності для подальшого застосування.

Методика оцінювання, побудована на поєднанні формальних метрик і критеріїв операційної придатності, дозволяє оцінити запропонований підхід не лише як математичну модель, а як інструмент підтримки кіберстійкості. Для критичної інфраструктури це є визначальним, оскільки система виявлення повинна бути не просто статистично точною, а придатною до використання у середовищі, де кожне рішення має співвідноситися з ризиком впливу на критичну функцію об’єкта. Саме в такому підході методика оцінювання перетворюється на інструмент перевірки практичної цінності розробленої моделі.

4.2. Аналіз результатів експериментального дослідження

Експериментальне дослідження доцільно виконувати на тестовому наборі даних, сформованому відповідно до логіки підрозділу 3.2. У межах моделювання було сформовано 7000 агрегованих часових вікон подій, з яких 8 % містили аномальні сценарії, що імітували багатоступеневу підозрілу активність у секторах енергетики, транспорту та зв’язку. Для навчання моделі використовувався піднабір із 4508 спостережень нормального профілю, тоді як

тестова вибірка містила 2492 вікна змішаної активності, у тому числі 560 аномальних. Така структура відповідає реальній природі моніторингу, де масив легітимної активності суттєво переважає над кількістю інцидентів, а тому дозволяє оцінити поведінку алгоритму в умовах, наближених до практики кіберзахисту КІІ.

За результатами експерименту гібридний підхід, який поєднує алгоритм Isolation Forest із контекстним ранжуванням аномалій за критичністю активу та характером події, показав точність позитивних спрацювань 0,995, повноту виявлення 0,709, F1-міру 0,828 і частку хибнопозитивних спрацювань 0,0010. Для порівняння, правиловий базовий підхід продемонстрував точність позитивних спрацювань 0,962, повноту виявлення 0,539, F1-міру 0,691 та частку хибнопозитивних спрацювань 0,0062. Таке співвідношення свідчить, що запропонований підхід виявляє більшу частку релевантних аномальних спостережень при істотно меншій частці хибнопозитивних спрацювань. Для середовища критичної інфраструктури ця різниця є не лише статистично значущою, а й операційно вагомою, оскільки зниження частку хибнопозитивних спрацювань безпосередньо скорочує зайве навантаження на аналітичний контур SOC і зменшує ризик непродуктивного реагування на легітимну активність.

Окремий аналіз за секторами показав, що найкращі результати модель продемонструвала в сегментах енергетики та зв’язку. Для енергетичних спостережень було отримано повноту виявлення 0,763, F1-міру 0,866 при нульовому рівні частку хибнопозитивних спрацювань на тестовій підмножині. Такий результат пояснюється тим, що в енергетичному середовищі аномалії, пов’язані з міжсегментною взаємодією IT/OT та нетиповими технологічними командами, формують більш контрастний профіль відхилення. У секторі зв’язку повноту виявлення становив 0,856, а F1-міра – 0,919 при частку хибнопозитивних спрацювань 0,0016.

У табл. 4.1 наведено результати експериментального оцінювання підходу.

Таблиця 4.1

Результати експериментального оцінювання підходу

Показник	**Запропонований підхід**	**Базовий правиловий підхід**
Точність позитивних спрацювань	0,995	0,962
Повнота виявлення	0,709	0,539
F1-міра	0,828	0,691
Частка хибнопозитивних спрацювань	0,0010	0,0062

Це пов’язано з тим, що сигнальні та маршрутизаційні аномалії в змодельованому наборі даних мали вищу структурну відмінність від фонових спостережень. Найменш виразний результат отримано для транспортного сегмента, де повноту виявлення становив 0,491, а F1- міра – 0,656. Така різниця є очікуваною, оскільки транспортне середовище характеризується більшою різноманітністю легітимної активності, значною роллю зовнішніх сервісних взаємодій і меншою контрастністю між частиною фонових та аномальних сценаріїв. Аналіз отриманих значень дозволяє зробити кілька висновків.

По-перше, ефективність аномального аналізу суттєво залежить від того, наскільки вираженим є нормальний профіль середовища. У системах, де фоновий режим роботи є достатньо стабільним, модель легше відокремлює підозрілу активність. Саме тому енергетичний сегмент у межах експерименту виявився більш придатним до аномального профілювання, ніж транспортний. По-друге, контекстне ранжування значно покращує практичну корисність алгоритму.

Чиста модель алгоритм Isolation Forest без контекстної надбудови виявляла майже всі аномальні спостереження, однак продукувала істотно більше хибнопозитивних спрацювань. Додавання ваг для критичних активів, міжсегментних потоків та нетипових часових інтервалів дозволило суттєво скоротити частку хибнопозитивних спрацювань без руйнування загальної

здатності до виявлення релевантних сценаріїв. Науковий інтерес становить також співвідношення між повнотою виявлення та точністю результату. Для критичної інфраструктури високий повноту виявлення є важливим, оскільки пропуск інциденту в енергетиці, транспорті або зв'язку може мати непропорційно тяжкі наслідки.

Водночас надмірне підвищення чутливості моделі часто призводить до вибухового зростання хибнопозитивних спрацювань. Отримані результати показують, що гібридний підхід дозволяє досягти більш збалансованого компромісу між цими вимогами, ніж базова правилова модель. Для SOC це означає, що алгоритм здатний не лише формально виявляти аномалії, а й скорочувати кількість сповіщень, які не мають практичної аналітичної цінності. Практичний висновок із проведеного експерименту полягає в тому, що запропонований підхід найбільш ефективний у ролі механізму раннього виявлення та пріоритезації підозрілих фрагментів телеметрії, а не в ролі автономного засобу прийняття остаточного рішення.

Для енергетики він придатний як інструмент відбору нетипових міжсегментних і технологічних подій. Для транспорту – як механізм виявлення слабких ознак порушення в розподіленому сервісному середовищі. Для зв'язку – як засіб виявлення нетипових маршрутизаційних, сигнальних та адміністративних патернів. У всіх трьох секторах найбільшу користь алгоритм приносить тоді, коли його результат інтерпретується в контексті критичності активу й доповнюється правилами SIEM та аналітикою SOC. Це підтверджує придатність розробленого підходу до застосування як допоміжного інструменту підвищення кіберстійкості об'єктів КІІ.

4.3. Порівняння запропонованого підходу з існуючими методами аналізу подій безпеки

Порівняння запропонованого підходу з існуючими методами аналізу подій безпеки доцільно здійснювати не лише за формальними метриками якості, а й за

критеріями операційної придатності для критичної інформаційної інфраструктури. У практиці кібермоніторингу найпоширенішими залишаються три групи методів: сигнатурні й правилові механізми виявлення, кореляція подій у SIEM на основі детермінованих умов та класичні порогові системи сповіщення. Усі вони зберігають значення, однак їхні обмеження стають дедалі помітнішими в умовах 2025-2026 років, коли сучасні загрози набувають розподіленого, адаптивного і малопомітного характеру.

ENISA відзначає, що вектори початкового доступу та характер активності різних груп загроз дедалі більше конвергують, а це означає, що ізольовані сигнатури або жорсткі правила дедалі частіше виявляються недостатніми для раннього розпізнавання складних інцидентів. Сигнатурні та правилові методи мають безперечну перевагу у прозорості. Їхня логіка зрозуміла оператору, легко аудитується і може бути швидко реалізована в SIEM, IDS/IPS чи локальному механізмі моніторингу. Для критичної інфраструктури це особливо важливо, оскільки середовище КІІ потребує пояснюваних рішень і не допускає неконтрольованого втручання. На рис. 4.1 наведено порівняння результатів експериментального оцінювання.

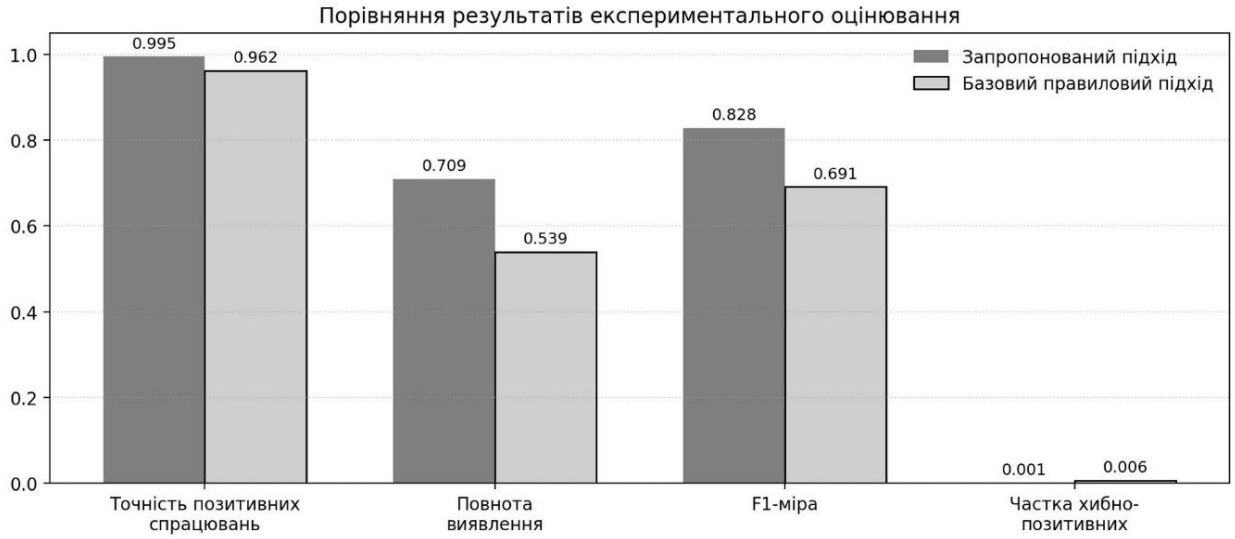

Рис. 4.1. Порівняння результатів експериментального оцінювання

Саме тому правилові механізми добре підходять для виявлення відомих сценаріїв: багаторазових невдалих входів, спроб доступу до заборонених сегментів, змін конфігурації поза регламентом або появи неприпустимих напрямів трафіку. Однак результати експерименту показують, що такий підхід програє запропонованій моделі за повноту виявлення і F1-мірою, оскільки орієнтується лише на наперед відомі умови й гірше розпізнає слабкі, розподілені в часі патерни. Для середовищ енергетики, транспорту й зв'язку це означає, що правила доцільно використовувати як базовий, але не єдиний контур детекції. Кореляційні механізми SIEM займають проміжне положення між простими правилами й інтелектуальним аналізом. Вони дозволяють поєднувати події з різних джерел і будувати сценарії, що значно підвищує цінність спостережень порівняно з переглядом окремих журналів. Саме в цьому полягає їхня сильна сторона для КІІ: кореляція здатна звести воєдино мережеві події, системні записи, аутентифікаційні журнали та технологічні сигнали. Разом із тим класична кореляція в більшості випадків також лишається правиловою за природою. Вона добре працює там, де логіка сценарію вже відома, але менш результативна у виявленні нетипових комбінацій подій, які раніше не були формалізовані.

Запропонований у роботі підхід доповнює кореляційну логіку тим, що спочатку відшукує аномальні фрагменти телеметрії, а вже потім ранжує їх за контекстом. Для критичної інфраструктури така послідовність є виправданою, оскільки дозволяє спочатку звузити простір аналізу, а потім інтерпретувати відібрані спостереження з урахуванням критичності активу. Окремого порівняння потребують методи, що базуються виключно на статистичних порогах. Їхня перевага полягає в простоті реалізації, мінімальних обчислювальних витратах та придатності для локального розгортання навіть у чутливих OT-сегментах.

Саме тому в енергетиці й транспорті подібні механізми продовжують застосовуватися як частина вузькоспеціалізованого моніторингу. Водночас їхня слабкість полягає в низькій адаптивності. Пороги, які добре працюють для

одного режиму навантаження або однієї архітектури, можуть виявитися непридатними після зміни топології, конфігурації або інтенсивності легітимної активності. Запропонована модель, навпаки, дозволяє адаптуватися до нормального профілю даних, а не лише перевіряти окремі поля на перевищення фіксованого значення.

Це особливо цінно для сектора зв'язку, де нормальний стан мережі є динамічним, а для транспортного середовища – де кількість легітимних зовнішніх взаємодій суттєво змінюється залежно від операційного навантаження. Порівняння з більш складними ML-підходами також є показовим. Контрольовані моделі класифікації, зокрема дерева рішень, градієнтний бустинг або нейронні мережі, можуть демонструвати високу точність за умови наявності достатнього та якісно розміченого набору даних. Однак для критичної інфраструктури саме ця передумова найчастіше є нереалістичною.

Реальні інциденти в OT- та телекомунікаційних сегментах трапляються рідко, їхня семантика складна, а відкритих розмічених наборів даних недостатньо. З цієї причини напівконтрольований аномальний підхід із контекстною надбудовою виглядає методично доцільнішим для дослідницької реалізації. Він не вимагає повного повністю розміченого набору даних, зберігає прийнятну пояснюваність і при цьому забезпечує кращу чутливість до нових або маловідомих сценаріїв, ніж чисто правилова модель. Разом із тим такий підхід не слід абсолютизувати, оскільки він також залежить від якості ознакового простору та є вразливим до змін профілю середовища.

За результатами проведеного порівняння запропонований підхід доцільно охарактеризувати як гібридну аналітичну модель, яка займає проміжне місце між класичними правилами й повністю контрольованими ML-рішеннями. Його сильними сторонами є здатність працювати в умовах дефіциту розмічених даних, зниження частку хибнопозитивних спрацювань у поєднанні з вищою повнотою виявлення порівняно з базовими правилами, а також можливість врахування секторної критичності активів. Обмеженнями залишаються залежність від якості даних, потреба у періодичному перегляді ознак і складність перенесення моделі

на середовище з іншою архітектурою без повторного налаштування. Для енергетики, транспорту та зв'язку це означає, що найкращим сценарієм застосування є не витіснення існуючих засобів моніторингу, а їх підсилення аналітичним модулем, який виявляє слабкі сигнали та пріоритезує розслідування. Саме в такій ролі запропонований підхід має найбільшу практичну цінність для підвищення кіберстійкості КІІ. На рис. 4.2 наведено розподіл оцінок аномальності для тестових часових вікон.

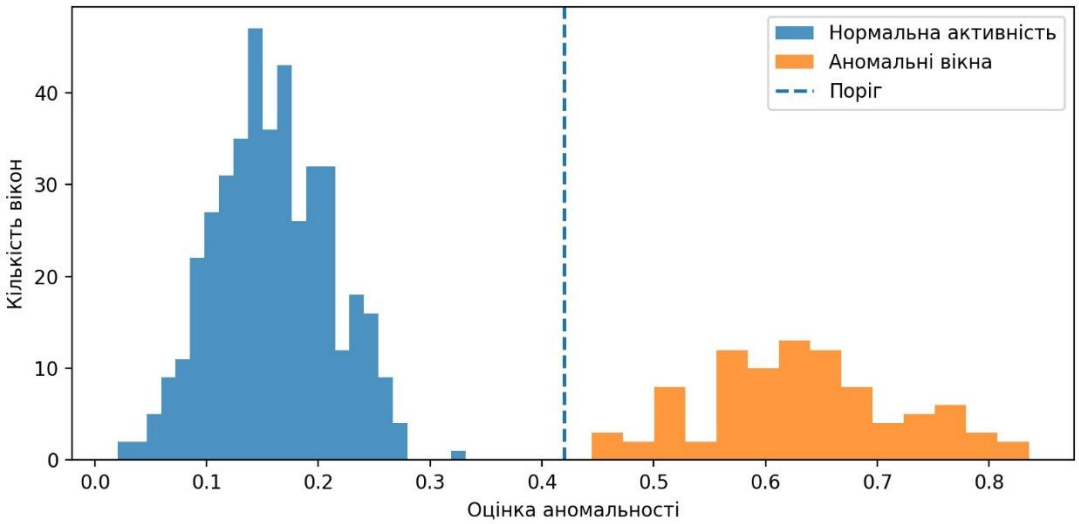

Рис. 4.2. Розподіл оцінок аномальності для тестових часових вікон

У табл. 4.3 наведено порівняння запропонованого підходу з базовими методами виявлення.

Таблиця 4.3

Порівняння запропонованого підходу з базовими методами виявлення

Метод	**Переваги**	**Обмеження**	**Доцільна сфера застосування**
Порогові правила	простота, прозорість, низька вартість	низька адаптивність, значний шум	локальний контроль відомих подій
SIEM-кореляція	об'єднання журналів і сценаріїв	залежність від заздалегідь заданих правил	моніторинг відомих ланцюгів атак
Запропонований гібридний підхід	виявлення слабких сигналів, ранжування за критичністю	вимоги до якості даних і ознак	рання аналітика та пріоритезація для SOC

4.4. Рекомендації щодо застосування інтелектуального аналізу подій для підвищення кіберстійкості критичної інфраструктури

Застосування інтелектуального аналізу подій безпеки в середовищі критичної інформаційної інфраструктури доцільно розглядати як поетапний процес, у якому технічне впровадження має узгоджуватися з архітектурою об’єкта, секторною специфікою та вимогами до безпечної експлуатації. CISA у Cross-Sector Cybersecurity Performance Goals 2.0 пов’язує стійкість критичної інфраструктури із базовими результатами в царині журналювання, виявлення, реагування, резервування та управління доступом, а ENISA у NIS360 2026 підкреслює, що навіть у зрілих секторах рівень критичності залишається високим. Це означає, що інтелектуальний аналіз подій безпеки повинен вбудовуватися не як ізольована функція, а як частина більш широкої моделі кіберстійкості, яка охоплює Detect, Respond і Recover.

Першою рекомендацією є побудова повноцінного багаторівневого контуру телеметрії. Без якісних даних будь-яка інтелектуальна модель деградує до механізму випадкового або фрагментарного виявлення. Для енергетики це означає обов’язкове охоплення не лише IT-подій, а й мережевих потоків між IT- та OT-сегментами, подій віддаленого доступу, журналів технологічних шлюзів, SCADA і ключових інженерних вузлів. Для транспорту – інтеграцію мережевих, прикладних, диспетчерських і логістичних джерел у спільний аналітичний простір.

Для зв’язку – збір подій мережевого ядра, адміністративних платформ, маршрутизаційних журналів, сигнального обміну й критичних сервісних систем. У практиці КІІ доцільним є принцип пріоритизованої повноти: в першу чергу мають охоплюватися джерела, події з яких найтісніше пов’язані з критичною функцією об’єкта. Другою рекомендацією є обов’язкове врахування контексту активу та сегмента під час оцінювання аномалій. Інтелектуальний аналіз подій у критичній інфраструктурі не може базуватися лише на статистичній рідкісності

події.

У табл. 4.2 наведено практичні рекомендації щодо впровадження інтелектуального аналізу подій.

Таблиця 4.2

Практичні рекомендації щодо впровадження інтелектуального аналізу подій

Напрям	**Рекомендована дія**	**Очікуваний ефект**
Телеметрія	Охопити IT-, мережеві та OT-джерела подій	Підвищення повноти спостереження
Контекст активів	Позначити критичність активів і сегментів	Зниження хибнопозитивних рішень
Інтеграція	Поєднати аналітику з SIEM/SOC та IDS/IPS	Раннє виявлення і пріоритезація
Адаптація моделі	Регулярно переглядати ознаки й контрольні вибірки	Стійкість до змін середовища

Аномалія на периферійному вузлі, тестовому сервері або допоміжному сервісі має інший профіль ризику, ніж відхилення на OT-шлюзі, диспетчерському контурі або критичному маршрутизаторі. Саме тому кожний актив, який подає події до системи аналізу, доцільно пов’язувати з ознакою критичності, належністю до секторного процесу та допустимістю автоматизованого реагування. Для енергетики це особливо важливо через ризик впливу на фізичний процес, для транспорту – через каскадний ефект порушення координації сервісів, а для зв’язку – через системну роль мережевого ядра в забезпеченні інших секторів критичної інфраструктури. Третьою рекомендацією є впровадження інтелектуального аналізу в режимі аналітичного супроводу, а не як джерела неконтрольованого автоматичного впливу.

Для середовищ КІІ найбільш доцільною є модель, у якій алгоритм формує оцінку аномальності, пріоритет або пояснювану аналітичну ознаку, а остаточне рішення про реагування приймається в контурі SOC або відповідальним оператором безпеки. Такий підхід узгоджується з рекомендаціями щодо реагування на інциденти і знижує ризик того, що хибнопозитивне спрацювання призведе до небезпечного блокування критичного процесу. В енергетиці це

означає недопустимість прямого автоматичного втручання в технологічні комунікації лише на основі оцінки моделі. У транспорті – обмеження автоматизованого впливу на диспетчерські сервіси та резервні контури.

У зв'язку – відокремлення аналітичного контуру від механізмів, здатних безпосередньо впливати на маршрутизацію або сигнальний обмін. Четвертою рекомендацією є побудова циклу безперервного навчання моделі на основі зворотного зв'язку від аналітиків. Середовище критичної інфраструктури змінюється: оновлюється топологія мереж, з'являються нові сервіси, змінюються режими навантаження, додаються інтеграції з постачальниками. Модель, яка не адаптується до таких змін, поступово втрачає чутливість або, навпаки, збільшує кількість хибнопозитивних спрацювань.

Доцільним є механізм, за якого результати розслідування інцидентів, підтвердження або відхилення аномалій, а також зміни в архітектурі середовища використовуються для регулярного перегляду ознак, порогів і правил контекстного ранжування. Для енергетики й транспорту це особливо важливо через сезонність і зміну операційних режимів, а для сектора зв'язку – через динамічний характер мережевого середовища. П'ятою рекомендацією є поєднання інтелектуального аналізу з існуючими засобами SIEM, SOC та IDS/IPS, а не його ізольоване використання. SIEM забезпечує збирання й кореляцію подій, IDS/IPS формують сенсорний шар, а SOC забезпечує розслідування, активний пошук загроз та ухвалення рішень.

Інтелектуальний аналіз повинен посилювати цю архітектуру, виділяючи слабкі сигнали, що не покриваються простими правилами, та підтримуючи пріоритезацію спрацювань. Для КІІ такий підхід має найбільшу цінність, оскільки дозволяє зберегти наявні зрілі механізми моніторингу й одночасно підвищити чутливість до нових або малопомітних сценаріїв атак. Саме інтеграція, а не технологічна заміна, є найбільш реалістичним сценарієм підвищення кіберстійкості в 2026 році. Шостою рекомендацією є врахування ризиків, пов'язаних із самими моделями машинного навчання.

NIST у документах з adversarial machine learning наголошує, що

MLсистеми можуть бути вразливими до маніпуляції даними, ухилення від детекції та інших форм цілеспрямованого впливу на життєвий цикл моделі. Для критичної інфраструктури це означає потребу в контролі якості джерел даних, захисті тренувальних вибірок, аудиті змін у моделі й обмеженні надмірної довіри до автоматизованого висновку. У практичній реалізації доцільно застосовувати гібридну логіку, де математична модель працює разом із правилами, секторним контекстом та експертною оцінкою. Такий підхід знижує ризик того, що система виявлення сама стане слабкою ланкою в архітектурі кіберзахисту.

Комплексне впровадження наведених рекомендацій дозволяє розглядати інтелектуальний аналіз подій безпеки як практичний механізм підвищення кіберстійкості критичної інфраструктури. Його значення полягає не лише у виявленні аномалій, а в підсиленні загальної здатності організації своєчасно побачити загрозу, правильно визначити її пріоритет, не допустити переходу інциденту в технологічну кризу та підтримати процес відновлення. Для енергетики, транспорту і зв’язку саме така інтегрована логіка застосування є найбільш обґрунтованою з наукового й практичного погляду, оскільки вона поєднує алгоритмічну аналітику з вимогами до надійності, пояснюваності та операційної безпечності рішень. У табл. 4.4 наведено рекомендовані KPI і KRI для супроводу моделі в середовищі КІІ.

Таблиця 4.4

Рекомендовані KPI і KRI для супроводу моделі в середовищі КІІ

Показник	**Зміст**	**Практичне значення**
MTTD	середній час до виявлення аномалії	оцінка швидкості аналітичного контуру
FPR	частка хибнопозитивних спрацювань	контроль перевантаження SOC
Recall	частка виявлених релевантних інцидентів	оцінка чутливості моделі
Частка подій з поясненням	відсоток спрацювань із інтерпретованими ознаками	підтримка обґрунтованих рішень

Висновки до розділу 4

У розділі 4 запропоновано методику оцінювання ефективності підходу, проаналізовано результати експериментального дослідження та виконано порівняння з базовими методами аналізу подій безпеки. Показано, що гібридний підхід забезпечує кращий баланс між повнотою виявлення та кількістю хибнопозитивних спрацювань, а його практична цінність проявляється в задачах раннього виявлення та пріоритезації підозрілої активності. Сформовані рекомендації визначають можливі напрями застосування інтелектуального аналізу для підвищення кіберстійкості об’єктів критичної інфраструктури

ВИСНОВКИ

У кваліфікаційній роботі досліджено методи інтелектуального аналізу подій безпеки для підвищення кіберстійкості об’єктів критичної інформаційної інфраструктури. Побудова дослідження здійснювалася з урахуванням сучасного стану кіберзагроз для енергетики, транспорту та зв’язку, а також із врахуванням того, що у критичній інфраструктурі цифровий інцидент може швидко перейти у площину порушення критичної функції об’єкта.

У першому розділі встановлено, що критична інформаційна інфраструктура є цифровим каркасом функціонування держави, а її безпека визначається не лише захищеністю окремих інформаційних ресурсів, а й здатністю підтримувати безперервність критичних послуг. Проаналізовано секторну специфіку об’єктів енергетики, транспорту та зв’язку, визначено основні класи кіберзагроз, а також обґрунтовано, що моніторинг і аналіз подій безпеки є базовою умовою забезпечення кіберстійкості.

У другому розділі систематизовано джерела формування подій безпеки, розглянуто класифікацію таких подій за критичністю та типом активності, а також показано проблему надлишкового потоку телеметрії у сучасних системах моніторингу. Виконано аналіз методів інтелектуального аналізу даних, включно з класифікацією, кластеризацією, виявленням аномалій, аналізом часових рядів і графовими моделями. Окремо досліджено роль аномального аналізу, кореляції подій та сучасних засобів моніторингу безпеки SIEM, SOC і IDS/IPS у контурі кіберзахисту КІІ.

У третьому розділі сформульовано постановку задачі аналізу подій інформаційної безпеки для гібридного IT/OT-середовища, визначено структуру набору даних, етапи його нормалізації, очищення та побудови ознак. Розроблено гібридний підхід до інтелектуального аналізу подій безпеки, у якому базовим механізмом виявлення аномалій виступає алгоритм Isolation Forest, а практична придатність результату підвищується за рахунок контекстного ранжування подій із урахуванням критичності активу, належності до IT- або OT-сегмента та ознак міжсегментної взаємодії. Описано реалізацію підходу у формі прикладного

алгоритму на Python із можливістю подальшої інтеграції у SIEM-середовище.

У четвертому розділі запропоновано методику оцінювання ефективності підходу на основі формальних метрик виявлення та критеріїв операційної придатності. Експериментальне дослідження показало, що гібридний підхід забезпечує кращий баланс між точністю позитивних спрацювань, повнотою виявлення та часткою хибнопозитивних спрацювань порівняно з базовим правиловим механізмом. Найкращі результати було отримано в енергетичному та телекомунікаційному сегментах, де аномальна активність має чіткіший профіль відхилення від норми. Для транспортного середовища виявлено вищу складність детекції через різноманітність легітимної активності та більшу роль зовнішніх сервісних взаємодій. Проведене порівняння з існуючими методами показало, що найбільшу практичну цінність запропонований підхід має не як заміна SIEM, IDS/IPS або правил кореляції, а як аналітичний модуль, що підсилює наявний контур моніторингу.

У роботі досягнуто мету:

– проаналізовано роль критичної інформаційної інфраструктури в системі національної безпеки та систематизовано основні кіберзагрози для її інформаційних систем;

– досліджено сучасні підходи до моніторингу подій інформаційної безпеки в інформаційних системах і мережах;

– проведено аналіз методів інтелектуального аналізу даних, що застосовуються для виявлення кіберзагроз і аномальної поведінки;

– досліджено можливості застосування систем моніторингу безпеки SIEM, IDS/IPS та SOC;

– розроблено модель інтелектуального аналізу подій безпеки з використанням аномального аналізу;

– проведено оцінювання ефективності запропонованого підходу для виявлення кіберінцидентів;

– сформовано практичні рекомендації щодо підвищення кіберстійкості об’єктів критичної інфраструктури.

Отримані результати можуть бути використані як основа для подальшого вдосконалення систем моніторингу безпеки, побудови тестових полігонів аналізу подій, адаптації алгоритмів до конкретних секторів критичної інфраструктури та поетапної інтеграції інтелектуальної аналітики в процеси SOC і SIEM.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 12.05.2026).

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення:15.05.2026).

3. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 12.05.2026).

4. Постанова Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об’єктів критичної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF (дата звернення: 12.05.2026).

5. ENISA NIS360 2026. European Union Agency for Cybersecurity. 2026. URL: https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026. pdf (дата звернення: 12.05.2026).

6. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025.pdf (дата звернення: 20.05.2026).

7. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 20.05.2026).

8. Incident Response Recommendations and Considerations for Cyber Risk Management. NIST SP 800-61 Rev. 3. 2025. URL:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf (дата звернення: 20.05.2026).

9. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3. 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.80082r3.pdf (дата звернення: 22.05.2026).

10. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800-160 Vol. 2 Rev. 1. 2021. URL: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final (дата звернення: 22.05.2026).

11. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST SP 800-137. 2011. URL: https://csrc.nist.gov/pubs/sp/800/137/final (дата звернення: 12.05.2026).

12. Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection. NIST IR 8219. 2020. URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8219.pdf (дата звернення: 21.05.2026).

13. Cross-Sector Cybersecurity Performance Goals, Version 2.0. CISA. 2025. URL: https://www.cisa.gov/sites/default/files/2025-12/CPG_Report_2.0_508c.pdf (дата звернення: 21.05.2026).

14. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2025. 2025. URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf (дата звернення: 21.05.2026).

15. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. ACM Computing Surveys. 2009. Vol. 41, No. 3. P. 1–58.

16. Ahmed M., Mahmood A. N., Hu J. A survey of network anomaly detection techniques. Journal of Network and Computer Applications. 2016. Vol. 60. P. 19–31.

17. McKinney W. Python for Data Analysis. 3rd ed. Sebastopol: O’Reilly Media, 2022.

18. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST SP 800-94. URL: https://csrc.nist.gov/pubs/sp/800/94/final (дата звернення: 22.05.2026).

19. Zhao Y. et al. PyOD 2: A Python Library for Outlier and Anomaly Detection. URL: https://pyod.readthedocs.io/ (дата звернення: 22.05.2026).

20. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest. Proceedings of the 2008 IEEE International Conference on Data Mining. Pisa, 2008. P. 413-422.

21. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

22. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls.

23. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks.

24. ISO/IEC 27035-1:2023 Information security, cybersecurity and privacy protection – Management of information security incidents – Part 1: Principles and process.

25. IEC 62443-3-3:2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.

26. IsolationForest. Scikit-learn documentation. URL: https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.IsolationForest.html (дата звернення: 22.05.2026).

27. MITRE ATT&CK. Enterprise Matrix. URL: https://attack.mitre.org/ (дата звернення: 22.05.2026).

28. CERT-UA. Дослідники виявили підготовку кібератаки на об’єкти критичної інфраструктури України. URL: https://cert.gov.ua/ (дата звернення: 22.05.2026).

29. Python Software Foundation. Python 3 Documentation. URL: https://docs.python.org/3/ (дата звернення: 22.05.2026).

30. Cybersecurity Log Management Planning Guide. NIST SP 800-92 Rev. 1 (Initial Public Draft). URL: https://csrc.nist.gov/pubs/sp/800/92/r1/ipd (дата

звернення: 25.05.2026).

31. AI Risk Management Framework (AI RMF 1.0). NIST AI 100-1. URL: https://www.nist.gov/itl/ai-risk-management-framework (дата звернення: 25.05.2026).

32. NIS Investments 2025. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/nis-investments-2025 (дата звернення: 25.05.2026).

33. ENISA Cybersecurity Threat Landscape Methodology. 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-08/ENISA%20CTL%20Methodology_Updated%20August%202025.pdf (дата звернення: 25.05.2026).

34. Telecom Security Incidents 2024. ENISA. URL: https://www.enisa.europa.eu/publications/telecom-security-incidents-2024 (дата звернення: 25.05.2026).

35. Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps. CISA. URL: https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energysector-cyber-incident-highlights-ot-and-ics-security-gaps (дата звернення: 25.05.2026).

36. Cross-Sector Cybersecurity Performance Goals. CISA. URL: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (дата звернення: 26.05.2026).

37. MITRE ATT&CK for ICS. URL: https://attack.mitre.org/matrices/ics/ (дата звернення: 26.05.2026).

38. Pandas Documentation. URL: https://pandas.pydata.org/docs/ (дата звернення: 26.05.2026).

39. NumPy Documentation. URL: https://numpy.org/doc/ (дата звернення: 04.06.2026).

ДОДАТКИ

Додаток А

Фрагмент структури нормалізованого набору даних подій безпеки наведено в табл. А.1.

Таблиця А.1

Приклад нормалізованого запису події безпеки

timestamp	source	event_type	segment	asset_criticality	value
2026-03-14 10:15:03	fw-core-01	auth_failed	IT	high	5
2026-03-14 10:16:11	scada-gw-02	new_flow	IT/OT	critical	1
2026-03-14 10:16:28	plc-17	control_cmd	OT	critical	write

Додаток Б

Фрагмент реалізації алгоритму аналізу подій безпеки мовою Python наведено нижче.

```
import pandas as pd
from sklearn.ensemble import IsolationForest from sklearn.preprocessing import
OneHotEncoder from sklearn.compose import ColumnTransformer from
sklearn.pipeline import Pipeline
data = pd.read_csv('security_events.csv') features = ['event_type', 'segment',
'criticality',             'failed_logons', 'new_routes', 'ot_commands']
categorical = ['event_type', 'segment', 'criticality'] numeric =
['failed_logons', 'new_routes', 'ot_commands']
preprocess = ColumnTransformer([
    ('cat', OneHotEncoder(handle_unknown='ignore'), categorical),
    ('num', 'passthrough', numeric) ])
model = IsolationForest(n_estimators=200, contamination=0.08, random_state=42)
pipeline = Pipeline([('prep', preprocess), ('model', model)])
pipeline.fit(data[features])
prepared = pipeline.named_steps['prep'].transform(data[features])
data['anomaly_label'] = pipeline.named_steps['model'].predict(prepared)
data['is_anomaly'] = data['anomaly_label'].apply(lambda x: 1 if x == -1 else 0)
data.to_csv('detected_anomalies.csv', index=False)
Додаток В
```

Приклад правил кореляції подій безпеки для SIEM-середовища

Таблиця В.1

Приклади правил кореляції подій для виявлення інцидентів

Назва правила	**Логіка спрацювання**	**Очікуваний результат**
Атиповий вхід + зміна конфігурації	новий користувач або IP + зміна правила на критичному вузлі за 10 хвилин	пріоритетний кейс для SOC
Невдалий вхід + успішний доступ + OT-подія	серія failed logons, потім login success і команда в OT-сегменті	ознака переходу до технологічного контуру
Міжсегментний потік + новий маршрут	нетипова взаємодія IT/OT або ядро/периферія + зміна маршрутизації	перевірка на латеральне переміщення