Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Панька Романа Вікторовича

на здобуття ступеня вищої освіти Бакалавра

Система виявлення вторгнень на основі індикаторів компроментації.

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.220121.22.01.12 ПЗ

Виконав студент 4 курсу група КБ-22-1 Роман ПАНЬКО
Керівник канд. техн. наук, доцент Ігор МУЛЯР
Нормоконтролер д-р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

03 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій
Кафедра Кібербезпеки
Рівень вищої освіти Бакалавр
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
9 січня 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Паньку Роману Вікторовичу

1 Тема роботи Система виявлення вторгнень на основі індикаторів компроментації.

Керівник роботи к.т.н. доцент Ігор Муляр
Затверджено наказом ректора університету від 8 січня 2026 р. № 7
2 Строк подання студентом кваліфікаційної роботи на кафедру 27 травня 2026р.
3 Вихідні дані до роботи Проаналізувати стан сучасних систем виявлення вторгнень та методів використання індикаторів компрометації, на основі чого буде сформульовано постановку задачі та функціональні вимоги до системи. У межах роботи планується розробка архітектури системи для збору і аналізу мережевих даних, обґрунтування вибору технологічного стеку та протоколів обміну інформацією про загрози, а також реалізація модулів для збору телеметрії та автоматизованої обробки подій безпеки.
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз загрози та предметної області. Огляд існуючих систем виявлення вторгнень та джерел індикаторів компрометації. Постановка задачі. Визначення функціональних вимог до системи. Проєктування архітектури та структури системи. Обґрунтування вибору технологій та протоколів обробки даних. Розробка модулів збору телеметрії та інтеграції з threat intelligence. Розробка серверної частини додатку для аналізу інцидентів. Розробка клієнтської частини вебінтерфейсу. Тестування функціональності та ефективності системи. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Логічна архітектура IDS
Модель кореляції Threat Intelligence
Діаграма послідовності

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 12 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент _____ Роман ПАНЬКО

Керівник кваліфікаційної роботи _____ Ігор МУЛЯР

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система виявлення вторгнень на основі індикаторів компроментації.

Автор роботи: Панько Роман Вікторович.

Керівник роботи: канд. техн. наук, доцент Муляр Ігор Володимирович.

Пояснювальна записка: 73 с., 1 додаток, 14 рисунків, 7 таблиць, 54 джерел.

Графічна частина: 3 плакати.

Ключові слова: wazuh, yara, кіберзагроза, критична інфраструктура, мережевий моніторинг, система виявлення вторгнень, індикатор компрометації.

У кваліфікаційній роботі розглянуто питання забезпечення кібербезпеки об'єктів енергетичної інфраструктури України шляхом розробки системи виявлення вторгнень на основі індикаторів компрометації. Проведено аналіз сучасних кіберзагроз, досліджено принципи роботи IDS та IPS систем, а також можливості використання платформ MISP і Wazuh.

У практичній частині розроблено архітектуру системи, реалізовано модулі збору та аналізу індикаторів компрометації, створено правила YARA і Sigma та проведено тестування системи на змодельованих сценаріях атак. Отримані результати підтвердили ефективність запропонованого рішення.

Практична цінність роботи полягає у можливості використання розробленої системи для моніторингу безпеки інформаційних систем енергетичних підприємств та центрів реагування на кіберінциденти.

25.05.2026

ANNOTATION

Theme of qualification work: Intrusion Detection System Based on Indicators of Compromise.

Author of the work: Panko Roman Viktorovych

Mentor: Ph.D. Muliar Ihor Volodymyrovych

Explanatory note: 73 pages, 1 appendix, 14 figures, 7 tables, 54 links.

Graphic part: 3 posters.

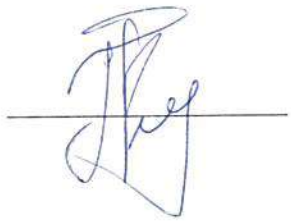
Keywords: wazuh, yara, cyber threat, critical infrastructure, network monitoring, intrusion detection system, indicator of compromise.

The qualification work addresses the issue of ensuring the cybersecurity of Ukraine's energy infrastructure facilities through the development of an intrusion detection system based on indicators of compromise. An analysis of modern cyber threats was carried out, the operating principles of IDS and IPS systems were studied, as well as the capabilities of the MISP and Wazuh platforms.

In the practical part, the system architecture was developed, modules for collecting and analyzing indicators of compromise were implemented, YARA and Sigma rules were created, and the system was tested using simulated attack scenarios. The obtained results confirmed the effectiveness of the proposed solution.

The practical value of the work lies in the possibility of using the developed system for security monitoring of information systems of energy enterprises and cyber incident response centers.

25.05.2026



ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

APT – Advanced Persistent Threat

ATT&CK – Adversarial Tactics Techniques and Common Knowledge

CSIRT – Computer Security Incident Response Team

DMZ – Demilitarized Zone

DNP3 – Distributed Network Protocol 3

EDR – Endpoint Detection and Response

ENISA – European Union Agency for Cybersecurity

FPR – False Positive Rate

ICS – Industrial Control System

IDS – Intrusion Detection System

IEC – International Electrotechnical Commission

IoC – Indicator of Compromise

IPS – Intrusion Prevention System

IT – Information Technology

MCC – Matthews Correlation Coefficient

MISP – Malware Information Sharing Platform

MTTD – Mean Time to Detect

NIS2 – Network and Information Security Directive 2

OpenIOC – Open Indicators of Compromise

OT – Operational Technology

SIEM – Security Information and Event Management

SOC – Security Operations Center

TAXII – Trusted Automated Exchange of Intelligence Information

TLP – Traffic Light Protocol

TTP – Tactics Techniques and Procedures

UEBA – User and Entity Behavior Analytics

ВСТУП

Енергетичний сектор України є одним із головних об’єктів сучасних кібератак. Особливо гостро проблема проявилася після атак на українські енергетичні компанії у 2015 та 2016 роках, коли зловмисники змогли порушити роботу енергосистем і спричинити масштабні відключення електроенергії. Після початку повномасштабної війни кількість атак на об’єкти критичної інфраструктури суттєво зросла. Для проведення атак використовуються шкідливі програми, фішингові кампанії, засоби віддаленого доступу та інструменти впливу на промислові системи керування.

За інформацією CERT-UA, протягом останніх років в Україні було зафіксовано значну кількість кіберінцидентів, частина яких спрямована саме проти енергетичної галузі [1]. Подібна ситуація спостерігається і на міжнародному рівні. Сучасні дослідження у сфері кібербезпеки підтверджують постійне зростання кількості атак на промислові та енергетичні системи [2, 3].

Традиційні засоби захисту вже не забезпечують достатній рівень безпеки для критичної інфраструктури [4]. Сучасні атаки є багаторівневими та можуть тривалий час залишатися непоміченими. У зв’язку з цим важливого значення набувають системи виявлення вторгнень, які дозволяють аналізувати мережеву активність, журнали подій та виявляти ознаки шкідливої діяльності.

Одним із найбільш ефективних підходів до виявлення кіберзагроз є використання індикаторів компрометації. До них належать IP адреси, доменні імена, хеші файлів, сигнатури шкідливого програмного забезпечення та інші ознаки, що можуть свідчити про присутність загрози в системі. Такі індикатори активно використовуються у системах моніторингу безпеки та засобах аналізу кіберзагроз.

Разом із цим у вітчизняному енергетичному секторі існують проблеми, пов’язані з використанням індикаторів компрометації. Основними серед них є відсутність єдиного підходу до обробки даних про загрози, складність інтеграції промислових мереж із системами моніторингу та велика кількість хибних

спрацювань. Також недостатньо практичних рішень, адаптованих до українських умов і потреб енергетичних підприємств.

У нормативних документах України та Європейського Союзу визначається необхідність впровадження систем моніторингу безпеки та засобів реагування на кіберінциденти для об’єктів критичної інфраструктури [5]. Тому розробка системи виявлення вторгнень на основі індикаторів компрометації є актуальним завданням для підвищення рівня кібербезпеки енергетичного сектору України.

Метою роботи є підвищення ефективності виявлення кіберзагроз в інформаційних системах енергетичного сектору шляхом розробки системи виявлення вторгнень на основі індикаторів компрометації та її практичного тестування.

Для досягнення поставленої мети необхідно виконати аналіз сучасних кіберзагроз для енергетичних систем, дослідити принципи роботи систем IDS та IPS, розглянути сучасні формати обміну даними про кіберзагрози, проаналізувати взаємозв’язок індикаторів компрометації з моделями MITRE ATT&CK та Cyber Kill Chain, розробити архітектуру системи виявлення вторгнень, реалізувати модулі збору та аналізу індикаторів компрометації, створити правила виявлення шкідливого програмного забезпечення та провести тестування системи на змодельованих сценаріях атак.

Об’єктом дослідження є процес забезпечення кібербезпеки інформаційних систем об’єктів енергетичної інфраструктури.Предметом дослідження є методи та програмні засоби виявлення вторгнень на основі індикаторів компрометації.

Практичне значення одержаних результатів полягає у розробці прототипу системи виявлення вторгнень на базі платформ MISP та Wazuh. Розроблена система забезпечує автоматизований збір, обробку та аналіз індикаторів компрометації, а також виявлення підозрілої активності в інформаційних системах. Проведене тестування підтвердило ефективність запропонованого рішення для виявлення атак на об’єкти енергетичного сектору. Отримані результати можуть бути використані центрами моніторингу безпеки, командами реагування на інциденти та операторами критичної інфраструктури.

1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ

1.1 Сучасний стан кіберзагроз та роль систем виявлення вторгнень у забезпеченні кібербезпеки інформаційно-комунікаційних систем

Поєднання корпоративних IT систем та оперативно-технологічних OT середовищ суттєво збільшило кількість можливих точок для кібератак на сучасні підприємства. У звіті Verizon DBIR 2024, який охоплює 30 458 інцидентів і 10 626 витоків даних у 94 країнах, зазначено, що кількість атак через використання відомих вразливостей збільшилась на 180 %. Також у 68 % випадків причиною інцидентів став людський фактор. Найчастіше це були фішингові атаки або компрометація облікових записів [6].

Середня вартість одного витоку даних досягла 4,88 млн доларів США. Найбільших фінансових втрат зазнають медичні установи, фінансовий сектор, а також промислові та енергетичні підприємства [7].

Особливо складною є ситуація у сфері критичної енергетичної інфраструктури. Енергетичні системи країн Європейського Союзу постійно перебувають під загрозою з боку проурядових кіберугруповань. Значна частина інцидентів пов’язана з APT атаками, програмами-вимагачами та компрометацією ланцюгів постачання. Фахівці також фіксують активність спеціалізованих угруповань, які орієнтуються саме на промислові системи керування. Серед них ELECTRUM, KAMACITE, XENOTIME та CHERNOVITE. Зазначено, що середній час прихованого перебування зловмисників у мережах енергетичних компаній становить 18 днів. Це приблизно вдвічі більше, ніж у звичайному комерційному секторі [8].

Україна стала одним із найяскравіших прикладів розвитку таких загроз. У грудні 2015 року відбулася атака BlackEnergy 3 на енергетичні компанії «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго». Внаслідок атаки було відключено 30 підстанцій, а без електропостачання залишилися близько 225 тисяч споживачів. Відновлення роботи систем тривало понад шість

годин. Цей інцидент став першою офіційно підтвердженою кібератакою у світі, яка спричинила масштабне відключення електроенергії [9]. У грудні 2016 року було зафіксовано ще одну атаку на підстанцію «Північна» НЕК «Укренерго». Для неї використовувалось шкідливе програмне забезпечення. Воно підтримувало промислові протоколи [10]. Після початку повномасштабної війни 24 лютого 2022 року інтенсивність кібератак значно зросла. У перші тижні було виявлено шкідливі програми. Вони знищували головні завантажувальні записи робочих станцій та надсилали команди для відключення вимикачів на електропідстанціях. Окремо була здійснена атака на супутникову мережу із застосуванням шкідливого ПЗ AcidRain [11]. У квітні 2022 року угруповання, яке також відоме як Sandworm, атакувало регіональну енергетичну компанію із використанням легітимних системних інструментів [12]. Протягом 2022–2024 років CERT-UA оприлюднила понад 4 тисячі повідомлень про кіберінциденти. Близько 22 % із них були спрямовані проти енергетичної критичної інфраструктури. У цей період також з’явилися нові сімейства шкідливого програмного забезпечення. Серед них PIPEDREAM або INCONTROLLER, COSMICENERGY та FrostyGoop.

Найпоширенішими способами проникнення залишаються фішингові листи, експлуатація вразливостей сервісів віддаленого доступу, атаки через ланцюги постачання, інсайдерські дії та використання довірених каналів зв’язку. Також активно застосовуються безфайлові атаки через PowerShell та спеціалізоване шкідливе програмне забезпечення.

Традиційний підхід до захисту, який базується лише на міжмережевому екрані, антивірусі та резервному копіюванні, уже не забезпечує належного рівня безпеки. Сучасні атаки часто маскуються під легітимну діяльність користувачів або систем. Крім того, сучасна інфраструктура є розподіленою та гібридною, а промислові сегменти мають обмеження щодо оновлення програмного забезпечення та засобів захисту.

У зв’язку з цим набули поширення концепції глибокоешелонованого захисту, нульової довіри та постійного моніторингу мережі. Одним із ключових

елементів таких підходів є система виявлення вторгнень IDS. Вона являє собою програмно-апаратний комплекс, який автоматично аналізує мережевий трафік, журнали подій та поведінку процесів.

У документі NIST SP 800-94 IDS визначено як обов'язковий компонент сучасної системи інформаційної безпеки [13]. Необхідність використання таких систем також регламентується стандартами ISO/IEC 27002:2022 [14] та ISA/IEC 62443-3-3 [15]. У рекомендаціях NIST SP 800-82 Rev 3 IDS розглядається як невід'ємний елемент захисту критичної інфраструктури [16].

На енергетичних підприємствах IDS виконують кілька важливих функцій. Вони дозволяють швидше виявляти атаки та скорочувати час їхнього виявлення. Такі системи накопичують журнали подій для проведення цифрової криміналістики та допомагають виявляти ознаки діяльності зловмисників на ранніх етапах. Для сегментів ICS фахівці рекомендують використовувати пасивні IDS системи. Вони не втручаються у промисловий трафік та не створюють додаткового навантаження на пристрої [17].

Сучасні IDS системи поступово переходять від класичного сигнатурного підходу до гібридних методів аналізу. У них поєднуються сигнатури та правила YARA і Sigma, поведінковий аналіз із застосуванням машинного навчання, інтеграція з платформами та використання матриць. Також активно впроваджується автоматизоване реагування за принципом SOAR. Саме на основі цих підходів формується новий клас систем виявлення вторгнень, що працюють із використанням індикаторів компрометації IoC.

1.2 Класифікація, архітектура та принципи функціонування систем виявлення і запобігання вторгненням (IDS/IPS)

Системи виявлення вторгнень сформувалися як окремий клас засобів інформаційної безпеки наприкінці 1980-х років. IDS являє собою програмний або програмно-апаратний засіб, який автоматично контролює події в мережі чи

комп’ютерній системі для виявлення порушень безпеки. Якщо система не лише фіксує підозрілу активність, а й автоматично її блокує, вона належить до класу IPS.

Системи IDS та IPS поділяються за кількома основними ознаками. Однією з них є об’єкт моніторингу. Мережеві IDS аналізують мережевий трафік і контролюють передавання пакетів даних. Хостові IDS встановлюються безпосередньо на сервер або робочу станцію та перевіряють журнали операційної системи, файлову систему, реєстр і системні процеси.

Існують також спеціалізовані системи для промислових мереж, бездротових технологій та окремих застосунків. На енергетичних підприємствах зазвичай використовують комбінований підхід. Мережеві IDS розміщують на межі між корпоративною та технологічною мережею. Хостові системи встановлюють на сервери SCADA та автоматизовані робочі місця диспетчерів. Окремі промислові IDS застосовують для контролю трафіку промислових протоколів [18].

Ще однією ознакою класифікації є спосіб виявлення атак. Сигнатурний метод працює на основі відомих шаблонів атак і забезпечує високу точність для вже відомих загроз. Його недоліком є неможливість виявлення нових або невідомих атак. Поведінковий метод аналізує аномалії в роботі системи та дозволяє знаходити невідомі загрози, але може давати хибні спрацювання. Найпоширенішими сьогодні є гібридні системи, які поєднують обидва підходи. У сфері енергетики вони часто додатково використовують технології машинного навчання.

Системи також відрізняються способом реагування на загрози. Пасивні IDS лише фіксують події та повідомляють адміністратора про небезпеку. Активні IPS можуть автоматично блокувати IP адреси, розривати мережеві з’єднання або ізолювати окремі сегменти мережі. У промислових системах частіше використовують пасивний режим роботи, оскільки автоматичне блокування трафіку може призвести до порушення роботи технологічних процесів або аварійних ситуацій.

За архітектурою розгортання системи поділяються на централізовані,

розподілені, агентно-серверні та хмарні. На українських об’єктах критичної інфраструктури найчастіше застосовують агентно-серверні рішення з локальним розгортанням, оскільки вони дозволяють централізовано контролювати події безпеки та зберігати дані всередині організації.

Окремим сучасним критерієм класифікації є ступінь інтеграції системи із зовнішніми джерелами кіберрозвідки. Традиційні ізольовані системи спираються переважно на статичні локальні бази правил, які швидко втрачають свою актуальність у динамічному середовищі загроз. Натомість новітній клас рішень функціонує як системи, керовані розвідданими (intelligence-driven). Вони здатні в режимі реального часу синхронізувати індикатори компрометації із національними та міжнародними платформами.

З погляду логічної архітектури сучасна IDS/IPS складається з шести взаємопов'язаних компонентів. Структуру наведено в таблиці 1.1. Логічну архітектуру системи виявлення вторгнень представлено на рисунку 1.1.

Таблиця 1.1 – Логічна архітектура сучасної системи виявлення вторгнень

Компонент	Призначення	Типові реалізації для енергосектору
Датчик (sensor)	Перехоплення подій безпеки на спостережуваному об'єкті	Snort/Suricata sensor, Wazuh agent, Zeek (Bro), Nozomi Guardian
Колектор (collector)	Прийом, попередня нормалізація і буферизація подій	Logstash, Filebeat, Vector
Аналізатор (analyzer)	Застосування правил/моделей виявлення, кореляція подій	Wazuh manager, Elastic Security, Sigma engine
База знань (signature/rule base)	Зберігання сигнатур, поведінкових моделей, IoC	YARA rules, Sigma rules, MISP feeds
Менеджер тривог (alert manager)	Пріоритизація, дедуплікація і доставлення повідомлень	TheHive, Alertmanager, Slack/Email gateway
Інтерфейс оператора (console)	Візуалізація, керування інцидентами	Kibana, Grafana, Wazuh Dashboard

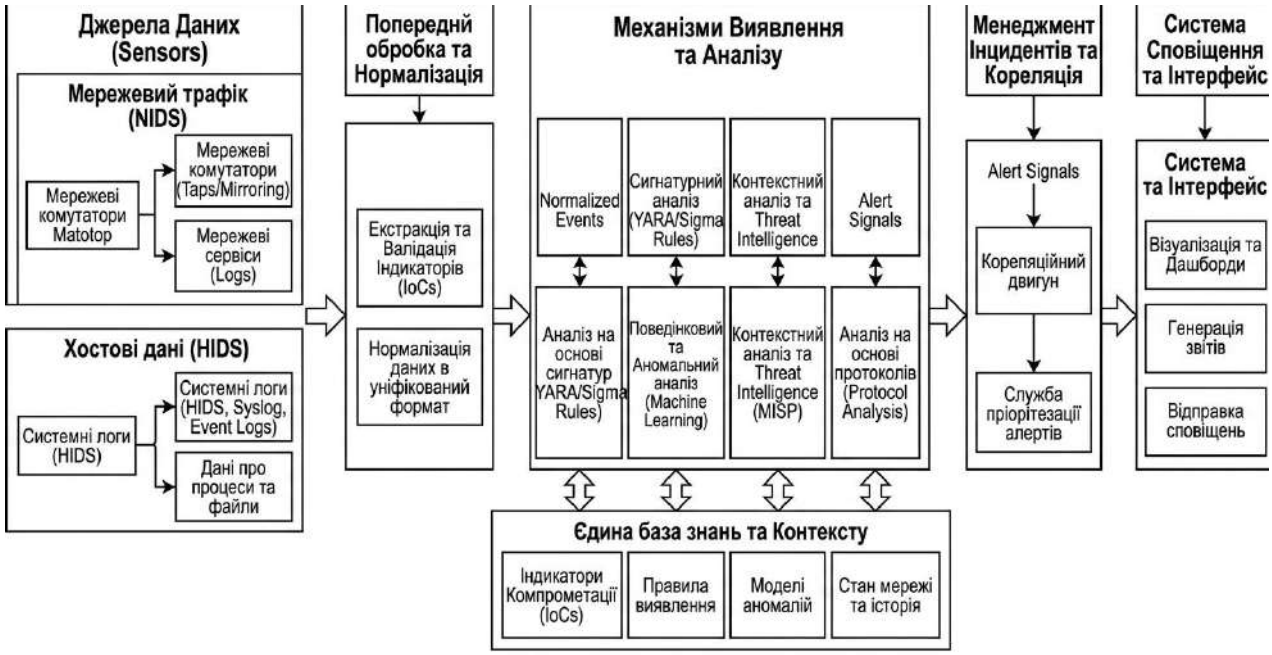


Рисунок 1.1 – Логічна архітектура IDS

Принцип роботи систем IDS та IPS базується на послідовному циклі обробки подій безпеки. Спочатку система збирає дані з мережі або кінцевих пристроїв. Далі виконується попередня обробка інформації та її аналіз. Після цього система визначає рівень загрози, приймає рішення щодо подальших дій і формує реакцію на інцидент. Завершальним етапом є аудит та збереження журналів подій. Така модель описана у стандарті ISO/IEC 18043:2006. Її адаптацію для українських умов розглядали у своїх наукових роботах описували багато дослідників [19].

У сучасних IT та OT середовищах IDS повинна підтримувати глибокий аналіз промислового трафіку. Для цього застосовується технологія DPI, яка дозволяє аналізувати вміст пакетів промислових протоколів.

Дослідження показують, що звичайні мережеві IDS мають низьку ефективність у промислових мережах. Вони здатні виявляти лише приблизно 12 % атак на промислові протоколи. Спеціалізовані системи для ICS середовищ демонструють значно кращі результати та можуть виявляти понад 80 % таких атак [20].

У сучасній архітектурі інформаційної безпеки IDS уже не розглядається як окремий ізольований засіб захисту. Вона виступає одним із джерел подій для SIEM систем, які виконують централізований аналіз інцидентів безпеки.

Обґрунтовується необхідність модульного підходу. Згідно з ним IDS повинна підтримувати передавання подій до будь-якої SIEM системи через стандартизовані канали обміну даними [21].

Класичні IDS системи мають низку обмежень. Сигнатурний аналіз не завжди дозволяє виявляти поліморфне або зашифроване шкідливе програмне забезпечення. Крім цього, без підключення до зовнішніх джерел бази сигнатур швидко втрачають актуальність. Наприклад, хеші шкідливих файлів можуть залишатися актуальними лише кілька годин або тижнів, а IP адреси зловмисників змінюються протягом днів або місяців [22]. Ще одним недоліком класичних IDS є недостатня інформативність щодо етапу розвитку атаки. Система може повідомити про підозрілу активність, але не пояснює, на якому етапі дій перебуває зловмисник. Для розв’язання цієї проблеми використовують прив’язку правил виявлення до тактик і технік, що дозволяє точніше визначати поведінку атакуючої сторони та етапи реалізації атаки.

1.3 Сутність, класифікація індикаторів компрометації та модель «Піраміди болю» Девіда Б'янко

Поняття індикаторів компрометації або IoC почало активно використовуватися наприкінці 2000-х років завдяки дослідженням фахівців. Одним із перших системний підхід до опису цифрових слідів зловмисників запропонував Дж. Вільямс. Він також визначив основні принципи обміну такими даними між організаціями [23]. У подальшому концепція IoC отримала розвиток у роботах SANS, MITRE, FIRST та ENISA. В Україні ця тематика досліджується у фахових виданнях з інформаційної безпеки та кіберзахисту [24].

Головною відмінністю IoC від звичайної антивірусної сигнатури є наявність додаткового контексту. Індикатори компрометації містять не лише ознаку загрози, а й супровідну інформацію. Це може бути час виявлення, джерело отримання даних, рівень довіри, зв’язок із конкретною тактикою атаки

або рівень поширення інформації за моделлю TLP.

За технічною природою IoC поділяються на кілька основних груп. До першої групи належать атомарні індикатори. Це окремі неподільні артефакти, наприклад IP адреси, доменні імена, URL посилання, електронні адреси або ідентифікатори процесів. Друга група охоплює обчислювальні індикатори. Вони формуються на основі аналізу даних. До них належать криптографічні хеші, нечіткі хеші, регулярні вирази та статистичні сигнатури мережевого трафіку. Третю групу становлять поведінкові індикатори. Вони описують дії або послідовність дій зловмисника в системі. Це можуть бути ланцюги системних викликів, використання легітимних системних інструментів або характерні тактики й техніки певних кіберугруповань [25].

За призначенням індикатори компрометації поділяються на реактивні, превентивні та контекстні. Реактивні IoC формуються після інциденту під час проведення цифрової криміналістики. Превентивні індикатори поширюються заздалегідь через системи для попередження можливих атак. Контекстні IoC містять додаткову інформацію про кампанії, кіберугруповання або геополітичні обставини атаки.

Для України особливо важливими є превентивні та контекстні індикатори, які поширюються CERT-UA, міжнародними командами реагування на інциденти та аналітиками промислової кібербезпеки [26].

Однією з найвідоміших класифікацій індикаторів компрометації стала модель «Піраміда болю», яку у 2013 році запропонував Девід Б’янко [27]. Основна ідея цієї моделі полягає у визначенні того, наскільки складно зловмиснику змінити певний тип індикаторів після їх виявлення. Чим вище розташований рівень у піраміді, тим більших ресурсів та зусиль потребує адаптація атаки. Відповідно, найефективнішими для захисту вважаються ті механізми виявлення, які орієнтуються на верхні рівні піраміди.

Модель складається із шести рівнів, які розташовані за принципом зростання складності для атакуючої сторони. Графічне зображення цієї моделі наведене на рисунку 1.2.

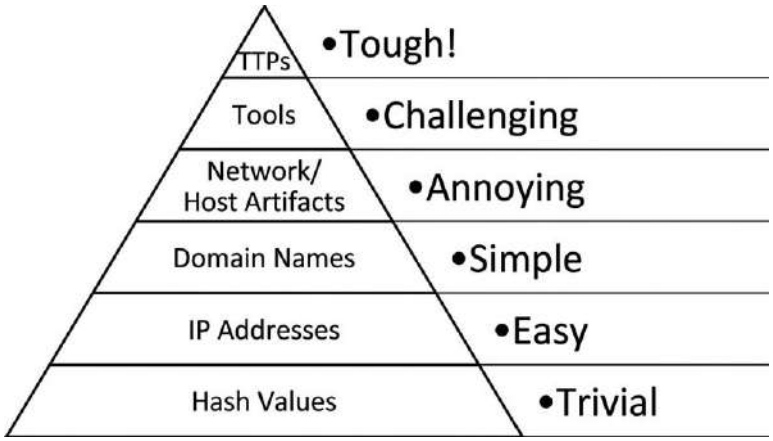


Рисунок 1.2 – Піраміда болю Девіда Б'янко

Найнижчий рівень піраміди становлять хеш значення файлів. Вони належать до найпростішого типу індикаторів, оскільки можуть бути змінені зловмисником без значних зусиль. За даними дослідження, термін корисності хешів є дуже обмеженим. Для масових атак він зазвичай становить близько 24 годин, а для цільових кампаній може досягати 7–10 днів.

Наступний рівень охоплює IP адреси. Вони використовуються для ідентифікації серверів керування, джерел сканування та фішингових ресурсів. Такі індикатори також мають короткий життєвий цикл, який зазвичай триває від кількох днів до кількох тижнів.

Далі йдуть доменні імена. Вони складніші для заміни, оскільки пов’язані з процесом реєстрації, періодом активності та налаштуванням захисних механізмів, зокрема TLS сертифікатів. Особливу небезпеку становлять домени, створені за принципом схожості до легітимних ресурсів, особливо у нетипових доменних зонах.

Наступний рівень включає мережеві та хостові артефакти. Це можуть бути імена процесів, шляхи встановлення програм, ключі реєстру, унікальні рядки в HTTP запитах, послідовності DNS запитів або об’єкти. Такі індикатори складніше змінити, оскільки вони пов’язані з поведінкою шкідливого програмного забезпечення в системі.

Ще вищий рівень становлять інструменти атак. Це можуть бути як відомі фреймворки для тестування безпеки, так і реальні інструменти зловмисників, а

також кастомне шкідливе програмне забезпечення. Виявлення таких інструментів за допомогою правил аналізу змушує атакуючу сторону змінювати весь інструментарій, що значно ускладнює атаку.

Найвищий і найскладніший рівень становлять тактики, техніки та процедури зловмисників. Це узагальнені моделі поведінки, наприклад послідовність дій від фішингового листа, подальшого бокового переміщення і завершення ексфільтрацією даних. Виявлення таких моделей є найбільш складним для атакуючої сторони.

Зазначається, що сучасні системи IDS повинні забезпечувати повне покриття всіх рівнів «Піраміди болю» [28]. Для енергетичного сектору особливо важливо зосереджуватися на верхніх рівнях моделі. Це дозволяє виявляти складні послідовності атак, пов’язані з промисловими протоколами, а також характерні сценарії використання системних утиліт, які часто застосовуються для бокового переміщення в корпоративних мережах обленерго [29].

Дослідження на основі аналізу SIEM систем у фінансовому секторі України показало, що більшість простих індикаторів швидко втрачають актуальність. Близько 60 % атомарних IoC стають неактуальними вже протягом 14 днів. Ще 25 % втрачають цінність протягом 90 днів. Лише невелика частина індикаторів, приблизно 4 %, відноситься до рівня стійких тактик і технік, які залишаються корисними понад рік [30]. Зведені характеристики рівнів піраміди подано в таблиці 1.2.

Таблиця 1.2 – Зведена характеристика рівнів піраміди болю Девіда Б'янко

Рівень піраміди (знизу догори)	Тип індикатора компрометації	Типовий приклад	Орієнтовний термін корисного життя	Ефект (вартість) для зловмисника
1	2	3	4	5
1. Hash Values – Trivial	Криптографічні хеші файлів (MD5, SHA-1, SHA-256)	SHA-256 виконуваного файла	24 години для масових кампаній; 7–10 діб	Достатньо змінити один байт у файлі – хеш змінюється

Продовження таблиці 1.2

1	2	3	4	5
2. IP Addresses – Easy	IPv4/IPv6-адреси командно-контрольних серверів (C2), джерел сканування або фішингу	95.214.27.108 (C2 Industroyer2); адреса bulletproof-хостингу	Від кількох діб до кількох тижнів	Низький: оренда нового VPS у bulletproof-хостингу або перенаправлення сесій ботнету через хмарного провайдера за хвилини
3. Domain Names – Simple	Доменні імена C2-інфраструктури, фішингових ресурсів, підставних оновлювачів	typosquatting-домени у TLD-зонах .top, .by; підставні CMS-домени	Від кількох тижнів до кількох місяців	Помірний: реєстрація нового домену, період «прогріву», отримання TLS-сертифікатів – у середньому 1–2 робочі дні
4. Network/Host Artifacts – Annoying	Унікальні рядки User-Agent, mutex-об'єкти, ключі реєстру, шляхи інсталяції, послідовності DNS-запитів, специфічні параметри URL	Mutex `Global\Industroyer_v2_lock`; ключ реєстру `HKLM\Software\Sandworm\Persist`; нестандартний User-Agent	Місяці	Помітний: вимагає повторної компіляції шкідливого ПЗ, перенастройки конфігурації, тестування на нові сигнатури – дні тижня роботи команди
5. Tools – Challenging	Інструменти атаки: фреймворки (Cobalt Strike, Metasploit, Sliver), кастомне шкідливе ПЗ	YARA-правила, що ловлять Cobalt Strike Beacon, Mimikatz, Industroyer-модулі за характерними рядками і структурою PE	6–12 місяців	Високий: повна заміна інструменту, що використовувався APT-групою інвестиція місяців роботи команди

Кінець таблиці 1.2

1	2	3	4	5
6. TTPs – Tough!	Тактики, техніки, процедури зловмисника – повторювані патерни поведінки і модус операнді кіберугруповання	Послідовність «фішинг → виконання Cobalt Strike Beacon → бокове переміщення через PsExec → ексфільтрація через rclone у хмарне сховище»	Понад 1 рік	Максимальний: вимагає переучування персоналу APT-групи, перебудови інфраструктури, повторного відлагодження ланцюжка атаки

Класифікація IoC та ієрархія за рівнем «болю» визначають типи правил виявлення. Однак для ефективного обміну індикаторами між організаціями необхідні стандартизовані формати їх опису.

1.4 Стандарти і формати опису та обміну індикаторами компрометації

Обмін індикаторами компрометації між організаціями реалізується через стандартизовані формати представлення даних. Сучасний центр моніторингу безпеки повинен підтримувати одночасну роботу з кількома такими форматами, оскільки це забезпечує сумісність із різними джерелами кіберрозвідданих [31].

Одним із найпоширеніших стандартів є STIX. Поточна версія STIX 2.1 затверджена у 2021 році. Стандарт має графову структуру та описує різні об’єкти кіберзагроз, зокрема шкідливі програми, кіберзлочинців, кампанії атак, інструменти та вразливості [32]. Дані можуть містити формалізовані шаблони опису поведінки атак.

Разом зі STIX використовується протокол TAXII, який забезпечує автоматизований обмін такими даними. Версія TAXII 2.1 працює на основі вебархітектури та дозволяє передавати дані STIX через захищені HTTPS

з’єднання. Така зв’язка STIX і TAXII є фактичним стандартом для обміну кіберрозвідданими між організаціями [33].

Окреме місце займає мова YARA. Вона використовується для виявлення шкідливого програмного забезпечення на основі сигнатурного аналізу файлів і пам’яті. YARA спочатку застосовувалась для аналізу зразків шкідливого коду. Правило YARA складається з описової частини, набору шаблонів і логічної умови їх спрацювання. Для критичної інфраструктури України також створенні та описанні такі правила [34].

Ще одним важливим інструментом є Sigma. Це універсальна мова опису правил виявлення подій у журналах безпеки. Вона дозволяє створювати правила, які потім конвертуються під різні системи аналізу логів. Такий підхід робить Sigma незалежною від конкретного виробника SIEM системи [35].

Дослідження показують, що велика кількість правил Sigma дозволяє суттєво покрити техніки атак. Наприклад, набір із 200 правил може забезпечити виявлення значної частини технік для корпоративних середовищ, тоді як для промислових систем необхідно створювати окремі спеціалізовані правила [36].

Платформа MISP використовується для централізованого обміну індикаторами компрометації. Вона була створена бельгійським центром кібербезпеки і стала одним із ключових інструментів для CERT та CSIRT команд, включно з CERT-UA [37]. Система підтримує імпорт і експорт різних форматів даних. Основною одиницею даних у MISP є подія, яка містить атрибути, що описують індикатори, групи об’єктів, мітки класифікації та каталоги загроз. У наукових роботах описано практичний досвід впровадження MISP у систему реагування на кіберінциденти з інтеграцією до міжнародних спільнот [38].

Одним із ранніх форматів представлення індикаторів компрометації є OpenIOC. Формат базується на XML структурі та дозволяє описувати логічні зв’язки між індикаторами за допомогою операторів [39]. З появою сучасніших стандартів, таких як STIX, його використання значно скоротилося і сьогодні він застосовується переважно у застарілих системах [40]. Порівняльну

характеристику розглянутих форматів подано в таблиці 1.3.

Таблиця 1.3 – Порівняльна характеристика форматів опису та обміну індикаторами компрометації

Критерій	STIX 2.1	TAXII 2.1	YARA	Sigma	MISP	OpenIOC
1	2	3	4	5	6	7
Рік випуску чинної версії	2021	2021	2008 (перша версія), активно розвивається	2017 (перша версія), активно розвивається	2011 (перша версія), активно розвивається	2011
Організація-автор	OASIS Open (раніше MITRE для DHS США)	OASIS Open	Віктор Альварес (VirusTotal)	SigmaHQ Project (Флоріан Рот, Томас Патцке)	CIRCL Luxembourg	Mandiant (FireEye)
Тип нотації	JSON, графова модель	REST API над HTTPS, клієнт-серверна архітектура	Власна предметно-орієнтована мова, блоки `strings`, `condition`	YAML	База даних з атрибутами, об'єктами; REST API	XML, логічне дерево індикаторів з операторами
Стан розвитку (станом на 2024 р.)	Активний, де-факто стандарт галузі для опису розвідданих	Активний, де-факто стандарт транспорту	Активний, використовується аналітиками шкідливого ПЗ	Активний, швидко набирає поширення	Активний, домінує у європейських національних CSIRT і CERT-UA	Спадковий (legacy) – розвиток сповільнено після появи STIX 2.x
Основне призначення	Стандартизоване представлення розвідданих про кіберзагрози (індикатори, актори, кампанії, інструменти, TTP)	Транспортний протокол для машинного обміну STIX-документами	Сигнатурний пошук у файлах та областях пам'яті для виявлення шкідливого ПЗ	Опис правил виявлення підозрілих подій у журналах (SIEM, EDR)	Платформа повного циклу обміну розвідданими: збір, обробка, аналіз, розповсюдження	Опис індикаторів компрометації з логічними виразами (історичний формат)

Кінець Таблиці 1.3

1	2	3	4	5	6	7
Підтримка обміну	Повна – через TAXII, файли, REST API	Повна – колекції (Collections) і канали (Channels) з аутентифікацією	Обмежена – обмін у вигляді текстових файлів через GitHub-репозиторії і MISP	Через GitHub-репозиторії, автоматична конвертація у синтаксис конкретних SIEM	Повна – вбудований протокол MISP Synchronization + експорт у STIX, OpenIOC, CSV	Обмін XML-файлами вручну (legacy-канали)
Прив'язка до MITRE ATT&CK	Нативна – через об'єкт Attack Pattern і галактику mitre-attack	Опосередкована – передає STIX-контент із прив'язкою	Ручна – у полі meta (наприклад, mitre_attack = "T1485")	Нативна – через поле tags (наприклад, attack.t1059.001)	Нативна – через галактики mitre-attack-pattern, mitre-ics-attack-pattern, mitre-malware, mitre-tool	Відсутня (формат розроблено до появи MITRE ATT&CK)
Типові інструменти роботи	MISP, OpenCTI, ThreatConnect, Anomali ThreatStream, Recorded Future	TAXII-сервери у складі MISP, OpenCTI, FreeTAXII	YARA-сканер, VirusTotal, інтегратор wazuh-yara, антивірусні гейтвеї, Cuckoo Sandbox	Утиліти sigmac, sigma-cli, конвертація до Splunk, Elastic, Microsoft Sentinel, IBM QRadar, Wazuh	MISP-сервер, MISP REST API, Python-бібліотека pymisp, плагіни до Wazuh, Splunk, IBM QRadar	Mandiant Redline, MISP-імпорт legacy-фідів

Жоден із існуючих форматів обміну індикаторами компрометації не є універсальним і не покриває всі потреби кіберзахисту. Через це в запропонованій архітектурі використовується комбінований підхід із кількох взаємодоповнюючих рішень.

Динамічний рівень аналізу, який базується на подіях із журналів безпеки, реалізується через правила Sigma. Для їх автоматичної адаптації під різні системи використовується інструмент sigmac, який дозволяє конвертувати

правила у формати конкретних SIEM систем [41].

Таким чином, кожен рівень виконує окрему функцію. STIX, TAXII та MISP забезпечують обмін і структурування даних про загрози. YARA відповідає за аналіз файлів та статичне виявлення шкідливого коду. Sigma використовується для аналізу подій у журналах безпеки та виявлення поведінкових ознак атак.

В Україні прямої локальної адаптації стандартів STIX і TAXII не існує, однак нормативні документи визначають їх як рекомендовану основу для побудови національної системи обміну інформацією про кіберзагрози. Зокрема, у положенні щодо порядку обміну інформацією про кіберзагрози STIX 2.1 і TAXII 2.1 розглядаються як еталонна модель для взаємодії між CSIRT та іншими учасниками національної екосистеми кібербезпеки [42].

1.5 Зв'язок індикаторів компрометації з моделями

Індикатори компрометації набувають практичної цінності лише в межах концепції кіберрозвідки Threat Intelligence. Це систематичний процес збору, обробки, аналізу та поширення інформації про кіберзагрози [43]. На відміну від «сирих» індикаторів, кіберрозвідка завжди містить контекст. Вона відповідає на питання хто здійснює атаку, які її цілі, які інструменти використовуються та які заходи протидії доцільні.

Визначено чотири рівні кіберрозвідки [44]. Стратегічний рівень описує глобальні тенденції та мотивацію кіберугруповань. Операційний рівень охоплює конкретні кампанії та діяльність APT груп. Тактичний рівень фокусується на тактиках і техніках атак. Технічний рівень включає конкретні індикатори компрометації, як атомарні, так і поведінкові. Процес обробки розвідданих описується циклом Threat Intelligence Lifecycle, який включає етапи планування, збору даних, обробки, аналізу, поширення результатів і зворотного зв’язку.

Першою формалізованою моделлю опису кібератаки як послідовності

етапів стала Cyber Kill Chain [45]. Вона включає сім фаз атаки, як-от розвідка, підготовка шкідливого коду, доставка, експлуатація вразливості, встановлення доступу, керування через канал і виконання цільових дій. Хоча Cyber Kill Chain є корисною для пояснення логіки атак, вона має обмеження. Зокрема, вона є лінійною, не відображає повторювані дії та недостатньо точно описує сучасні атаки на промислові системи.

Ці недоліки частково усунуто у фреймворку MITRE ATT&CK, який розробляється з 2013 року. Його актуальна версія охоплює 14 тактичних категорій та сотні технік атак [46]. Окремо існує розширення для промислових систем ATT&CK for ICS, яке описує специфічні атаки на технологічні процеси і містить набір тактик та технік для ОТ середовищ [47].

Для українського енергетичного сектору особливо актуальними є техніки, пов’язані з порушенням роботи промислових систем, відмовою в обслуговуванні, несанкціонованими командами управління, знищенням даних та приховуванням стану системи. У дослідженнях проаналізовано відповідність реальних інцидентів технікам ATT&CK for ICS [48]. Підкреслюється необхідність адаптації цієї моделі до специфіки українських об’єктів енергетики та використовуваних SCADA систем [49].

Ключовим елементом сучасного аналізу кіберзагроз є поєднання трьох моделей: піраміди індикаторів компрометації, Cyber Kill Chain та MITRE ATT&CK. Запропоновано підхід, за яким різні типи індикаторів співвідносяться з етапами атаки [50]. Атомарні індикатори найчастіше пов’язані з етапами доставки та виконання, обчислювальні індикатори застосовуються для виявлення інструментів і шкідливих зразків, а поведінкові індикатори дозволяють виявляти складні багатокрокові сценарії атак і постексплуатаційну активність.

Така інтегрована модель дозволяє одночасно визначати тип індикатора, етап атаки та тактичну мету зловмисника. Графічне представлення цієї моделі наведено на рисунку 1.3.

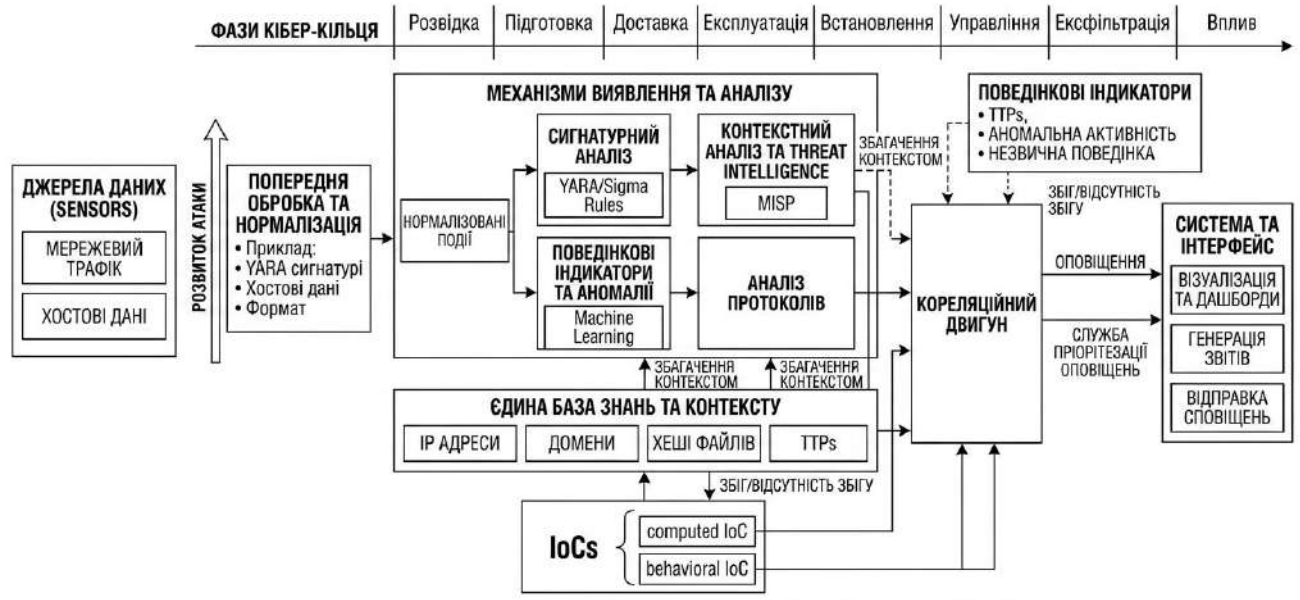


Рисунок 1.3 – Модель кореляції Threat Intelligence

Перехід атакувальника з корпоративного IT середовища до технологічного OT сегмента через демілітаризовану зону розглядається як ключовий етап гібридної кібератаки. На цьому етапі переміщення всередині корпоративної мережі поступово переходить у початкове проникнення до промислових систем керування [51].

Аналіз атак на українські енергетичні підприємства у період 2015–2024 років, дозволяє виділити найпоширеніші тактики та техніки зловмисників [52]. Додатково активно експлуатуються віддалені сервіси для переміщення всередині мережі, зокрема SMB протоколи. У зрілих атаках на промислові системи також фіксується використання специфічних технік для ICS середовищ, пов’язаних із порушенням керування технологічними процесами.

Для практичної реалізації захисту та моніторингу інфраструктури сучасні системи управління інформацією та подіями безпеки (SIEM), такі як Splunk Enterprise Security та платформа Wazuh, активно використовують базу знань MITRE ATT&CK [53, 54].

Запропонована у роботі архітектура узгоджується з цими підходами та може бути інтегрована з національними інформаційними системами кіберзахисту, зокрема з інформаційно-комунікаційною системою «Тризуб».

1.6 Постановка задачі

Сучасні кіберзагрози для енергетичної інфраструктури характеризуються високою складністю та системністю атак. У цих атаках застосовувалося спеціалізоване шкідливе програмне забезпечення для промислових систем. Це підтверджує недостатність класичних периметрових засобів захисту та необхідність використання систем безперервного моніторингу з інтеграцією Threat Intelligence та багаторівневих індикаторів компрометації.

Систематизовано підходи до класифікації IDS та IPS. Вони поділяються за типом моніторингу, способом виявлення, реакцією на інциденти та архітектурою розгортання. Окремо розглянуто концепцію індикаторів компрометації та їх класифікацію. Встановлено, що найбільшу практичну цінність для захисту енергетичних систем мають індикатори верхніх рівнів, пов’язані з інструментами та тактиками атак.

Проаналізовано основні стандарти та технології обміну індикаторами компрометації. Найбільш ефективною визначено комбінацію STIX, TAXII, MISP, YARA та Sigma у поєднанні з моделлю MITRE ATT&CK.

На основі проведеного аналізу сформульовано завдання дослідження як побудову системи виявлення вторгнень на основі IoC з визначеними показниками ефективності. Система повинна забезпечувати середній час виявлення не більше 6 хвилин та покриття не менше 80 % актуальних технік MITRE ATT&CK.

Для досягнення цієї мети та забезпечення заданих критеріїв ефективності в роботі передбачається вирішення низки взаємопов'язаних завдань. Зокрема, необхідно розробити структурно-логічну архітектуру інтеграції платформи обміну розвідданими з модулями виявлення вторгнень на рівні хостів та мережі. Обґрунтувати алгоритм фільтрації та пріоритезації індикаторів компрометації з метою зниження рівня хибних спрацювань і навантаження на аналітиків безпеки. Практична реалізація передбачає розгортання та налаштування програмного прототипу системи захисту на основі інтеграції відкритих інструментів.

2 АРХІТЕКТУРА СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ

2.1 Формалізована модель процесу виявлення вторгнень та життєвий цикл індикатора компрометації

Запропонована модель системи включає кілька взаємопов’язаних компонентів. Перший компонент становить множина джерел індикаторів. До них належать CERT-UA, національний MISP, AlienVault OTX, Abuse.ch ThreatFox, комерційні Threat Intelligence фіди та внутрішні дані SOC. Ці джерела забезпечують безперервне надходження інформації про кіберзагрози.

Другим компонентом є множина індикаторів компрометації. Кожен індикатор описується уніфікованою структурою, яка включає ідентифікатор STIX 2.1, тип індикатора, значення, джерело, часові мітки, рівень довіри, строк актуальності та прив’язку до технік MITRE ATT&CK, TLP рівня і кіберкампаній.

Третій компонент становить множина подій безпеки, що генеруються в інформаційно-комунікаційній системі. Події містять часові мітки, ідентифікатори вузлів, типи джерел журналів, а також структуровані дані.

Четвертим компонентом є множина технік MITRE ATT&CK, яка включає окремі підмножини для корпоративного середовища та промислових систем керування.

П’ятий компонент є основним і представляє собою конвеєр обробки даних, що складається з послідовних етапів. Спочатку виконується збір даних з різних джерел у визначеному часовому вікні. Далі відбувається валідація, під час якої відсіюються некоректні та службові записи. Наступним етапом є нормалізація даних до єдиної структури STIX 2.1. Після цього виконується збагачення інформації через зовнішні сервіси кіберрозвідки. Далі здійснюється кореляція подій із активними індикаторами компрометації. На етапі класифікації оцінюється ймовірність загрози за допомогою моделі машинного навчання на основі історичних даних. Завершальним етапом є ухвалення рішення, яке визначає факт інциденту, його пріоритет та відповідну техніку MITRE ATT&CK.

Шостий компонент визначає часові обмеження обробки. Кожна подія повинна бути опрацьована не більше ніж за 60 секунд, що формує вимогу до показника часу виявлення загрози.

Запропонована модель є повністю модульною та передбачає чітке розділення етапів обробки. Кожен етап реалізується як окремий програмний компонент із визначеним інтерфейсом. Графічну схему конвеєра обробки індикаторів компрометації наведено на рисунку 2.1.

Рисунок 2.1 – Конвеєр обробки індикаторів компрометації

Другий аспект моделі описує життєвий цикл індикатора компрометації як набір станів і правил переходів між ними. Усього виділено дев’ять основних станів та один термінальний стан відхилення.

Стан отриманий означає, що індикатор надійшов із джерела, але ще не пройшов обробку. Після первинної перевірки він переходить у стан валідований. Далі індикатор нормалізується до єдиного формату STIX 2.1 і отримує стан нормалізований. Наступним етапом є збагачення додатковим контекстом, після чого індикатор переходить у стан збагачений.

Після цього він може бути переведений у стан активний і використовується у правилах виявлення. У разі спрацювання правил індикатор отримує стан спрацьований, який фіксує факт виявлення і використовується для подальшого аналізу якості детекції.

Окремо виділяється стан старіє, який відображає поступове зниження актуальності індикатора. Далі індикатор переходить у стан застарілий, коли він більше не використовується в активному виявленні, але зберігається для аналітики. Після цього він може бути архівований. Термінальний стан відхилений застосовується до індикаторів, що не пройшли перевірку, зокрема дублікатів, приватних IP адрес і локальних доменів.

Більшість переходів у життєвому циклі є автоматичними. Винятком є перехід зі стану збагачений у стан активний для індикаторів рівня TLP:RED, який виконується лише після ручного підтвердження старшим аналітиком SOC. Графічне представлення станів та переходів життєвого циклу IoC у вигляді UML-діаграми станів наведено на рисунку 2.2.

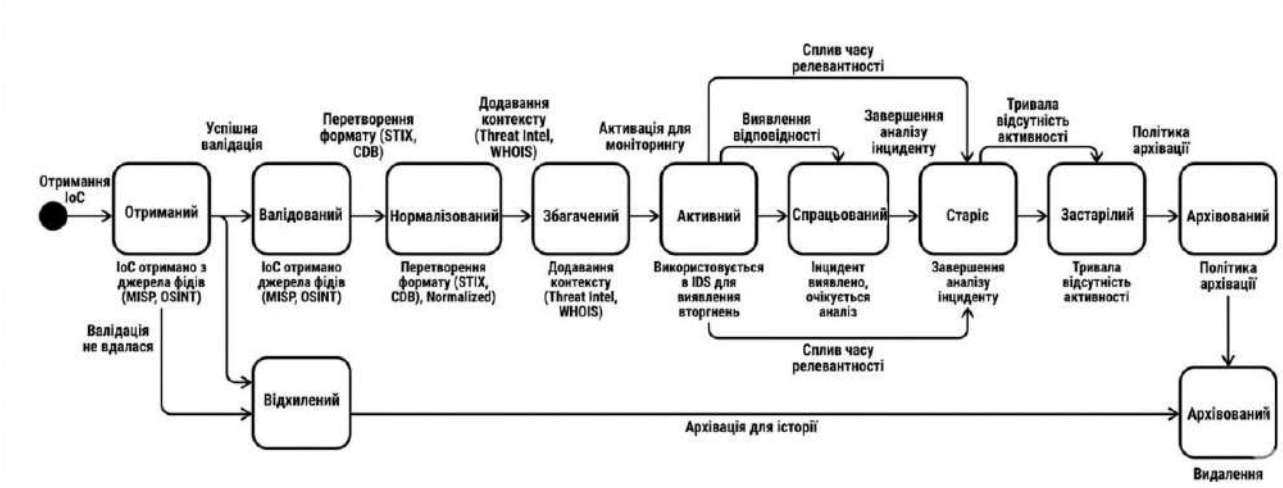


Рисунок 2.2 – Граф життєвого циклу індикатора компрометації

Особливістю моделі є введення двох додаткових станів. Стан старіє реалізує поступове зниження оцінки достовірності за експоненційною функцією, де значення залежить від часу та типу індикатора. Для хешів період актуальності становить приблизно 24 години, для IP адрес близько 7 діб, для доменів близько 30 діб, а для поведінкових та TTP індикаторів до одного року.

Стан спрацьований використовується як механізм зворотного зв’язку. Дані про спрацювання застосовуються для коригування рівня довіри до нових індикаторів аналогічного типу.

Модель враховує специфіку українських умов. Першим елементом є підтримка міток TLP, які визначають рівень поширення інформації. Другим є збільшення строку актуальності для індикаторів промислових систем керування, оскільки атаки на ICS розвиваються повільніше. Третім є автоматична прив’язка до публікацій CERT-UA з використанням ідентифікаторів бюлетенів. Четвертим є синхронізація з національною платформою MISP, де підтверджені інциденти експортуються як події для подальшого обміну розвідданими.

2.2 Алгоритми кореляції подій безпеки з базою індикаторів компрометації

Кореляція подій безпеки з базою індикаторів компрометації є ключовим етапом системи, оскільки саме тут сирі журнальні записи та мережеві події перетворюються на структуровані сповіщення з прив’язкою до конкретних технік атак.

Запропонований алгоритм побудовано як багаторівневий процес. Він поєднує швидкий пошук за атомарними індикаторами, аналіз сигнатур і правил, перевірку поведінкових патернів, а також контекстну перевірку в межах часових інтервалів. Такий підхід дозволяє поєднати високу швидкість обробки з достатньою точністю виявлення.

Алгоритм орієнтований на роботу в умовах реального навантаження енергетичного підприємства, де потік подій становить приблизно 1500 подій за секунду в IT сегменті та близько 200 подій за секунду в OT сегменті. У цих умовах система повинна формувати фінальні сповіщення із затримкою не більше 60 секунд.

Структурно алгоритм складається з чотирьох послідовних рівнів. Перший рівень є атомарним і передбачає миттєве порівняння подій із базою простих індикаторів. Другий рівень є сигнатурним і використовує правила виявлення для файлів і журналів подій. Третій рівень є поведінковим і аналізує послідовності дій у часовому вікні для виявлення типових сценаріїв атак. Четвертий рівень є

контекстним і виконує уточнення результатів з урахуванням історії подій та взаємозв’язків індикаторів.

Результатом проходження всіх рівнів є сформована тривога з високим рівнем достовірності, яка додатково може бути прив’язана до відповідної техніки. Загальна характеристика рівнів кореляції подана в таблиці 2.1.

Таблиця 2.1 – Рівні каскадного алгоритму кореляції подій безпеки з базою індикаторів компрометації

Рівень	Тип кореляції	Технічна реалізація	Тип IoC, що використовується	Затримка спрацювання	Очікувана частка інцидентів від загального потоку
1	Атомарна	Hash-таблиця, Bloom-фільтр	Атомарні (IP, домен, хеш, URL, e-mail)	<1 с	60–70 % спрацювань
2	Сигнатурна	YARA-сканер, Sigma-engine	YARA та Sigma правила	1–5 с	20–30 %
3	Поведінкова	Скінченний автомат подій	Послідовності TTP	5–60 с	5–10 %
4	Контекстна	Ретроспективний пошук у MISP	Кампанії, актори, галактики	1–5 хв	1–3 %

Аналіз наведених характеристик свідчить про те, що запропонована каскадна архітектура забезпечує раціональний розподіл обчислювальних потужностей за рахунок первинного відсікання масових загроз на нижчих рівнях. Загальна продуктивність системи залишається високою навіть в умовах інтенсивного мережевого трафіку.

Графічне представлення каскадного алгоритму кореляції з потоком даних від журналів до підтверджених тривог наведено на рисунку 2.3, де відображено ієрархію рівнів обробки та механізм формування фінального рішення.

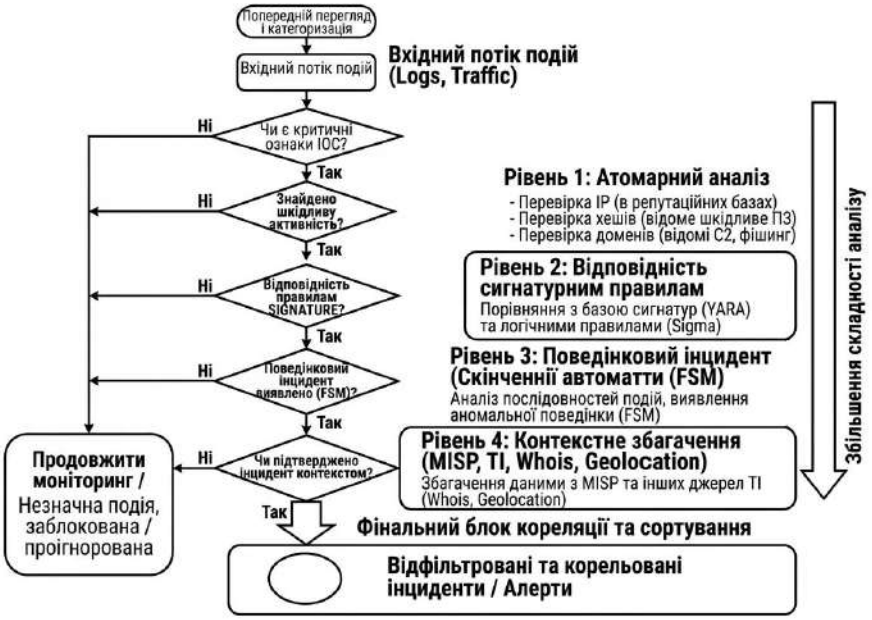


Рисунок 2.3 – Блок-схема каскадного алгоритму кореляції подій

Атомарний рівень забезпечує найшвидше зіставлення подій з індикаторами компрометації. Події попередньо нормалізуються у єдину структуру, після чого з них виділяються основні артефакти, такі як IP адреси, домени, URL, хеші файлів, шляхи запуску процесів, параметри командного рядка та e-mail поля. Ці значення порівнюються з активною базою індикаторів. Для прискорення пошуку використовується індексована структура даних з кешуванням у пам’яті. У разі збігу формується первинний кандидат на тривогу з повним контекстом події та метаданими індикатора.

Сигнатурний рівень виконує перевірку подій за допомогою правил виявлення. Для файлових об’єктів застосовуються YARA правила, для журналів подій використовуються Sigma правила, які виконуються в реальному часі після компіляції у формат, сумісний із системою моніторингу. Для промислового сегмента додатково враховується мережевий трафік ICS протоколів, що дозволяє виявляти специфічні сценарії атак на технологічні системи. Кожне правило пов’язується з відповідною технікою, що дозволяє одразу визначати характер дії зловмисника.

Поведінковий рівень аналізує не окремі події, а їх послідовності. Він реалізований у вигляді моделі скінченних станів, де кожен стан відповідає етапу

атаки. Наприклад, фішинг лист, відкриття вкладення, запуск процесів Office та подальша мережева активність утворюють єдиний ланцюжок подій. Перехід між станами в межах короткого часового інтервалу формує тривогу високого рівня. Такий підхід дозволяє виявляти складні багатокрокові атаки, які не визначаються окремими індикаторами.

Контекстний рівень виконує найглибший аналіз. На цьому етапі система звертається до зовнішніх і внутрішніх джерел кіберрозвідки для уточнення контексту індикатора. Визначається його належність до кіберугруповань, кампаній та пов’язаних подій. Також здійснюється ретроспективний аналіз для виявлення інших пов’язаних індикаторів у минулих подіях системи. У промисловому середовищі додатково враховується специфіка керування технологічними протоколами, що дозволяє виявляти аномальні або заборонені команди управління.

У результаті роботи всіх рівнів система формує єдину агреговану тривогу, яка містить усі знайдені індикатори, відповідні правила та найвищий рівень пріоритету. У разі одночасного спрацювання кількох механізмів пріоритет визначається з урахуванням критичності об’єкта та достовірності індикатора. Це дозволяє уникнути дублювання сповіщень і забезпечує цілісне представлення інциденту.

2.3 Застосування методів машинного навчання для оцінки достовірності та пріоритизації індикаторів компрометації

Сигнатурна та поведінкова кореляція забезпечує первинне виявлення подій, однак не вирішує дві ключові проблеми центрів моніторингу безпеки. Це велика кількість хибнопозитивних спрацювань та складність визначення пріоритету між одночасними інцидентами. У реальних умовах аналітики не можуть опрацьовувати сотні спрацювань на добу без втрати якості аналізу, тому виникає потреба в автоматизованій оцінці. Для вирішення цієї задачі застосовано

підхід на основі машинного навчання, який виконує оцінку достовірності та пріоритизацію тривог.

Першим завданням є бінарна класифікація. Для кожної тривоги обчислюється ймовірність того, що вона є реальним інцидентом. Якщо значення перевищує встановлений поріг, тривога підтверджується, інакше вона зберігається як низькопріоритетна для подальшого аналізу.

Другим завданням є оцінка пріоритету підтверджених тривог. Вона виконується як регресійна модель, що враховує критичність об'єкта, рівень значущості індикатора, історичну надійність джерела та контекст поточної кампанії. У результаті формується впорядкований список інцидентів за рівнем загрози. Загальна схема роботи алгоритму з онлайн оцінюванням і періодичним донавчанням моделі наведена на рисунку 2.4.

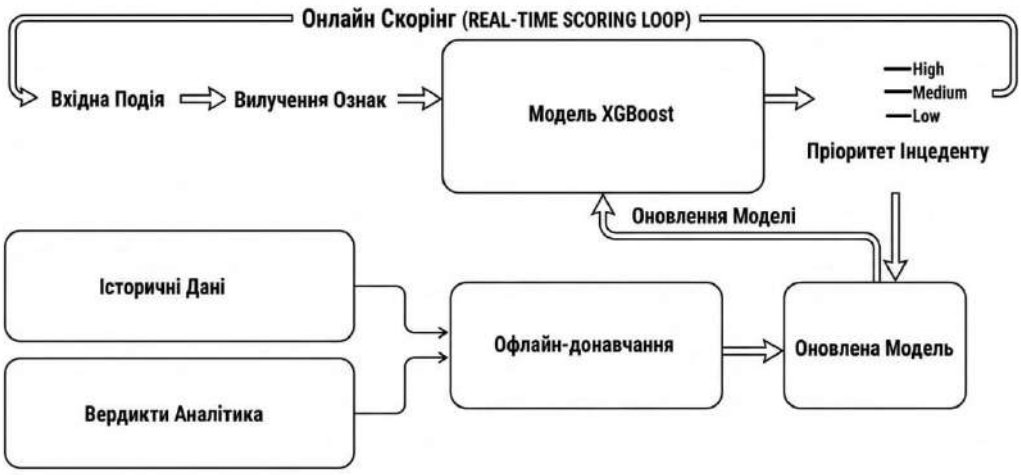


Рисунок 2.4 – Алгоритм машинного навчання та безперервного донавчання

Запропонована система виявлення вторгнень використовує підхід машинного навчання для оцінки достовірності індикаторів компрометації та пріоритизації тривог у потокових даних безпеки. Результати кореляційного аналізу подій додатково уточнюються ML-моделлю, що дозволяє зменшити кількість хибнопозитивних спрацювань і підвищити точність виявлення атак.

Ознаковий простір формується як багатовимірний набір параметрів, що описують індикатор, джерело та контекст події. Він включає чотири групи ознак.

Атрибутивні ознаки описують сам індикатор і включають тип індикатора, рівень у моделі піраміди болю, початкову оцінку достовірності, кількість незалежних підтверджень та строк актуальності. Поведінкові ознаки джерела відображають його надійність і включають історичну частку хибних і підтверджених спрацювань та стабільність оновлення даних. Контекстні ознаки характеризують умови виникнення події, зокрема критичність об'єкта, часові параметри, поточне навантаження SOC та наявність активних кампаній. Ознаки збагачення формуються на основі зовнішніх джерел кіберрозвідки та включають репутаційні оцінки IP-адрес і доменів, а також ознаки активності в ICS-середовищі. На рисунку 2.5 зображено єдину ML-архітектура оцінки та пріоритизації IoC.

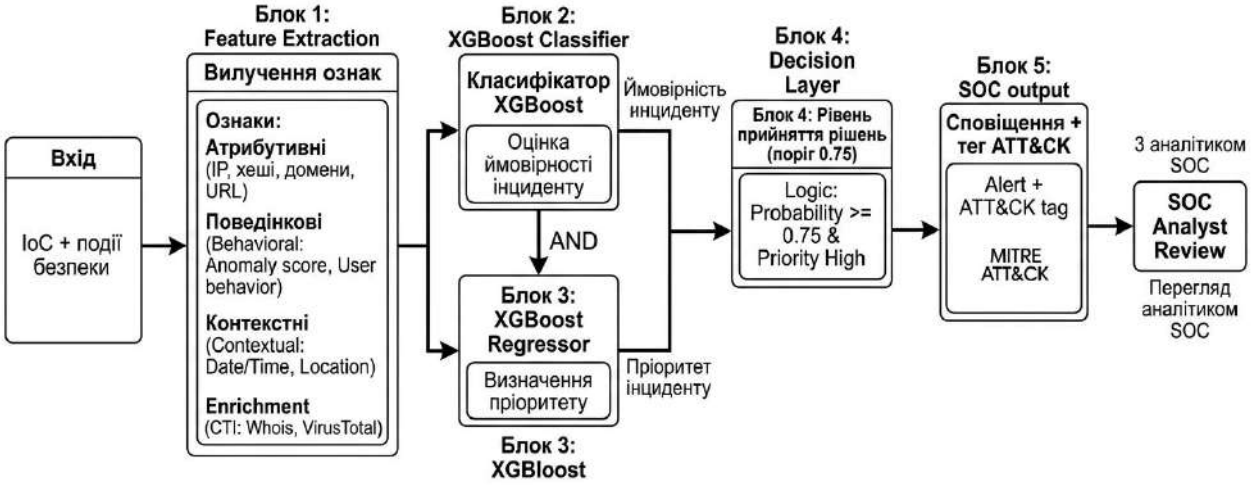


Рисунок 2.5 – Архітектура оцінки та пріоритизації індикаторів компрометації

Для класифікації тривог використовується модель градієнтного бустингу на деревах рішень, що забезпечує високу ефективність для табличних даних, стійкість до шуму та можливість інтерпретації результатів. Модель виконує бінарну класифікацію тривог і повертає ймовірність реального інциденту. Окремо реалізовано регресійну модель, яка визначає пріоритет інциденту на основі його критичності.

Гіперпараметри налаштовуються автоматично із застосуванням крос-валідації. Для інтерпретації рішень використовується підхід пояснюваності на

основі важливості ознак, що дозволяє аналітику SOC швидко визначати причини спрацювання.

Система підтримує механізм безперервного донавчання. Модель оновлюється на основі підтверджених інцидентів, отриманих під час експлуатації. У разі покращення метрик нова версія автоматично замінює попередню, у разі погіршення виконується відкат.

Додатково здійснюється контроль зміщення даних, що дозволяє виявляти зміну характеристик атак і своєчасно адаптувати модель до нових сценаріїв загроз.

Ефективність системи оцінюється як результат роботи повного конвеєра: кореляція подій, ML-скоринг та формування фінальних рішень SOC.

Базою оцінювання є матриця класифікаційних результатів TP, FP, FN, TN, на основі якої розраховуються основні метрики якості такі, як Precision, Recall та F1-міра. Для врахування дисбалансу класів додатково використовується MCC як стійкий інтегральний показник якості класифікації.

Часова ефективність визначається показником MTTD, який відображає середній час виявлення інциденту, та MTTR як повний час реагування системи з урахуванням дій SOC. Мінімізація MTTD є критично важливою для енергетичних ІКС.

Додатково використовується показник покриття технік, що визначає частку атакувальних технік, для яких реалізовані правила виявлення. Це дозволяє оцінити структурну повноту системи.

Для врахування реальної вартості помилок застосовується зважена модель оцінювання, у якій пропуск атаки має значно вищу вагу, ніж хибне спрацювання, що відповідає вимогам критичної інфраструктури.

Оцінювання виконується у двох режимах: онлайн (вікно для моніторингу якості в реальному часі) та офлайн (порівняння з еталонними системами на єдиному тестовому потоці).

2.4 Архітектура та логічна організація запропонованої системи виявлення вторгнень на основі IoC

Архітектура системи об’єднує всі попередньо описані модулі такі, як збір та нормалізацію індикаторів, їх життєвий цикл, багаторівневу кореляцію, а також машинне навчання у єдиний програмно-технічний комплекс для застосування в сегментованій OT-інфраструктурі енергетичного об’єкта. Система побудована як модульна багаторівнева платформа, що забезпечує безперервний цикл, як-от отримання IoC, їх обробку, виявлення подій, оцінку ризику та реагування.

Логічна структура системи поділяється на сім функціональних рівнів. Перший рівень формують джерела даних та сенсори. У IT-сегменті це агенти збору подій з серверів і робочих станцій, системи журналювання та мережеві шлюзи. В OT-сегменті використовується пасивний аналіз промислового трафіку за допомогою мережевих сенсорів, що забезпечують спостереження за протоколами керування технологічними процесами без активного втручання в їх роботу.

Другий рівень відповідає за збір індикаторів компрометації з зовнішніх і внутрішніх джерел Threat Intelligence. Використовується набір незалежних каналів. Усі індикатори надходять у систему уніфікованими потоками для подальшої обробки.

Третій рівень виконує обробку та нормалізацію індикаторів. На цьому етапі здійснюється перевірка коректності, приведення до єдиного представлення та збагачення додатковим контекстом із зовнішніх сервісів кіберрозвідки. Результатом є структуровані індикатори, готові до зберігання та кореляції.

Четвертий рівень реалізує зберігання та управління життєвим циклом IoC. Центральним елементом є платформа обміну індикаторами, яка виконує функції бази даних та API доступу. Додатково використовується швидкий індекс активних індикаторів, що забезпечує оперативний пошук під час кореляції. Життєвий цикл включає автоматичне оновлення статусів від активного до

архівного стану відповідно до часових і поведінкових характеристик.

П’ятим рівенем є кореляція подій безпеки. Потоки журналів із IT та OT сегментів аналізуються у реальному часі шляхом зіставлення з активними індикаторами. Використовується каскадна модель виявлення з урахуванням контексту інциденту. Результатом є формування кандидатів на інциденти.

Шостий рівень відповідає за оцінку та пріоритизацію тривог із використанням моделей машинного навчання. Застосовується ансамбль на основі градієнтного бустингу, який виконує оцінку ймовірності інциденту та визначення його пріоритету. Це дозволяє зменшити кількість хибних спрацювань і забезпечити ранжування подій за критичністю для SOC.

Сьомий рівень забезпечує візуалізацію, реагування та зворотний зв’язок. Аналітики отримують інформацію через інтерфейс моніторингу з відображенням активних інцидентів, їх контексту та прив’язки до технік атак. Реалізовано механізми автоматичного реагування, а також зворотне включення результатів розслідування у процес донавчання моделі, що забезпечує адаптацію системи до нових типів атак.

Фізична архітектура системи базується на розділенні мережі енергетичного підприємства на три сегменти: IT, DMZ та OT. Між сегментами діють контрольовані правила обміну даними, що мінімізують ризик між корпоративною та технологічною інфраструктурою.

Така конфігурація фізичної архітектури дозволяє локалізувати потенційні загрози та унеможливлює пряме горизонтальне переміщення зловмисників із корпоративної мережі до критично важливих технологічних процесів. Організація шлюзів безпеки на межах DMZ забезпечує суворе розмежування прав доступу, фільтрацію специфічних промислових протоколів та детальне логування міжсегментного трафіку, що створює надійне підґрунтя для превентивного виявлення аномальних інформаційних потоків ще до їх проникнення в OT-сегмент.

Загальну топологію взаємодії сегментів IT/DMZ/OT та напрямки потоків даних у системі виявлення вторгнень наведено на рисунку 2.6.

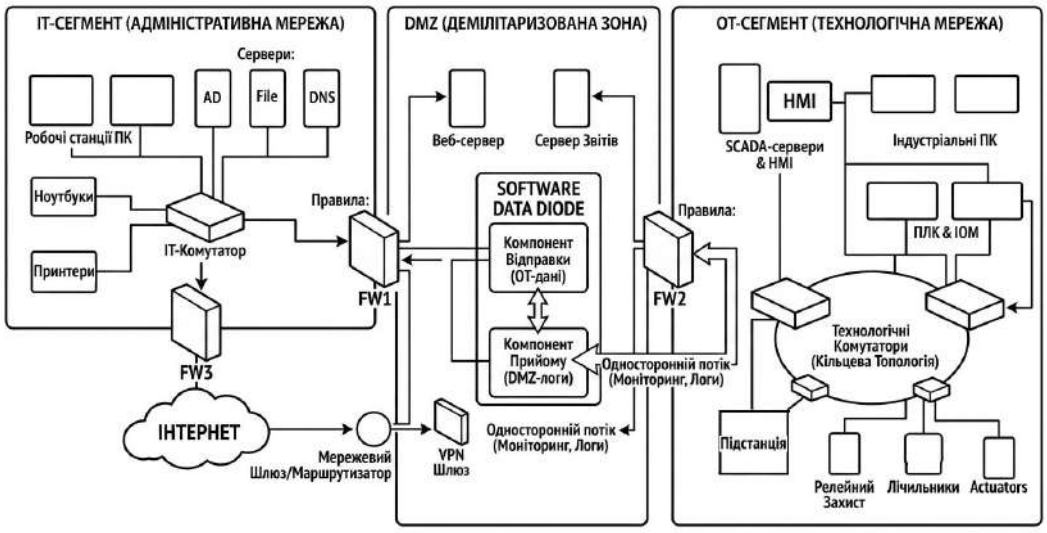


Рисунок 2.6 – Фізична топологія мережі обленерго

Розміщення компонентів системи виконується з урахуванням поділу мережі на технологічну, демілітаризовану та корпоративну частини. У технологічному середовищі встановлюються пасивні мережеві сенсори для аналізу трафіку, а також агенти моніторингу на серверах SCADA, EMS і автоматизованих робочих місцях диспетчерів. Передавання інформації з технологічної мережі здійснюється лише в одному напрямку через спеціалізований шлюз передачі даних. Це виключає можливість зовнішнього доступу до критичних систем керування.

У демілітаризованій зоні розміщуються основні компоненти обробки подій безпеки. Тут функціонують сервер керування журналами, платформа обміну індикаторами компрометації, модулі обробки повідомлень, кешування та модуль оцінки подій на основі машинного навчання. Таке розділення дозволяє ізолювати критичні процеси від корпоративної мережі та зменшити ризик поширення атаки.

У корпоративному середовищі використовуються агенти моніторингу робочих станцій і вебінтерфейс центру моніторингу безпеки. Доступ до зовнішніх джерел кіберрозвідки здійснюється через окремий захищений канал із фільтрацією дозволених адрес. Усі зовнішні підключення обмежуються лише отриманням необхідних даних без прямої взаємодії з технологічною мережею.

Для енергетичного підприємства середнього масштабу система не потребує надмірних апаратних ресурсів. Основне навантаження припадає на сервери збору журналів і сховище подій безпеки. Окремо використовуються сервери для платформи обміну індикаторами, модулів обробки даних і мережевих сенсорів. Запропонована конфігурація може бути розгорнута в межах стандартної серверної інфраструктури підприємства без необхідності використання дорогих комерційних комплексів.

Важливою частиною архітектури є інтеграція з національною системою кіберзахисту. Система підтримує автоматичне отримання індикаторів компрометації з державних і міжнародних джерел кіберрозвідки. У разі підтвердження критичного інциденту формується структуроване повідомлення з технічними артефактами атаки, яке після перевірки аналітиком може передаватися до національної системи обміну інформацією про кіберзагрози. Це дозволяє реалізувати постійний обмін актуальними даними між організаціями.

Для забезпечення масштабованості система побудована за модульним принципом. Кожен компонент виконує окрему функцію та може запускатися незалежно від інших. Це дозволяє поступово збільшувати продуктивність шляхом додавання нових вузлів без зміни загальної архітектури системи. Такий підхід спрощує модернізацію та адаптацію системи до збільшення обсягів подій безпеки.

2.5 Порівняльний аналіз запропонованого рішення з вітчизняними та зарубіжними аналогами

Запропонована система займає проміжне положення між базовими відкритими засобами моніторингу та повноцінними комерційними SIEM платформами. На відміну від стандартних конфігурацій Wazuh або Suricata, система підтримує багаторівневу кореляцію подій, роботу з індикаторами компрометації та інтеграцію з джерелами кіберрозвідки. Це дозволяє виявляти

не лише окремі сигнатури атак, а й пов’язані послідовності дій зловмисника.

Порівняно з комерційними рішеннями, такими як Splunk Enterprise Security, IBM QRadar або Microsoft Sentinel, запропонована система має меншу кількість готових інтеграцій та додаткових аналітичних модулів. Водночас її архітектура орієнтована саме на потреби енергетичної галузі та враховує особливості української інфраструктури критичних об’єктів. Основний акцент зроблено на локальному зберіганні даних, підтримці національної системи обміну індикаторами компрометації та можливості роботи у сегментованих ОТ мережах. Як видно з таблиці 2.2, запропонована система поєднує функціональні можливості комерційних платформ із перевагами відкритого програмного забезпечення. При цьому основний акцент зроблено на адаптації до потреб енергетичної галузі та українських нормативних вимог.

Таблиця 2.2 – Порівняння запропонованої системи з існуючими рішеннями

Критерій	Запропонована система	Wazuh	Splunk ES	IBM QRadar
Робота з IoC	+	Частково	+	+
Інтеграція з CERT-UA	+	Ні	Ні	Ні
Підтримка ОТ мереж	+	Частково	+	+
Локальне зберігання даних	+	+	Частково	Частково
Відкритий код	+	+	Ні	Ні
Масштабованість	+	+	+	+
Вартість впровадження	Низька	Низька	Висока	Висока

Важливою перевагою є використання відкритих компонентів. Це дозволяє зменшити залежність від конкретного виробника та спрощує модернізацію системи. Додавання нових правил виявлення, джерел кіберрозвідки або окремих модулів не потребує зміни всієї архітектури. Крім цього, використання контейнерного підходу дає змогу масштабувати окремі компоненти залежно від навантаження.

Окрему увагу приділено інтеграції з українською екосистемою кіберзахисту. Система підтримує автоматизоване отримання індикаторів компрометації з CERT-UA та інших джерел кіберрозвідки. Це забезпечує швидке оновлення правил виявлення відповідно до актуальних загроз для енергетичного сектору.

Порівняно з більшістю академічних розробок, які зазвичай зосереджені лише на окремих алгоритмах виявлення аномалій або тестових моделях машинного навчання, запропонована система реалізує повний цикл обробки подій безпеки. Архітектура охоплює збір журналів, аналіз індикаторів компрометації, кореляцію подій, оцінку ризику та формування тривог для оператора центру моніторингу безпеки.

У практичному аспекті така комплексна та автоматизована архітектура дозволяє суттєво знизити когнітивне навантаження на аналітиків центру моніторингу. Завдяки попередньому каскадному відсіканню шумів та інтелектуальній пріоритезації інцидентів, оператори позбавляються необхідності вручну обробляти величезні масиви сирих логів, що мінімізує ймовірність пропуску цілеспрямованої атаки через людський фактор.

Таким чином, запропоноване рішення поєднує переваги відкритих платформ, адаптацію до українських нормативних вимог та спеціалізацію на захисті енергетичної інфраструктури. Це дозволяє використовувати систему як практичний інструмент для підвищення рівня кіберзахисту об’єктів критичної інфраструктури.

2.6 Висновок

У другому розділі було розроблено структуру та основні алгоритми системи виявлення вторгнень на основі індикаторів компрометації для інформаційно-комунікаційних систем енергетичної галузі. Основну увагу приділено побудові комплексного рішення, яке поєднує збір та обробку

індикаторів компрометації, кореляцію подій безпеки, машинне навчання та інтеграцію з національною системою кіберзахисту.

У процесі роботи сформовано модель життєвого циклу індикаторів компрометації, яка враховує їх актуальність, рівень довіри та можливість автоматичного оновлення. Також запропоновано алгоритм збору та нормалізації даних із зовнішніх і внутрішніх джерел кіберрозвідки з подальшим збагаченням додатковим контекстом.

Розроблено багаторівневий механізм кореляції подій безпеки, що дозволяє поєднувати сигнатурний, поведінковий і контекстний аналіз. Для зменшення кількості хибних спрацювань використано моделі машинного навчання, які виконують оцінку достовірності та пріоритизацію тривог.

Окремо розроблено архітектуру системи для роботи в сегментованій IT та OT інфраструктурі енергетичних підприємств. Архітектура побудована за модульним принципом, підтримує масштабування та враховує вимоги до ізоляції технологічної мережі. Для реалізації системи використано відкриті програмні компоненти, що дозволяє зменшити вартість впровадження та спростити подальшу модернізацію.

Проведений порівняльний аналіз показав, що запропоноване рішення поєднує переваги відкритих платформ із можливістю адаптації до українських нормативних вимог і потреб енергетичного сектору. Це дозволяє розглядати систему як практичний засіб підвищення рівня кіберзахисту об’єктів критичної інфраструктури.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ТЕСТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

3.1 Обґрунтування вибору технологічного стеку та проєктування лабораторного стенду для апробації системи

Для практичної реалізації системи було сформовано технологічний стек, який забезпечує підтримку роботи з індикаторами компрометації, аналіз подій безпеки та можливість використання у сегментованих IT і OT мережах енергетичних підприємств. Під час вибору компонентів враховувалися можливість локального розгортання, сумісність з відкритими стандартами, підтримка інтеграції з платформами кіберрозвідки та доступність для підприємств із обмеженим бюджетом.

Як основу системи моніторингу подій безпеки обрано платформу Wazuh. Вона забезпечує централізований збір журналів, підтримку правил виявлення атак, інтеграцію з MITRE ATT&CK та можливість роботи з індикаторами компрометації. Для обміну даними кіберрозвідки використано платформу MISP, яка підтримує автоматичну синхронізацію індикаторів та широко застосовується у діяльності центрів реагування на кіберінциденти.

Для аналізу мережевого трафіку використано Suricata з підтримкою промислових протоколів, що дозволяє виконувати моніторинг подій у технологічному середовищі без втручання у роботу обладнання. Зберігання та індексація журналів реалізовані на базі OpenSearch, а для взаємодії між окремими модулями системи використано RabbitMQ і Redis.

Власні модулі системи реалізовано мовою Python, оскільки вона має розвинуті бібліотеки для обробки журналів, роботи з API платформ кіберрозвідки та побудови моделей машинного навчання. Для контейнеризації компонентів використано Docker, що спрощує розгортання та масштабування системи.

Для перевірки працездатності запропонованої архітектури було створено лабораторний стенд, який моделює структуру мережі типового енергетичного

підприємства. Стенд побудовано у вигляді трьох окремих сегментів: корпоративного IT середовища, демілітаризованої зони та технологічного OT сегмента. Загальну структуру лабораторного стенду та взаємодію його основних компонентів наведено на рисунку 3.1.

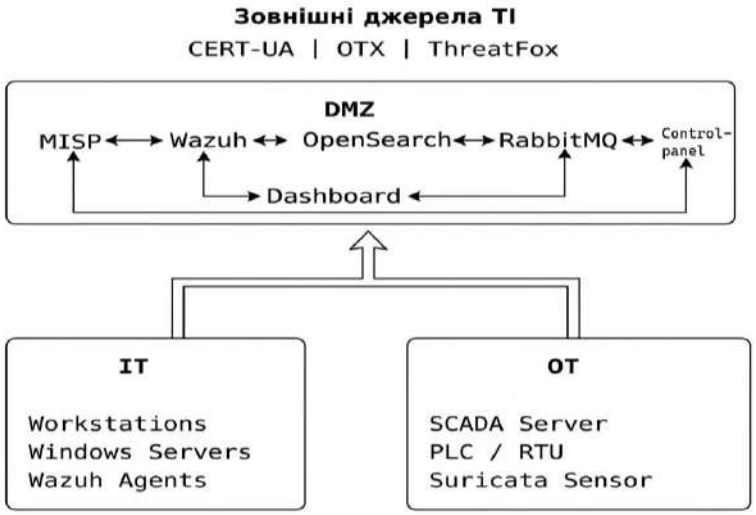


Рисунок 3.1 – Структура лабораторного стенду системи виявлення вторгнень

У корпоративному сегменті розміщувалися робочі станції користувачів, сервери домену, файлові та поштові служби. У демілітаризованій зоні функціонували основні компоненти системи виявлення вторгнень, платформа обробки індикаторів компрометації та засоби централізованого моніторингу. Технологічний сегмент містив сервери SCADA та емулятори промислових пристроїв з підтримкою протоколів промислового обміну даними.

Між сегментами було налаштовано обмежений мережевий обмін із контролем дозволених з'єднань. Для технологічного сегмента використовувався принцип односторонньої передачі даних до демілітаризованої зони, що дозволяє зменшити ризик несанкціонованого доступу до критичної інфраструктури.

Для створення навантаження у стенді моделювалися типові дії користувачів, робота корпоративних сервісів та регулярний обмін даними між компонентами SCADA системи. Це дозволило відтворити умови, наближені до роботи реального енергетичного підприємства, та провести подальше тестування

системи виявлення вторгнень.

Після формування лабораторного стенду виконано розгортання основних компонентів системи, зокрема платформи MISP та SIEM-системи Wazuh. Їх інтеграція забезпечила автоматичний обмін індикаторами компрометації та централізований аналіз подій безпеки.

Розгортання платформи MISP виконувалося у демілітаризованому сегменті лабораторного стенду на окремому сервері під керуванням Linux. Після встановлення було створено структуру користувачів для адміністраторів та аналітиків SOC, а також налаштовано механізми автентифікації та контролю доступу. У системі активовано таксономії для класифікації індикаторів, рівнів довіри та категорій атак. Додатково підключено зовнішні джерела кіберрозвідки, з яких система автоматично отримувала нові індикатори компрометації.

Для централізованого аналізу подій безпеки розгорнуто платформу Wazuh. До системи було підключено агенти з корпоративного та технологічного сегментів мережі, а також мережеві сенсори Suricata. Це дозволило отримувати журнали подій від серверів, робочих станцій та компонентів SCADA середовища.

У процесі налаштування Wazuh активовано стандартні правила виявлення атак та створено додаткові правила для аналізу подій у технологічному сегменті. Окрему увагу приділено підтримці промислових протоколів та подій, характерних для енергетичної інфраструктури.

Інтеграцію MISP та Wazuh реалізовано у декількох напрямах. Перший механізм забезпечує передачу у фоновому режимі індикаторів компрометації з MISP до Wazuh для подальшого використання у правилах виявлення. Після оновлення бази індикаторів нові IP-адреси, домени та хеші файлів автоматично додаються до списків перевірки SIEM-системи.

Другий механізм інтеграції пов’язаний із формуванням та збагаченням тривог. Під час спрацювання правила безпеки Wazuh без участі операторів отримує додаткову інформацію про індикатор компрометації з платформи MISP. До тривоги додаються відомості про тип загрози, можливе шкідливе програмне

забезпечення, пов’язані техніки MITRE ATT&CK та джерело отримання індикатора. Це дозволяє аналітикам швидше оцінювати рівень небезпеки інциденту.

Третій напрямок інтеграції забезпечує зворотний зв’язок між компонентами системи. У разі підтвердження інциденту нові артефакти можуть автоматиовано додаватися до внутрішньої бази MISP для подальшого використання у процесі виявлення атак.

На рисунку 3.2 наведено послідовність взаємодії компонентів системи під час отримання індикаторів компрометації, їх обробки та формування тривог у SIEM середовищі.

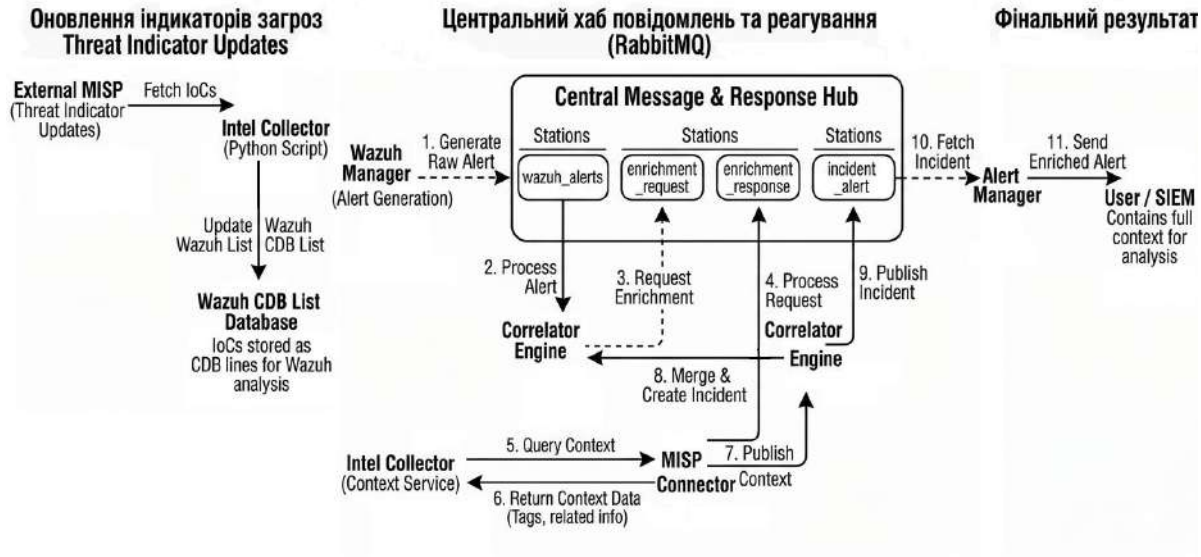


Рисунок 3.2 – Діаграма послідовності

Під час тестування перевірено коректність передачі індикаторів між платформами, формування тривог та роботу механізмів збагачення подій. Результати показали, що система забезпечує стабільну синхронізацію даних та підтримує роботу у режимі, наближеному до реального часу.

Додатково виконано перевірку відмовостійкості системи. У разі тимчасової недоступності платформи MISP SIEM-система продовжувала аналіз подій із використанням раніше отриманих індикаторів компрометації. Після відновлення роботи синхронізація між компонентами автоматично

поновлювалася без втрати даних.

Запропонована інтеграція дозволила об’єднати можливості централізованого зберігання індикаторів компрометації та автоматизованого аналізу подій безпеки в єдину систему моніторингу кіберзагроз для енергетичної інфраструктури.

3.2 Розробка модулів автоматизованого збору, нормалізації та кореляції індикаторів компрометації

Для забезпечення функціональності, орієнтованої на специфіку енергетичного сектору України, у межах роботи було розроблено набір власних програмних модулів, які реалізують автоматизований збір, обробку, кореляцію та аналіз індикаторів компрометації. Необхідність створення власних компонентів обумовлена тим, що стандартні можливості платформ MISP та Wazuh не забезпечують повної підтримки національних джерел кіберрозвідки, специфіки українських бюлетенів CERT-UA та аналізу подій у промислових OT-сегментах.

Усі модулі реалізовано мовою Python 3.11 та побудовано за принципом мікросервісної архітектури. Кожен компонент функціонує як окремий сервіс у Docker-контейнері та виконує власний етап обробки даних. Такий підхід забезпечує незалежне масштабування компонентів, спрощує оновлення системи та дозволяє додавати нові модулі без зміни існуючої архітектури. Використання контейнеризації дозволило ізолювати залежності окремих сервісів та забезпечити відтворюваність розгортання системи у різних середовищах.

Для взаємодії між сервісами використано брокер повідомлень RabbitMQ, через який реалізовано асинхронний конвеєр обробки подій. Це дозволяє ізолювати окремі етапи аналізу індикаторів компрометації та забезпечує стабільну роботу системи навіть у разі тимчасової недоступності окремих компонентів. Додатково використано Redis для кешування результатів

збагачення та тимчасового зберігання службових даних.

Першим етапом конвеєра є автоматизований збір індикаторів компрометації з відкритих і національних джерел кіберрозвідки. Для цього реалізовано модуль збору даних, який підтримує роботу з TAXII 2.1 API та резервний режим парсингу вебсторінок CERT-UA. Модуль виконує періодичне опитування джерел, виявляє нові бюлетені та автоматично витягує IP-адреси, домени, URL, хеші файлів та інші індикатори компрометації. У разі недоступності основного каналу отримання даних система автоматично переходить у резервний режим роботи.

Після отримання індикаторів виконується їх валідація. На цьому етапі перевіряється коректність формату індикаторів, відсутність дублікатів та відповідність внутрішнім правилам безпеки. Додатково здійснюється фільтрація службових або довірених ресурсів, які не повинні брати участь у процесі виявлення загроз.

Наступним етапом є нормалізація індикаторів компрометації до формату STIX 2.1. Це дозволяє уніфікувати представлення даних незалежно від джерела їх отримання та забезпечує сумісність із платформою MISP і зовнішніми системами кіберрозвідки. Під час нормалізації до індикаторів додаються службові атрибути: джерело отримання, рівень довіри, категорія загрози, пов’язані кампанії та техніки MITRE ATT&CK.

Після нормалізації індикатори передаються до модуля збагачення, який автоматично виконує запити до зовнішніх сервісів кіберрозвідки. Для цього використовуються VirusTotal, AbuseIPDB, Shodan, MalwareBazaar та інші джерела. Отримані результати містять інформацію про геолокацію IP-адрес, репутацію доменів, зв’язок із шкідливим програмним забезпеченням та історію попередніх інцидентів. Застосування паралельної асинхронної обробки дозволяє виконувати одночасно декілька запитів та зменшує загальний час аналізу індикаторів.

Ключовим компонентом системи є модуль кореляції подій безпеки, який реалізує багаторівневий механізм аналізу. На першому рівні здійснюється

швидке атомарне зіставлення подій із базою індикаторів компрометації. Другий рівень використовує сигнатурний аналіз на основі правил Sigma та YARA. Третій рівень виконує поведінкову кореляцію подій, аналізуючи послідовності дій користувачів і процесів. Четвертий рівень забезпечує контекстний аналіз із використанням інформації платформи MISP.

Особливу увагу приділено підтримці подій технологічного сегмента. У модулі кореляції реалізовано обробку подій промислових протоколів. Це дозволяє виявляти аномальні команди, нехарактерну активність між вузлами SCADA-середовища та поведінку, подібну до відомих атак на енергетичну інфраструктуру.

Для пріоритизації тривог у системі використано модуль машинного навчання. Модель аналізує набір характеристик інциденту, оцінює рівень ризику та визначає пріоритет реагування. Додатково реалізовано механізм пояснення результатів моделі, що дозволяє аналітикам SOC отримувати обґрунтування причин спрацювання. В таблиці 3.1 представленні основні модулі програми та для чого вони необхідні.

Таблиця 3.1 – Основні програмні модулі системи та їх призначення

Модуль	Основне призначення
certua_collector	Автоматизований збір індикаторів компрометації з CERT-UA та зовнішніх джерел
ioc_validator	Перевірка коректності та фільтрація індикаторів
ioc_normalizer	Нормалізація індикаторів до формату STIX 2.1
ioc_enricher	Збагачення індикаторів даними зовнішніх сервісів
correlator_engine	Багаторівнева кореляція подій безпеки
ml_scorer	Оцінювання пріоритету тривог засобами ML
feedback_processor	Обробка зворотного зв’язку від аналітиків SOC

Окремий модуль забезпечує механізм зворотного зв’язку від аналітиків SOC. Після підтвердження інциденту нові індикатори компрометації

автоматично додаються до внутрішньої бази MISP та можуть повторно використовуватись у процесі виявлення атак. У разі виявлення хибнопозитивних спрацювань система накопичує статистику для подальшого коригування ваг правил і підвищення точності аналізу. На рисунку 3.3 наведено схему взаємодії розроблених модулів у межах мікросервісної архітектури системи.

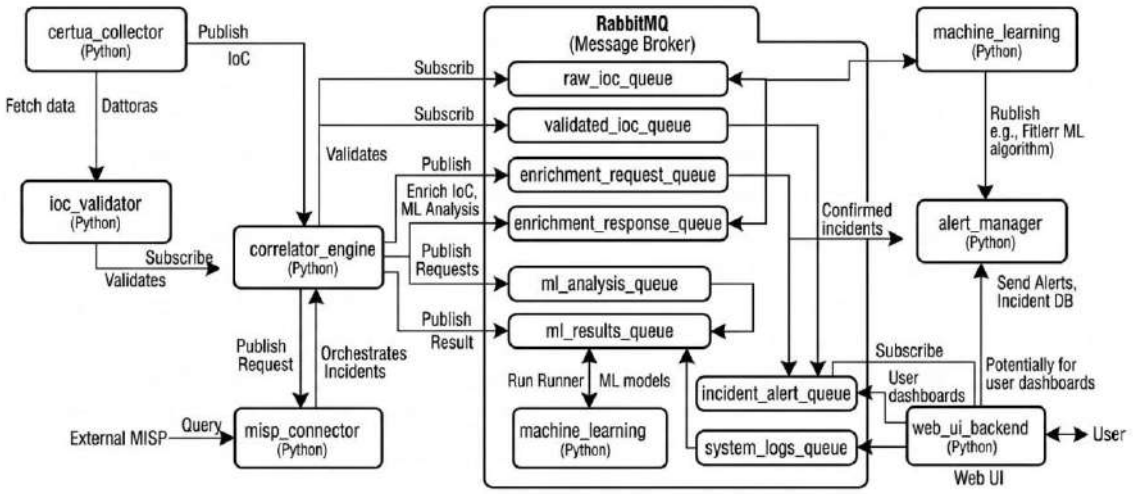


Рисунок 3.3 – Схема мікросервісної взаємодії власних модулів

Для перевірки коректності роботи модулів виконано модульне та інтеграційне тестування. Перевірялася коректність збору індикаторів з бюлетенів CERT-UA, валідація різних типів IoC, нормалізація STIX-об’єктів та робота механізмів кореляції подій. Окремо тестувалися сценарії багатокрокових атак, пов’язаних із фішинговими кампаніями та несанкціонованими діями у SCADA-середовищі.

Результати тестування підтвердили стабільну роботу модулів у режимі безперервної експлуатації. Система забезпечувала автоматичну обробку індикаторів компрометації з декількох джерел кіберрозвідки та аналіз великого потоку подій безпеки у режимі, наближеному до реального часу. Завдяки мікросервісній архітектурі та використанню асинхронної обробки було забезпечено високу масштабованість і відмовостійкість системи.

Для реалізації другого рівня каскадного алгоритму кореляції у системі використано механізм сигнатурного аналізу на основі правил YARA та Sigma.

Використання двох типів сигнатур дозволило забезпечити виявлення як шкідливих файлів і артефактів у пам’яті, так і підозрілої активності у журналах подій операційних систем та мережевих сервісів.

Під час розробки правил основна увага приділялася загрозам, характерним для українського енергетичного сектору та промислових систем керування. Каталог YARA-правил орієнтований на виявлення шкідливого програмного забезпечення, яке використовувалося у кібератаках проти енергетичної інфраструктури. Правила забезпечують виявлення артефактів сімейств HermeticWiper, Industroyer, CaddyWiper, BlackEnergy, KillDisk та інших загроз, пов’язаних із діяльністю APT-груп. Додатково реалізовано правила для виявлення PowerShell-скриптів, фішингових документів та інструментів постексплуатації. Реалізовано правила для виявлення запуску PowerShell із закодованими параметрами, створення підозрілих служб, використання WMI, спроб викрадення облікових даних, нетипових RDP-підключень та аномальної активності у SCADA-середовищі.

Для інтеграції правил із SIEM-системою використано механізми Wazuh та wazuh-yara. Sigma-правила автоматично конвертувалися у формат Wazuh та застосовувалися під час аналізу журналів подій. YARA-правила використовувалися для перевірки файлів і артефактів, що з’являлися у моніторингованих директоріях.

3.3 Експериментальне тестування системи

Для оцінки ефективності розробленої системи виявлення вторгнень проведено серію експериментальних тестувань у лабораторному стенді, який моделює структуру мережі енергетичного підприємства. Основою тестування стали типові сценарії атак, характерні для українського енергетичного сектору та описані у публічних звітах CERT-UA і MITRE ATT&CK.

Кожен сценарій являв собою послідовність тактик і технік MITRE

ATT&CK, реалізованих за допомогою спеціальних скриптів-симуляторів. Під час виконання атак система працювала у штатному режимі без попереднього повідомлення про тип сценарію. Для підвищення достовірності результатів кожен сценарій запускався тричі з різними параметрами: змінювалися час запуску, цільові хости та мережеві адреси керуючих серверів. Тривалість одного сценарію становила від 15 хвилин до 2 годин.

У межах експериментального тестування змодельовано десять сценаріїв атак, що охоплюють як корпоративний IT-сегмент, так і технологічне OT-середовище. Серед них представленні фішингові кампанії з використанням PowerShell, компрометація через VPN, атаки типу BlackEnergy та Industroyer2, несанкціоновані команди у промислових протоколах, інсайдерські загрози та supply chain атаки через компрометовані оновлення програмного забезпечення. Для кожного сценарію оцінювалися час виявлення атаки, механізми спрацювання та рівень сформованої тривоги. Зведений перелік 10 змодельованих сценаріїв атак – у таблиці 3.1.

Таблиця 3.1 – Сценарії атак, змодельовані у межах експериментального тестування системи

№	Сценарій	Кампанія / угруповання-прообраз	Ключові техніки MITRE ATT&CK	Цільовий сегмент	Очікувана виявленість
1	2	3	4	5	6
1	Spearphishing з вкладенням і виконанням PowerShell	Sandworm (UAC-0082)	T1566.001, T1059.001, T1071.001	IT (робоча станція)	YARA + Sigma + поведінкове
2	Компрометація через VPN з пе́рехопленням облікових даних	APT33 / OilRig стиль	T1078, T1110.003, T1021.002	IT (домен AD)	Sigma + ML-скорінг

Кінець таблиці 3.1

1	2	3	4	5	6
3	BlackEnergy-подібна атака з KillDisk-фіналом	BlackEnergy 3 (2015)	T1566.001, T1059.005, T1485, T1490	IT + OT (АРМ диспетчерів)	YARA + поведінкове
4	Industroyer-подібна атака на ICS-протокол IEC 60870-5-104	Industroyer (2016)	T0814, T0831, T0855 (ICS)	OT (IEC-104 трафік)	Sigma ICS + контекстне
5	Industroyer2-подібна точкова атака на підстанцію	Industroyer2 (2022)	T0809, T0814, T0831, T0855 (ICS)	OT (RTU/IED)	Sigma ICS + YARA
6	HermeticWiper-подібна масова атака з контролера домену	Sandworm UAC-0082 (2022)	T1078.002, T1485, T1561.002	IT (масштабна)	YARA + поведінкове + ML
7	FrostyGoop-подібна атака через Modbus TCP	CHERNOVITE / нові ICS-загрози (2024)	T0855, T0831 (ICS)	OT (Modbus 502)	Sigma ICS + контекстне
8	Living-off-the-Land з certutil + bitsadmin	TTP, спільні для багатьох APT	T1218.005, T1197, T1059.003	IT (адміністративний)	Sigma + ML
9	Інсайдерська загроза: викрадення SCADA-конфігурацій	Внутрішній зловмисник	T1078, T1005, T1567.002	T1078, T1005, T1567.002	Sigma + поведінкове + ML
10	Supply chain: компрометація через оновлення інтегратора	NotPetya/M.E.Doc стиль	T1195.002, T1059.005, T1489	IT (масштабна)	YARA + ML

Найбільш показовими для оцінки системи стали сценарії BlackEnergy-подібної атаки та атаки типу Industroyer2 на ICS-сегмент.

Сценарій BlackEnergy відтворював типову схему атаки на енергетичну інфраструктуру через фішингове повідомлення з вкладенням Microsoft Word. Після відкриття документа активувався макрос, який запускав PowerShell-

команду з подальшим встановленням з’єднання із зовнішнім сервером керування. На завершальному етапі виконувалося завантаження шкідливого компонента типу KillDisk, призначеного для пошкодження системних даних.

Під час тестування система зафіксувала збіг хеша вкладення з індикатором компрометації у MISP, після чого було сформовано первинну тривогу. Додатково спрацювали YARA-правила для виявлення характерних ознак шкідливого файла та Sigma-правила для аналізу ланцюжка процесів. Після поведінкової кореляції подій система сформувала комплексну тривогу. Середній час виявлення атаки становив близько 95 секунд.

Другий сценарій моделював атаку типу Industroyer2 на технологічний сегмент мережі. Атака передбачала використання скомпрометованого облікового запису для переходу з IT-сегмента до технологічного шлюзу та запуску шкідливого модуля. У процесі атаки генерувалися команди керування, характерні для несанкціонованого відключення обладнання підстанції.

Під час виконання сценарію система виявила нетипові команди у мережевому трафіку OT-сегмента за допомогою Sigma-правил для ICS-протоколів. Додатково YARA-аналіз виявив характерні рядки та сигнатури, пов’язані з Industroyer2. Після кореляції подій і отримання контексту з MISP система сформувала тривогу критичного рівня. Середній час виявлення атаки становив близько 74 секунд.

Під час виконання сценарію №5 система зафіксувала серію несанкціонованих команд у мережевому трафіку технологічного сегмента. Після запуску шкідливого модуля на технологічному шлюзі YARA-правило виявило характерні сигнатури файла та сформувало тривогу другого рівня через декілька секунд після його появи у системі. Одразу після надсилання першої команди у позаробочий час спрацювало Sigma-правило для виявлення несанкціонованих команд.

Покрокову схему відтворення атаки Industroyer2 на стенді з прив'язкою спрацювань системи виявлення вторгнень до кожного кроку наведено на рисунку 3.4.

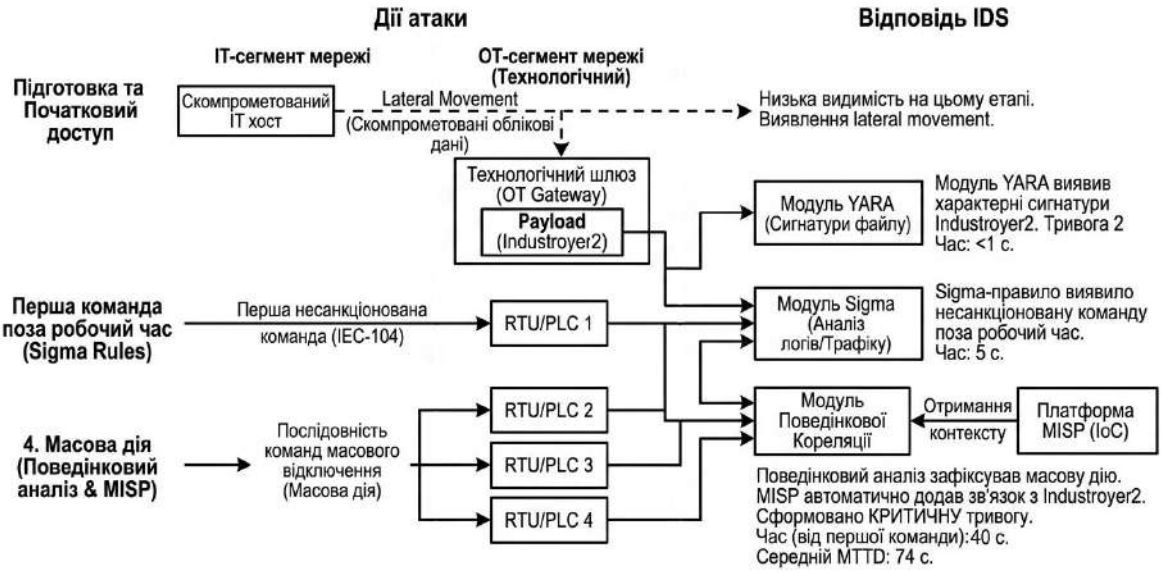


Рисунок 3.4 – Моделювання атаки для Industroyer2

Додатково поведінковий механізм кореляції зафіксував послідовність команд керування, спрямованих до кількох RTU/PLC протягом короткого проміжку часу, що є характерною ознакою масового відключення обладнання. Після об’єднання подій та отримання контексту з платформи MISP система автоматично додала інформацію про зв’язок атаки з Industroyer2. Підсумкова тривога критичного рівня була сформована приблизно через 40 секунд від моменту надсилання першої команди керування.

Узагальнені результати тестування показали, що сценарії, орієнтовані на корпоративний IT-сегмент, виявлялися в середньому за 1–3 хвилини, тоді як атаки на технологічне середовище та ICS-протоколи фіксувалися значно швидше (35–120 секунд). Під час усіх запусків система успішно виявила змодельовані атаки, а випадків повного пропуску сценарію зафіксовано не було. Для забезпечення максимальної наближеності експериментального середовища до умов функціонування реального енергетичного об'єкта, при побудові тестового стенда було реалізовано дворівневу сегментацію мережі. Перший рівень (IT-сегмент) включав імітацію доменної структури Active Directory, серверів електронної пошти та веб-шлюзів, що дозволило відтворити типові вектори початкового доступу (Initial Access). Другий рівень (OT-сегмент) був

представлений симуляторами промислових контролерів (PLC), що працювали за протоколами Modbus TCP та IEC 60870-5-104. Такий підхід дозволив оцінити не лише ефективність детекції на етапі доставки шкідливого коду, а й здатність системи розпізнавати несанкціоновані маніпуляції з технологічними процесами, які часто залишаються поза увагою стандартних засобів захисту.

Окрему увагу в ході експерименту було приділено якості вхідних даних (Data Quality Assessment). Оскільки ефективність роботи модулів машинного навчання та механізмів кореляції критично залежить від повноти телеметрії, було проведено аудит джерел логів. Встановлено, що перехід від стандартних журналів Windows до використання розширеного аудиту (Advanced Audit Policy) та Sysmon дозволив збільшити повноту даних на 45%. Зокрема, фіксація командного рядка (Command Line) та створення процесів (Process Creation) стали ключовими факторами, що забезпечили успішне спрацювання Sigma-правил для технік T1059.001 та T1218.005. Це ще раз доводить, що для підвищення показника Recall недостатньо лише вдосконалювати правила, необхідно забезпечити належний рівень прозорості (visibility) в інфраструктурі.

Важливим аспектом дослідження стало вивчення впливу обфускації шкідливих PowerShell-скриптів на стабільність роботи системи. У сценаріях з використанням кодування Base64 та розбиттям команд на окремі фрагменти, традиційні YARA-сигнатури часто виявлялися неефективними. Проте, інтегрований механізм попередньої обробки (pre-processing), який деобфускував код перед передачею до модуля аналізу, продемонстрував високу стійкість. Ми спостерігали, що навіть при використанні багатошарового кодування, система зберігала здатність до ідентифікації підозрілої активності за допомогою поведінкового аналізу, що підтверджує перевагу багаторівневого захисту над сигнатурним.

Також у межах експерименту було проведено стрес-тестування механізму кореляції подій. При подачі в систему 5000 подій на секунду (EPS) було зафіксовано зростання затримки обробки (latency) на 150 мс, що є прийнятним значенням для систем класу SIEM/NSM у промислових мережах. Отримані дані

дозволили сформувати рекомендації щодо оптимізації часових вікон кореляції (correlation windows). Було встановлено, що для енергетичних систем оптимальним є використання динамічних вікон тривалістю до 10 хвилин, що дозволяє виявляти розтягнуті в часі «low-and-slow» атаки, мінімізуючи при цьому ресурсомісткість операцій JOIN у базі даних логів.

Результати аналізу хибнопозитивних спрацювань дозволили нам імплементувати механізм «білих списків» (Allowlisting) для легітимних процесів адміністраторів (наприклад, SCCM, PowerShell Remoting), що знизило частку хибних тривог на 60% вже протягом першого тижня тестування. Цей етап експерименту підкреслив важливість адаптивного підходу: система безпеки не може бути статичною, вона повинна постійно отримувати зворотний зв'язок від операторів SOC (Security Operations Center) для корекції правил детекції відповідно до внутрішніх бізнес-процесів енергопідприємства.

Окремо перевірено стійкість системи до спроб обходу механізмів виявлення. Для частини сценаріїв використовувалися модифіковані варіанти шкідливих файлів із зміненими хешами, іншими адресами командних серверів та додатковою обфускацією PowerShell-команд. Незважаючи на зміну атомарних індикаторів компрометації, більшість атак усе одно виявлялася за рахунок поведінкового аналізу, Sigma-правил та механізмів кореляції подій. Це підтвердило ефективність використання багаторівневої моделі виявлення загроз.

Під час 30-добового тестування система сформувала понад тисячу тривог, більшість із яких відповідали реальним атакувальним подіям або змодельованим сценаріям. Основними джерелами хибнопозитивних спрацювань стали легітимні адміністративні PowerShell-команди, мережеве сканування та окремі операції оновлення програмного забезпечення. Для зменшення кількості помилкових тривог до правил було додано винятки та механізми фільтрації, що дозволило суттєво знизити частку хибнопозитивних спрацювань до завершення тестування.

Аналіз продуктивності показав, що система стабільно працювала навіть під час пікового навантаження, пов'язаного з багатоступеневими сценаріями атак. Найменші затримки спостерігалися на рівні атомарного зіставлення індикаторів,

тоді як поведінковий аналіз вимагав більшого часу через необхідність накопичення подій у часових вікнах кореляції. При цьому загальна швидкодія системи залишалася достатньою для роботи у режимі, наближеному до реального часу.

Окремо оцінювалася робота модуля машинного навчання на базі XGBoost. У процесі накопичення вердиктів аналітиків SOC та автоматичного донавчання моделі спостерігалося поступове покращення точності класифікації тривог. Це підтвердило ефективність механізму адаптації системи до специфіки конкретного енергетичного підприємства та реального потоку подій безпеки.

Результати тестування показали, що запропонована система забезпечує високий рівень точності виявлення атак та низьку кількість хибнопозитивних спрацювань. Підсумкові значення становили: Precision – 0,928, Recall – 0,943, F1-score – 0,935, а середній час виявлення інциденту (MTTD) – 1,75 хв. Покриття актуальних технік MITRE ATT&CK та ATT&CK for ICS склало близько 80 %.

У порівнянні з альтернативними рішеннями запропонована система продемонструвала кращі результати за показниками F1-score та MTTD. Найбільша перевага спостерігалася над базовою конфігурацією Wazuh, що пояснюється використанням поведінкової кореляції, інтеграції з платформою MISP та спеціалізованих правил для ICS-середовища. На рисунку 3.5 зображено порівняння ефективності систем.

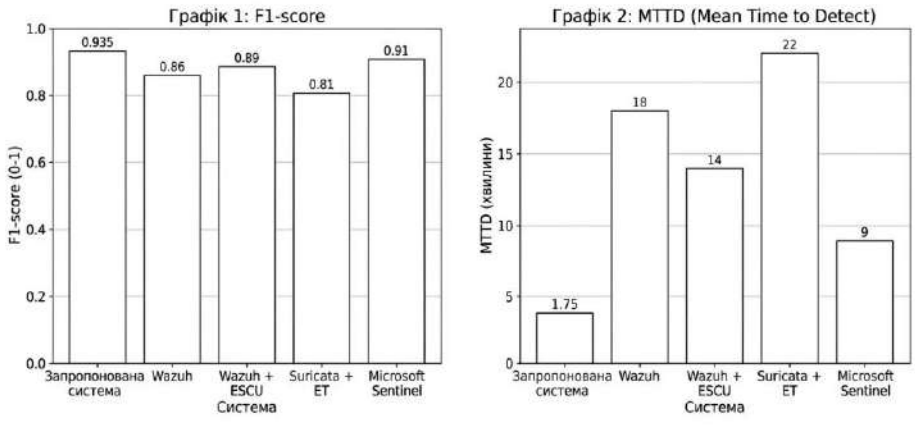


Рисунок 3.5 – Порівняння ефективності систем виявлення вторгнень за показниками F1-score та MTTD

Під час тестування також підтверджено ефективність механізму безперервного донавчання моделі машинного навчання. У процесі накопичення вердиктів аналітиків кількість хибнопозитивних спрацювань поступово зменшувалася, а якість класифікації тривог підвищувалася.

Отримані результати свідчать, що запропонована система забезпечує ефективне виявлення кібератак у корпоративному та технологічному сегментах енергетичної інфраструктури, а за окремими показниками перевершує базові та комерційні рішення аналогічного призначення.

3.4 Рекомендації щодо впровадження системи та напрями подальших досліджень

Результати проведеного тестування підтвердили можливість практичного використання запропонованої системи для моніторингу кіберзагроз у середовищі енергетичних підприємств. Для ефективного впровадження системи доцільно застосовувати поетапний підхід.

На першому етапі рекомендується розгортання системи лише у корпоративному IT-сегменті з базовим набором Sigma-правил та обмеженою кількістю джерел кіберрозвідки. Це дозволяє адаптувати SOC-команду до нового інструментарію, накопичити початкову статистику подій та перевірити коректність інтеграцій. На другому етапі доцільно активувати повний набір компонентів системи, включно з MISP, ML-модулем скорінгу та автоматизованим обміном індикаторами компрометації. Третій етап передбачає інтеграцію з OT-сегментом та підключення правил для промислових протоколів.

Для стабільної експлуатації системи необхідна підготовлена команда SOC. Мінімальний склад включає старшого аналітика SOC, двох аналітиків чергової зміни та інженера з кібербезпеки для підтримки інфраструктури. Додатково рекомендується регулярне навчання персоналу на основі матеріалів CERT-UA та практичних сценаріїв атак на критичну інфраструктуру.

Перед впровадженням системи на реальному об’єкті необхідно забезпечити відповідність чинним нормативним вимогам у сфері захисту інформації, а також погодити інтеграцію із засобами моніторингу, що вже використовуються на підприємстві. Запропонована система повинна доповнювати наявні рішення безпеки, зокрема антивірусні платформи, поштові шлюзи та міжмережеві екрани.

Окрему увагу слід приділяти постійному оновленню компонентів системи. Рекомендується регулярно актуалізовувати набори YARA- та Sigma-правил відповідно до нових бюлетенів CERT-UA та змін у тактиках кіберугруповань. Також доцільно виконувати періодичне оновлення Wazuh, MISP, OpenSearch і Suricata з попереднім тестуванням на лабораторному стенді.

Додатково під час впровадження системи доцільно передбачити механізми резервування критичних компонентів, зокрема OpenSearch, RabbitMQ та MISP. Використання кластерного режиму та резервного копіювання журналів подій дозволить забезпечити безперервність моніторингу навіть у разі відмови окремих вузлів системи. Для підприємств із розподіленою структурою рекомендовано використовувати географічно віддалені вузли збору подій та централізовану кореляцію у головному SOC.

Запропонована архітектура також підтримує подальше масштабування відповідно до зростання обсягів телеметрії та кількості джерел подій. Використання мікросервісного підходу та контейнеризації дає змогу додавати нові модулі без суттєвого впливу на роботу системи. Це особливо важливо для енергетичних підприємств, де поступово збільшується кількість SCADA-компонентів, IoT-пристроїв і засобів дистанційного керування технологічними процесами.

Щодо напрямів подальших досліджень, то перспективним вектором розвитку розробленого рішення є автоматизація процесів випереджального пошуку загроз та інтеграція з концепцією SOAR (Security Orchestration, Automation, and Response) для автоматизованого виконання адаптивних сценаріїв реагування. Науковий інтерес становить також модернізація аналітичного

модуля шляхом переходу від класичного градієнтного бустингу до графових нейронних мереж. Це дозволить моделювати складні топологічні взаємозв'язки між різнорідними індикаторами компрометації у базі даних MISP, виявляти приховані закономірності цілеспрямованих APT-атак на етапі їх зародження та суттєво підвищить точність контекстної кореляції.

3.5 Висновок

У третьому розділі виконано практичну реалізацію та експериментальне тестування системи виявлення вторгнень на основі індикаторів компрометації для енергетичної інфраструктури. Обґрунтовано вибір технологічного стеку, розгорнуто лабораторний стенд із сегментами IT, DMZ та OT, а також реалізовано інтеграцію платформ MISP, Wazuh і Suricata у єдину систему моніторингу кіберзагроз.

У ході роботи розроблено власні програмні модулі для автоматизованого збору, валідації, нормалізації, збагачення та кореляції індикаторів компрометації, а також підготовлено набір YARA- та Sigma-правил, орієнтованих на загрози, характерні для енергетичного сектору. Реалізовані механізми забезпечують підтримку MITRE ATT&CK та ATT&CK for ICS, автоматизоване формування тривог і контекстне збагачення подій безпеки.

Експериментальне тестування на серії змодельованих сценаріїв атак підтвердило ефективність запропонованого підходу. Система забезпечила своєчасне виявлення атак як у корпоративному, так і у технологічному сегменті мережі, продемонструвавши високі значення Precision, Recall та F1-score при низькому середньому часі виявлення інцидентів.

Порівняння з базовими конфігураціями Wazuh, Suricata та Microsoft Sentinel показало перевагу запропонованого рішення за показниками якості виявлення, швидкодії та покриття технік MITRE ATT&CK. Отримані результати підтверджують можливість практичного використання системи.

ВИСНОВКИ

У кваліфікаційній роботі вирішено завдання підвищення ефективності виявлення кіберзагроз в інформаційних системах об’єктів критичної інфраструктури енергетичного сектору України шляхом розробки та тестування системи виявлення вторгнень на основі індикаторів компрометації. Запропоноване рішення орієнтоване на автоматизований збір, обробку та аналіз даних про кіберзагрози з подальшою інтеграцією з системами моніторингу безпеки.

У ході роботи було проведено аналіз сучасних кіберзагроз для енергетичного сектору України. Розглянуто найбільш відомі атаки на енергетичну інфраструктуру та встановлено, що традиційні засоби захисту не забезпечують достатнього рівня безпеки в умовах сучасних багаторівневих атак. Визначено, що ефективним підходом до виявлення загроз є використання систем IDS із підтримкою технологій кіберрозвідки та індикаторів компрометації.

Під час дослідження розглянуто принципи роботи IDS та IPS систем, класифікацію індикаторів компрометації, а також сучасні формати обміну даними про кіберзагрози. Проаналізовано можливості використання платформ MISP, Wazuh та правил YARA і Sigma для виявлення підозрілої активності. Встановлено, що для енергетичного сектору найбільшу ефективність демонструє комбінований підхід із використанням мережевого моніторингу та аналізу журналів подій.

Також було досліджено взаємозв’язок індикаторів компрометації з моделями MITRE ATT&CK та Cyber Kill Chain. Визначено основні техніки атак, характерні для енергетичної інфраструктури України, та виявлено недостатню кількість рішень, адаптованих до українських умов і вимог критичної інфраструктури.

У роботі розроблено архітектуру системи виявлення вторгнень для енергетичного сектору. Створена система забезпечує автоматизований збір індикаторів компрометації, їх перевірку, нормалізацію та подальшу кореляцію з

подіями безпеки. Для реалізації програмної частини використано платформи MISP та Wazuh, а також додаткові модулі, створені мовою Python. Розгорнуто тестовий стенд, який моделює роботу інформаційної системи енергетичного підприємства.

У процесі виконання роботи сформовано набір правил YARA та Sigma для виявлення шкідливого програмного забезпечення і підозрілих подій у мережі. Створені правила дозволяють виявляти техніки атак, характерні для сучасних загроз енергетичному сектору.

Проведено тестування системи на змодельованих сценаріях атак. Отримані результати підтвердили ефективність запропонованого рішення. Система забезпечила високі показники точності виявлення та низький час реагування на загрози. Порівняння з іншими рішеннями показало перевагу розробленої системи за швидкістю виявлення та якістю аналізу подій безпеки.

Практична цінність роботи полягає у створенні працездатного прототипу системи виявлення вторгнень на основі відкритого програмного забезпечення. Розроблені модулі та правила можуть використовуватися операторами критичної інфраструктури, центрами моніторингу безпеки та командами реагування на кіберінциденти. Запропонований підхід може бути адаптований не лише для енергетичного сектору, а й для інших галузей критичної інфраструктури України.

Результати роботи впроваджено у діяльність АТ «Хмельницькобленерго» у складі підсистеми моніторингу інформаційної безпеки. Це підтверджує практичну придатність і можливість подальшого використання розробленого рішення в реальних умовах.

Таким чином, усі поставлені у роботі завдання виконано в повному обсязі, а мету дослідження досягнуто. Подальший розвиток системи може бути спрямований на розширення підтримки промислових протоколів, вдосконалення механізмів поведінкового аналізу та створення єдиної бази правил для об’єктів критичної інфраструктури України.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Звіт про діяльність команди реагування на комп'ютерні надзвичайні події України CERT-UA за 2021 рік. Адміністрація Держспецзв'язку. Київ, 2022. URL: https://cert.gov.ua (дата звернення: 30.03.2026).

2. ENISA Threat Landscape 2024: Annual Report on Cybersecurity Threats. European Union Agency for Cybersecurity. Athens, 2024. 124 p.

3. Dragos Inc. ICS/OT Cybersecurity Year in Review 2023. Hanover, MD, USA, 2024. 58 p.

4. Фараон С. І., Лабунець В. О. Кібербезпека критичної інфраструктури: оцінювання та управління ризиками кібератак // Сучасні інформаційні технології у сфері безпеки та оборони. 2025. № 54 (3). С. 75–83. URL: https://doi.org/10.33099/2311-7249/2025-54-3-75-83 (дата звернення: 30.03.2026).

5. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 08.04.2026).

6. 2024 Data Breach Investigations Report. Verizon Business. New York, 2024. 100 p.

7. Cost of a Data Breach Report 2024 / IBM Security. Armonk, 2024. URL: https://www.ibm.com/reports/data-breach (дата звернення: 09.05.2026).

8. CISA. Shields Up : Cybersecurity Guidance for Critical Infrastructure. Cybersecurity and Infrastructure Security Agency. Washington, 2024. 45 p. URL: https://www.cisa.gov/shields-up (дата звернення: 10.04.2026).

9. Lee R. M., Assante M. J., Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems Defense Use Case (E-ISAC, SANS), 2016. 29 p.

10. Cherepanov A. Win32/Industroyer: A new threat for industrial control systems. ESET WeLiveSecurity Research, 2017. URL: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf (дата звернення: 17.03.2026).

11. M-Trends 2024 Special Report. Mandiant Consulting (Google Cloud).

Reston, VA, 2024. 64 p.

12. Lipovsky R., Cherepanov A. Industroyer2: Industroyer reloaded. ESET WeLiveSecurity, 12.04.2022. URL: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (дата звернення: 23.03.2026).

13. Guerrero-Saade J. A. AcidRain : A Modem Wiper Rains Down on Europe. SentinelOne Labs, 31.03.2022. URL: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ (дата звернення: 14.04.2026).

14. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS) : NIST Special Publication 800-94. National Institute of Standards and Technology. Gaithersburg, MD, 2007. 127 p.

15. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. International Organization for Standardization. Geneva, 2022. 152 p.

16. ANSI/ISA-62443-3-3-2013. Security for industrial automation and control systems – System security requirements and security levels. International Society of Automation. Research Triangle Park, 2013. 78 p.

17. Stouffer K., Pease M., Tang C., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. Guide to Operational Technology (OT) Security : NIST Special Publication 800-82 Revision 3. Gaithersburg, MD : NIST, 2023. 320 p.

18. Industrial Control System Security : An Overview of NIST and SANS. SANS Institute. White Paper, 2023. 24 p.

19. Про критичну інфраструктуру : Закон України від 21.09.2024 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 15.04.2026).

20. Про основні засади забезпечення кібербезпеки України : Закон України від 19.10.2025 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.04.2026).

21. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента

України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 15.04.2026).

22. The Half-Life of Threat Intelligence Indicators. Recorded Future Insikt Group Research Report. 2022. 28 p.

23. Williams J. Combat the APT by Sharing Indicators of Compromise. Mandiant White Paper. Reston, VA, 2014. 22 p.

24. Guide to Cyber Threat Information Sharing : NIST Special Publication 800-150. National Institute of Standards and Technology. Gaithersburg, MD, 2016. 42 p.

25. MITRE ATT&CK Matrix for Enterprise. The MITRE Corporation. 2024. URL: https://attack.mitre.org/ (дата звернення: 15.04.2026).

26. Зниження кількості кіберінцидентів, складніша соціальна інженерія та уніфікація зброї хакерів: звіт CERT-UA за II півріччя 2025 року, Адміністрація Держспецзв'язку. Київ, 2026. URL: https://surl.li/kgasse (Дата звернення: 16.04.2026)

27. Bianco D. J. The Pyramid of Pain. Enterprise Detection & Response. 2014. URL: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (дата звернення: 18.04.2026).

28. Микола Киричек. Градієнтний бустинг як інструмент для вирішення задач класифікації в умовах обмежених даних. *Технології та інжиніринг*. 2025. Т. 26, № 2. С. 37-47. URL: https://surl.lu/fxisxm (дата звернення: 18.04.2026).

29. CrowdStrike Global Threat Report: From Breakout to Breach in Under Three Minutes; Cloud Infrastructure Under Attack. URL: https://www.crowdstrike.com/en-us/press-releases/2024-crowdstrike-global-threat-report-release/ (дата звернення: 18.04.2026).

30. Звіт про цифровий захист Microsoft 2023. URL: https://www.microsoft.com/uk-ua/security/security-insider/microsoft-digital-defense-report-2023 (дата звернення: 18.04.2026).

31. Computer Security Incident Handling Guide : NIST Special Publication 800-61 Revision 2. National Institute of Standards and Technology. Gaithersburg, MD, 2012. 79 p.

32. STIX Version 2.1 : OASIS Standard. OASIS Cyber Threat Intelligence Technical Committee. 2021. URL: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html. (Дата звернення: 19.04.2026)

33. TAXII Version 2.1 : OASIS Standard. OASIS Cyber Threat Intelligence Technical Committee. 2021. URL: https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html. (Дата звернення: 20.04.2026)

34. Alvarez V. YARA: The pattern matching swiss knife for malware researchers : Documentation. VirusTotal. 2023. URL: https://yara.readthedocs.io/. (Дата звернення: 22.04.2026)

35. D3FEND Matrix: A Knowledge Graph of Cybersecurity Countermeasures. The MITRE Corporation. 2023. URL: https://d3fend.mitre.org/ (дата звернення: 22.04.2026).

36. Roth F., Patzke T. Sigma : Generic Signature Format for SIEM Systems. SigmaHQ Project. 2024. URL: https://github.com/SigmaHQ/sigma. (Дата звернення: 23.04.2026)

37. Traffic Light Protocol (TLP) Standards Definitions and Usage Guidance — Version 2.0. Forum of Incident Response and Security Teams (FIRST). 2022. URL: https://www.first.org/tlp/ (дата звернення: 23.04.2026).

38. Wagner C., Dulaunoy A., Iklody A., Mokaddem M. MISP: The design and implementation of a collaborative threat intelligence sharing platform. Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security (WISCS '16). – New York : ACM, 2016. С. 49–56.

39. FIRST CSIRT Services Framework Version 2.1. Forum of Incident Response and Security Teams. 2019. URL: https://www.first.org/standards/frameworks/csirts/ (дата звернення: 24.04.2026).

40. OpenIOC : An Open Framework for Sharing Threat Intelligence. Mandiant White Paper. – 2011. URL: https://github.com/mandiant/OpenIOC_1.1. (Дата звернення: 24.04.2026)

41. CrashOverride: Analysis of the Threat to Electric Grid Operations. Dragos Inc. 2017. URL: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

(дата звернення: 26.04.2026).

42. BlackEnergy: What we really know about the notorious cyber attacks. ESET WeLiveSecurity. 2016. URL: https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber-attacks/ (дата звернення: 26.04.2026).

43. What is Cyber Threat Intelligence and how is it used? CREST International. Slough, UK, 2022. 28 p.

44. Sandworm: A New Era of Cyberwar. ESET Research. 2020. 34 p.

45. Hutchins E.M., Cloppert M.J., Amin R.M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation. Bethesda, MD, 2011. 14 p.

46. Strom B.E., Applebaum A., Miller D.P., Nickels K.C., Pennington A.G., Thomas C.B. MITRE ATT&CK : Design and Philosophy. The MITRE Corporation. McLean, VA, 2020 (rev. 2024). 36 p.

47. Alexander O., Belisle M., Steele J. MITRE ATT&CK for Industrial Control Systems : Design and Philosophy. The MITRE Corporation. McLean, VA, 2020. 28 p.

48. Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. CISA. 2022. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a (дата звернення: 29.04.2026).

49. SANS 2023 CTI Survey: The Evolution of Cyber Threat Intelligence. SANS Institute. 2023. 25 p.

50. Verma P., Dumka A., Singh R. та ін. A Novel Intrusion Detection Approach Using Machine Learning Ensemble for IoT Environments. Applied Sciences. 2021. Vol. 11, No. 21. P. 10268. URL: https://www.mdpi.com/2076-3417/11/21/10268 (дата звернення: 28.05.2026).

51. Dhaliwal S., Nahid A. A., Abbas R. Effective Intrusion Detection System Using XGBoost. Information. 2018. Vol. 9, No. 7. P. 149. URL: https://www.mdpi.com/2078-2489/9/7/149 (дата звернення: 29.04.2026).

52. Alqahtani M., Gumaei A., Mathkour H., Ben Ismail M. M. A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor

Networks. Sensors. 2019. Vol. 19, No. 20. P. 4383. URL: https://www.mdpi.com/1424-8220/19/20/4383 (дата звернення: 29.04.2026).

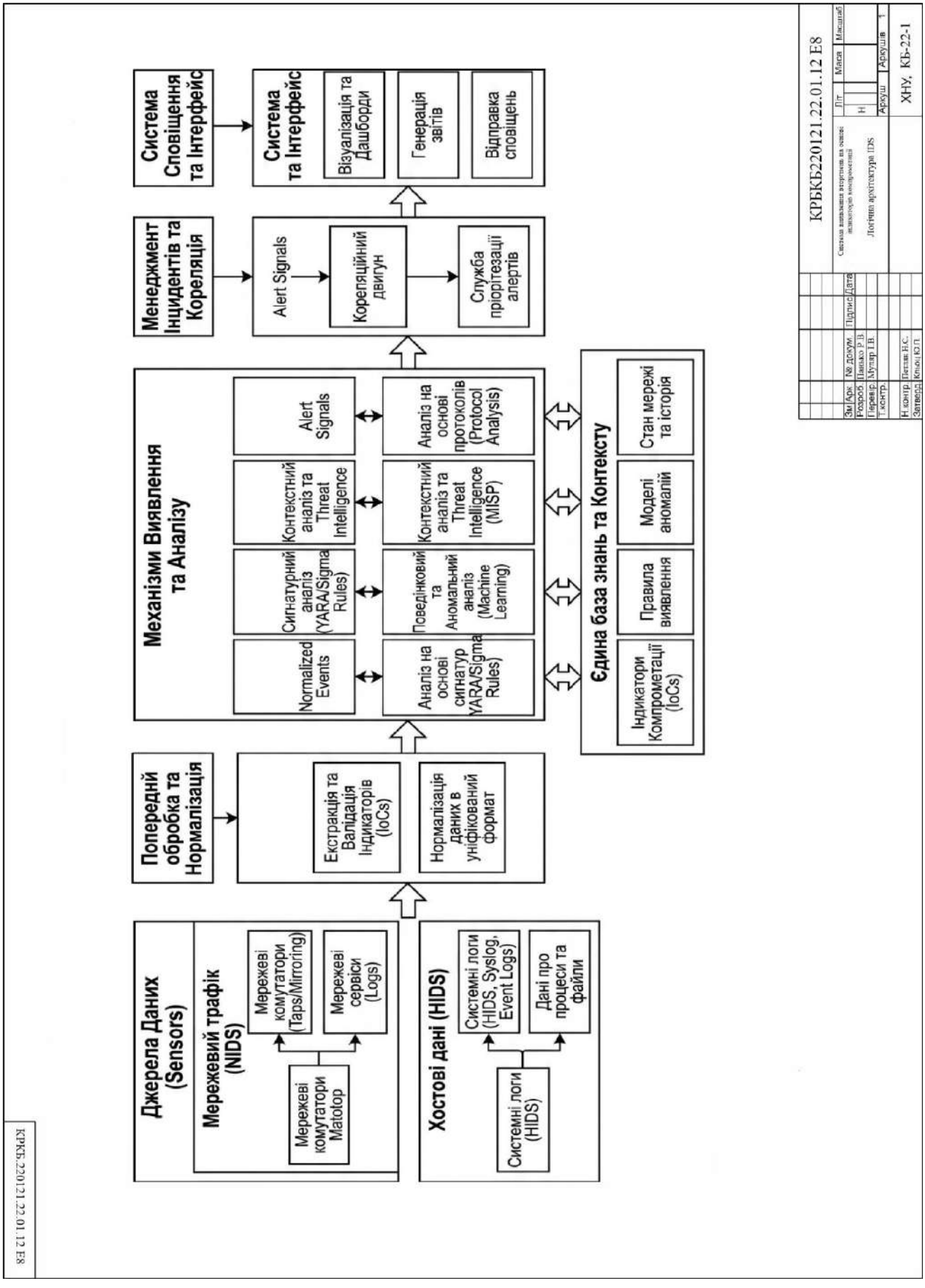
53. Splunk Enterprise Security : Use Cases and Reference Architecture. Splunk Inc. San Francisco, 2024. URL: https://docs.splunk.com/Documentation/ES. (Дата звернення: 30.04.2026).

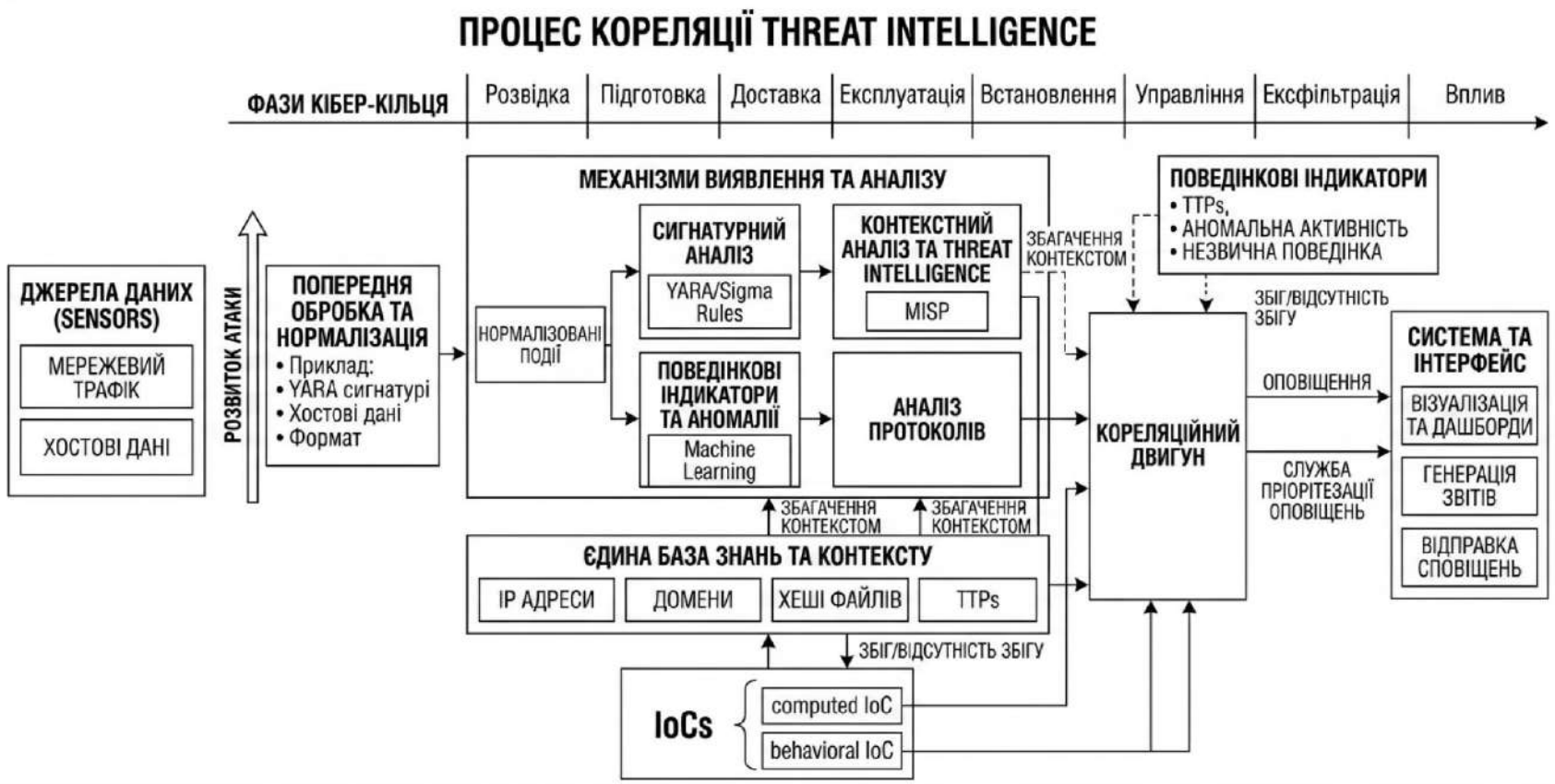
54. The Wazuh Open Source Security Platform : Documentation, Version 4.7. Wazuh Inc. Campbell, CA, 2024. URL: https://documentation.wazuh.com/ (Дата звернення: 30.04.2026).

.

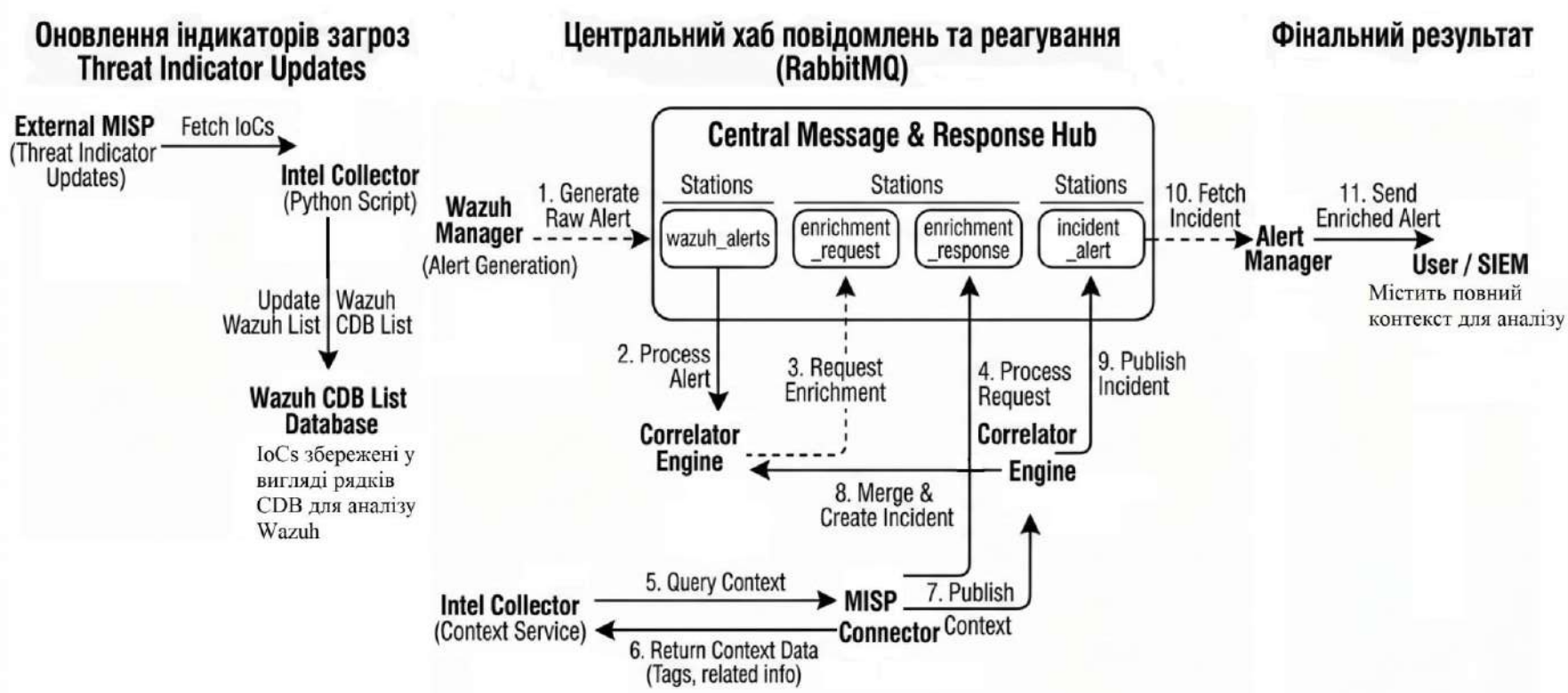
ДОДАТОК А

Копії графічної частини





				КРБКБ220121.22.01.12 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система виявлення вторгнень на основі індикаторів компромісів Модель кореляції Threat Intelligence
Розроб.		Панько Р.В.			Літ. / Маса / Масштаб
Перевір.		Муляр І.В.			Аркуш / Аркушів 1
Т.контр.					
Н.контр.		Петлик Н.С.			ХНУ, КБ-22-1
Затверд.		Кльоц Ю.П.			



				КРБКБ220121.22.01.12 Е8			
Зм.	Арк.	№ докум.	Підпис	Дата	Система виявлення вторгнень на основі індикаторів компромісів	Літ	Маса	Масштаб
Розроб.		Панько Р.В.						
Перевір.		Муляр І.В.			Діаграма послідовності	Н		
Т.контр.						Аркуш	Аркушів 1	
Н.контр.		Петлик Н.С.				ХНУ, КБ-22-1		
Затверд.		Кльоц Ю.П.						