Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:
ТЕХНОЛОГІЯ МОНІТОРИНГУ БЕЗПЕКИ ЗА ДОПОМОГОЮ ЗАСОБІВ SIEM

Виконав

студент групи БІКСм-1-25-1.4д

Завражний Богдан Едуардович
(прізвище, ім'я, по батькові)

_____
(підпис)

Науковий керівник

Кандидат технічних наук, доцент
(науковий ступінь, наукове звання)

Складанний Павло Миколайович
(прізвище, ініціали)

_____
(підпис)

Київ – 2025

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Завражному Богдану Едуардовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Технологія моніторингу безпеки за допомогою засобів SIEM;
керівник к.т.н., доц. Складанний Павло Миколайович
затверджені наказом ректора від «___»_____ 20___ року №__.
2. Термін подання студентом роботи «___»_____ 20___ р.
3. Вихідні дані до роботи:

3.1 науково-технічна та нормативна література з теми дослідження: науково-технічні праці - 55; нормативна література: ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO/IEC 27005:2022 — Information security risk management, ISO/IEC 22301:2019 — Security and resilience — Business continuity management systems, NIST SP 800-61 Rev. 2 — Computer Security Incident Handling Guide, NIST SP 800-207 — Zero Trust Architecture, NIST SP 800-137 — Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, Закон України "Про основні засади забезпечення кібербезпеки України" №2163-VIII від 05.10.2017, Закон України "Про інформацію", Постанова КМУ №518 від 19.06.2019 — Про затвердження Порядку забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури;

3.2 методи: Аналіз і синтез, порівняльний аналіз, системний підхід, декомпозиція, сценарний аналіз, статистичний аналіз (MTTD, MTTR), багатокритеріальна оцінка, імітаційне моделювання, методи машинного навчання, математичне формалізування процесів, візуалізаційний аналіз;

3.3 технології: SIEM, SOAR, SOC, Zero Trust Architecture, Splunk Enterprise, Wazuh, Elastic Stack, Flask, REST API, Alert Manager, Dashboard Analytics;

3.4 алгоритми: кореляційні правила, евристичні пороги, статистичне виявлення аномалій;

3.5 мова програмування: Python, SQL, JavaScript;

3.6 математичні моделі та методи: модель потоку подій безпеки, модель ймовірності виявлення інцидентів, модель аномалій на основі статистичних відхилень, модель класифікації

подій за ознаками, модель оцінки ризику інформаційної безпеки, модель оптимізації реагування на інциденти, кореляційна модель подій у SIEM (виявлення залежностей між джерелами логів).

4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):

4.1. Проаналізувати сучасний стан, тенденції розвитку та методологічні основи моніторингу інформаційної безпеки підприємства, визначити ключові принципи побудови систем спостереження та контролю інцидентів безпеки..

4.2. Дослідити нормативно-правову, технічну та наукову базу моніторингу інформаційної безпеки, зокрема міжнародні стандарти ISO/IEC 27001, ISO/IEC 27035, ISO/IEC 27005, NIST SP 800-61 і законодавчі акти України у сфері кібербезпеки.

4.3. Розглянути архітектуру, функціональні можливості та принципи роботи сучасних систем SIEM, визначити їх роль у забезпеченні комплексного моніторингу подій інформаційної безпеки підприємства.

4.4. Розробити концептуальну модель системи моніторингу інформаційної безпеки підприємства, визначити її структурні елементи, взаємодію між компонентами та потоки даних, що реалізують процес виявлення й оброблення інцидентів.

4.5. Сформувати математичну модель процесів моніторингу інформаційної безпеки, яка враховує ймовірнісні, статистичні та нечіткі методи оцінювання подій, а також визначити критерії ефективності та надійності системи.

4.6. Реалізувати прототип системи моніторингу інформаційної безпеки із використанням SIEM-платформи (Splunk, Wazuh або Elastic Stack), провести моделювання та тестування сценаріїв атак, сформувати правила кореляції подій.

4.7. Оцінити ефективність функціонування розробленої системи моніторингу за допомогою кількісних метрик (MTTD, MTTR), узагальнити результати дослідження та сформулювати висновки і рекомендації щодо підвищення рівня інформаційної безпеки підприємства.

5. Перелік графічного матеріалу:

5.1 Презентація доповіді, виконана в Microsoft PowerPoint.

5.2 Типові схеми: рисунків - 37.

6. Дата видачі завдання «___»_____ 20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання		
2.	Аналіз літератури		
3.	Обґрунтування вибору рішення		
4.	Збір даних		
5.	Виконання та оформлення розділу 1.		
6.	Виконання та оформлення розділу 2.		
7.	Виконання та оформлення розділу 3.		
8.	Вступ, висновки, реферат		
9.	Апробація роботи на науково-методичному семінарі та/або науково-технічній конференції		
10.	Оформлення та друк текстової частини роботи		
11.	Оформлення презентацій		
12.	Отримання рецензій		
13.	Попередній захист роботи		
14.	Захист в ЕК		

Студент _____ Завражний Богдан Едуардович
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Складанний Павло Миколайович
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню, аналізу та розробці технології моніторингу інформаційної безпеки з використанням засобів SIEM (Security Information and Event Management), спрямованої на підвищення рівня захищеності інформаційних ресурсів підприємства та ефективності реагування на інциденти безпеки.

Робота складається зі вступу, трьох розділів, що містять 37 рисунків та 4 таблиць, висновків, списку використаних джерел, що містить 55 найменувань. Загальний обсяг роботи становить 101 аркушів, а також додатки, перелік умовних скорочень.

Об'єктом дослідження є процес моніторингу стану інформаційної безпеки підприємства із застосуванням технологій збору, аналізу та кореляції подій безпеки в системах SIEM.

Предметом дослідження є моделі, методи та механізми побудови технології моніторингу інформаційної безпеки із використанням засобів SIEM, що забезпечують автоматизований збір, обробку, кореляцію та аналіз подій безпеки в інформаційно-комунікаційних системах підприємства.

Метою роботи є дослідження та розроблення технології моніторингу інформаційної безпеки із використанням засобів SIEM, яка забезпечує централізований збір, аналіз і кореляцію подій безпеки, сприяє своєчасному виявленню інцидентів, зниженню рівня кіберризиків, підвищенню ефективності реагування на загрози та формуванню інтелектуальної системи підтримки рішень у сфері управління інформаційною безпекою підприємства.

Для досягнення поставленої мети у роботі: проведено комплексне дослідження сучасних методів і технологій моніторингу інформаційної безпеки, здійснено аналіз архітектури, функціональних можливостей та принципів роботи SIEM-систем, розроблено модель процесів збору, нормалізації, кореляції та аналізу подій безпеки, запропоновано методику формування правил виявлення інцидентів на основі поведінкових характеристик та аналітики журналів подій, а також реалізовано експериментальне впровадження запропонованої технології у

тестовому середовищі з оцінкою ефективності за ключовими метриками (MTTD, MTTR, FPR, TPR).

Крім того, у роботі обґрунтовано вибір інструментальних засобів реалізації SIEM-моніторингу, зокрема платформ Wazuh та ELK Stack, проведено налаштування збору даних із різних джерел подій, побудовано дашборди для візуалізації інцидентів і стану безпеки, а також розроблено рекомендації щодо інтеграції SIEM у корпоративне середовище та подальшого розширення системи до рівня SOC/SOAR-платформи.

Наукова новизна одержаних результатів. Новими науково-обґрунтованими результатами, які отримані в роботі, є розроблення математичної моделі процесу моніторингу інформаційної безпеки із використанням засобів SIEM, що формалізує взаємозв'язки між подіями, джерелами, активами та ризиками з урахуванням їх часових імовірнісних характеристик. Удосконалено методи кореляції подій безпеки шляхом інтеграції правилового, поведінкового та статистичного аналізу, що дозволяє підвищити точність виявлення інцидентів і зменшити кількість хибних спрацьовувань. Створено технологічну модель SIEM-моніторингу, яка забезпечує адаптивне управління потоками подій, оптимізацію процесів збору, нормалізації та обробки даних, а також формування аналітичних звітів у режимі реального часу. Обґрунтовано ефективність впровадження запропонованої технології шляхом експериментальної перевірки її роботи на базі відкритих SIEM-платформ Wazuh та ELK Stack із використанням метрик MTTD, MTTR, TPR і FPR. Крім того, розроблено рекомендації щодо інтеграції SIEM у корпоративну інфраструктуру підприємства та побудови на її основі центру моніторингу безпеки (SOC) з можливістю подальшого розвитку до рівня автоматизованої системи реагування SOAR.

Галузь застосування. Результати роботи можуть бути використані для побудови та вдосконалення систем моніторингу інформаційної безпеки на підприємствах, в установах і організаціях різних форм власності, що мають розвинену інформаційно-комунікаційну інфраструктуру. Запропонована технологія може бути впроваджена у діяльність центрів моніторингу безпеки

(SOC), а також інтегрована в корпоративні SIEM-рішення для централізованого збору, аналізу та кореляції подій безпеки. Розроблені методичні та практичні підходи можуть бути використані під час створення систем управління інформаційною безпекою (ISMS) відповідно до стандартів ISO/IEC 27001, ISO/IEC 27035 та NIST SP 800-61, а також для проведення навчальних тренінгів з виявлення та реагування на інциденти інформаційної безпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, МОНІТОРИНГ БЕЗПЕКИ, SIEM, SOC, SOAR, КОРЕЛЯЦІЯ ПОДІЙ, ІНЦИДЕНТ БЕЗПЕКИ, АНАЛІЗ ЖУРНАЛІВ ПОДІЙ, ВИЯВЛЕННЯ ЗАГРОЗ, РЕАГУВАННЯ НА ІНЦИДЕНТИ, КІБЕРРИЗИКИ, WAZUH, ELK STACK.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AI – Artificial Intelligence — штучний інтелект

API – Application Programming Interface — програмний інтерфейс застосунку

CMDB – Configuration Management Database — база даних керування конфігураціями

CVE – Common Vulnerabilities and Exposures — загальні вразливості та експозиції

DLP – Domain Name System — система доменних імен

DNS – Identity Provider — постачальник ідентичностей

EDR – Endpoint Detection and Response — виявлення та реагування на події на кінцевих точках

GDPR – General Data Protection Regulation — Загальний регламент ЄС про захист даних

IDS/IPS – Intrusion Detection/Prevention System — система виявлення/запобігання вторгненням

ML – Machine Learning — машинне навчання

IR – Incident Response — реагування на інциденти

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission — Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісі

ITSM – IT Service Management — управління IT-послугами

JSON – JavaScript Object Notation — формат обміну даними

KPI – Key Performance Indicator — ключовий показник ефективності

SIEM – Security Information and Event Management — система моніторингу та кореляції подій безпеки

SOAR – Security Orchestration, Automation and Response — оркестрація, автоматизація та реагування на інциденти

KQL	–	Kusto Query Language — мова запитів до аналітичних систем Microsoft
MITRE ATT&CK	–	Knowledge Base of Adversary Tactics and Techniques — база знань тактик і технік противника
NIST	–	National Institute of Standards and Technology — Національний інститут стандартів і технологій (США)
NIS2	–	Network and Information Security Directive 2 — директива ЄС із мережевої та інформаційної безпеки
SQL	–	Structured Query Language — структурована мова запитів
UI/UX	–	User Interface / User Experience — інтерфейс і досвід користувача
XML	–	eXtensible Markup Language — розширювана мова розмітки

ВСТУП

У сучасних умовах цифрової трансформації підприємства активно використовують розподілені інформаційно-комунікаційні системи, хмарні сервіси та мобільні технології, що значно підвищує ризики виникнення інцидентів інформаційної безпеки. Збільшення кількості джерел подій, різноманіття форматів журналів та складність міжмережевої взаємодії призводять до того, що традиційні методи контролю безпеки не забезпечують своєчасного виявлення атак, а процес аналізу подій стає надмірно трудомістким і неефективним.

Основна проблема полягає у відсутності єдиної інтегрованої технології моніторингу, здатної централізовано збирати, нормалізувати, аналізувати та корелювати події безпеки з різних джерел у реальному часі. Недостатня автоматизація процесів обробки інформації, низький рівень адаптації до нових типів загроз і відсутність інтелектуальних механізмів реагування призводять до затримок у виявленні інцидентів, збільшення часу реагування (MTTR) та підвищення рівня кіберризику. Таким чином, постає науково-практична задача — розробити технологію моніторингу інформаційної безпеки на основі засобів SIEM, яка забезпечить підвищення оперативності виявлення інцидентів, зниження кількості хибних спрацьовувань та створення аналітичного підґрунтя для прийняття ефективних рішень у сфері кіберзахисту підприємства.

Актуальність роботи полягає в тому, що зростання кількості та складності кіберзагроз вимагає від підприємств впровадження ефективних технологій моніторингу інформаційної безпеки, здатних забезпечити своєчасне виявлення інцидентів і мінімізацію ризиків. Традиційні засоби контролю не дозволяють обробляти великі обсяги даних і швидко виявляти аномалії, що створює передумови для реалізації атак і витоку конфіденційної інформації. У цих умовах впровадження технології SIEM (Security Information and Event Management) набуває особливого значення, оскільки вона поєднує функції збору, нормалізації, аналізу та кореляції подій безпеки в реальному часі, забезпечуючи побудову інтегрованої системи моніторингу. Розроблення та вдосконалення таких технологій

є актуальним завданням як з наукової, так і з практичної точки зору, оскільки дозволяє підвищити рівень кіберзахисту підприємств, забезпечити відповідність міжнародним стандартам (ISO/IEC 27001, ISO/IEC 27035, NIST SP 800-61) і створити підґрунтя для формування сучасних центрів моніторингу безпеки (SOC) та систем автоматизованого реагування (SOAR).

Метою роботи є дослідження та розроблення технології моніторингу інформаційної безпеки із використанням засобів SIEM, яка забезпечує централізований збір, аналіз і кореляцію подій безпеки, сприяє своєчасному виявленню інцидентів, зниженню рівня кіберризиків, підвищенню ефективності реагування на загрози та формуванню інтелектуальної системи підтримки рішень у сфері управління інформаційною безпекою підприємства.

Для досягнення поставленої мети були поставлені та вирішенні такі **завдання**:

1. Проаналізувати сучасні підходи, стандарти та технології моніторингу інформаційної безпеки, визначити їх переваги, недоліки та тенденції розвитку систем класу SIEM.

2. Дослідити архітектуру, функціональні компоненти та принципи роботи SIEM-платформ, зокрема модулі збору, нормалізації, кореляції подій і генерації сповіщень.

3. Розробити математичну та інформаційну моделі процесів моніторингу безпеки, які відображають взаємозв’язки між подіями, джерелами даних, активами та рівнями ризику.

4. Створити технологічну модель SIEM-моніторингу, що забезпечує інтеграцію з елементами корпоративної інфраструктури та адаптивне управління потоками подій безпеки.

5. Розробити методику виявлення інцидентів інформаційної безпеки на основі поєднання правилових, статистичних і поведінкових методів аналізу.

6. Реалізувати експериментальне впровадження розробленої технології на базі відкритих платформ (Wazuh, ELK Stack) та налаштувати політики збору і кореляції подій.

7. Оцінити ефективність запропонованої технології моніторингу за ключовими метриками (MTTD, MTTR, TPR, FPR) і сформулювати рекомендації щодо її практичного застосування.

Об’єктом дослідження є процес моніторингу стану інформаційної безпеки підприємства із застосуванням технологій збору, аналізу та кореляції подій безпеки в системах SIEM.

Предметом дослідження є моделі, методи та механізми побудови технології моніторингу інформаційної безпеки із використанням засобів SIEM, що забезпечують автоматизований збір, обробку, кореляцію та аналіз подій безпеки в інформаційно-комунікаційних системах підприємства.

Методи дослідження. Для вирішення означених вище наукових завдань в роботі використано методи системного аналізу, математичне моделювання, ймовірнісно-статистичні методи, інформаційний та кореляційний аналіз, методи машинного навчання, поведінкова аналітика, експериментальні методи, порівняльний аналіз, моделювання інформаційних потоків, візуально-аналітичні методи.

Наукова новизна одержаних результатів. Новими науково-обґрунтованими результатами, які отримані в роботі, є: розроблення комплексної технології моніторингу інформаційної безпеки із використанням засобів SIEM, що забезпечує інтегроване керування подіями, автоматичну кореляцію та поведінковий аналіз інцидентів у режимі реального часу. Удосконалено підхід до обробки подій безпеки шляхом поєднання правилових, статистичних і машинно-навчальних методів, що дозволяє підвищити точність виявлення аномалій та зменшити кількість хибних спрацьовувань. Розроблено математичну модель процесів SIEM-моніторингу, яка враховує часові, ймовірнісні та вагові характеристики подій різної критичності, а також запропоновано метод оцінювання ефективності функціонування системи за метриками MTTD, MTTR, TPR і FPR. Отримано нові результати щодо формування адаптивної архітектури моніторингу, що забезпечує оптимальне розподілення навантаження між компонентами SIEM та створює основу для побудови центрів

моніторингу безпеки (SOC) із можливістю подальшого розвитку до рівня систем автоматизованого реагування (SOAR).

Зв'язок роботи з науковими програмами, планами, темами. Робота узгоджується з напрямами державних і галузевих програм у сфері розвитку інформаційного суспільства, цифрової трансформації та підвищення рівня кіберзахисту об'єктів критичної інфраструктури України, визначених Стратегією кібербезпеки України та Державною програмою інформатизації. Отримані результати спрямовані на вдосконалення методів і технологій моніторингу інформаційної безпеки, автоматизацію процесів виявлення та реагування на інциденти, а також підвищення ефективності функціонування систем управління інформаційною безпекою підприємств. Кваліфікаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№0122U200483, КУБГ, м. Київ).

Теоретичне та практичне значення. Нові наукові результати, отримані в роботі, мають важливе теоретичне та практичне значення для розвитку підходів до моніторингу інформаційної безпеки на основі засобів SIEM. У теоретичному аспекті робота розвиває наукові положення щодо формалізації процесів збору, нормалізації та кореляції подій безпеки, удосконалює математичні моделі оцінювання ризиків та ефективності функціонування систем моніторингу, а також обґрунтовує методологію побудови інтегрованої архітектури SIEM-моніторингу у корпоративному середовищі. Практичне значення одержаних результатів полягає у створенні технології, що забезпечує централізований моніторинг стану безпеки підприємства, підвищує рівень оперативності реагування на інциденти, знижує кількість хибних спрацьовувань та дозволяє оптимізувати роботу аналітиків у центрах моніторингу безпеки (SOC). Розроблені методи, моделі та технічні рішення можуть бути використані під час впровадження систем управління інформаційною безпекою (ISMS), створення корпоративних SIEM-рішень, а також

у навчальному процесі для підготовки фахівців з кібербезпеки, інформаційного та мережевого захисту.

Галузь застосування. Результати роботи можуть бути використані для побудови та вдосконалення систем моніторингу інформаційної безпеки на підприємствах, в установах і організаціях різних форм власності, що мають розвинену інформаційно-комунікаційну інфраструктуру. Запропонована технологія може бути впроваджена у діяльність центрів моніторингу безпеки (SOC), а також інтегрована в корпоративні SIEM-рішення для централізованого збору, аналізу та кореляції подій безпеки. Розроблені методичні та практичні підходи можуть бути використані під час створення систем управління інформаційною безпекою (ISMS) відповідно до стандартів ISO/IEC 27001, ISO/IEC 27035 та NIST SP 800-61, а також для проведення навчальних тренінгів з виявлення та реагування на інциденти інформаційної безпеки.

Розділ 1. МЕТОДОЛОГІЧНІ ОСНОВИ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Моніторинг інформаційної безпеки — це безперервний процес збору, аналізу та оцінювання подій, що впливають на стан захищеності інформаційних ресурсів підприємства [1-3, 7]. Його головна мета полягає у своєчасному виявленні інцидентів, мінімізації ризиків та забезпеченні стабільного функціонування інформаційно-комунікаційної інфраструктури [9-10]. Методологічні основи моніторингу базуються на принципах системності, безперервності, достовірності й адаптивності та реалізуються згідно з міжнародними стандартами ISO/IEC 27001, ISO/IEC 27035 і NIST SP 800-61 [36]. Вони охоплюють етапи збору, нормалізації, аналізу, кореляції подій безпеки та реагування на інциденти [11, 32]. Центральне місце в сучасних системах займають технології SIEM (Security Information and Event Management), які забезпечують централізований збір журналів подій, їх агрегацію, кореляцію та створення аналітичних звітів у реальному часі [1-2, 5-6, 12, 18-19]. Використання SIEM дозволяє своєчасно виявляти аномалії, знижувати кількість хибних спрацьовувань і підвищувати ефективність роботи центрів моніторингу безпеки (SOC) [8, 14, 17, 20, 23, 25, 46, 55]. Отже, методологічні засади моніторингу інформаційної безпеки передбачають поєднання організаційних, технічних та аналітичних методів у єдиній системі, здатній адаптивно контролювати стан кіберзахисту підприємства та забезпечувати своєчасне реагування на загрози.

1.1. Сутність, завдання та принципи моніторингу інформаційної безпеки

Моніторинг інформаційної безпеки є ключовим елементом системи управління кіберзахистом підприємства та полягає у безперервному зборі, аналізі й оцінюванні подій, що відображають стан захищеності інформаційно-комунікаційної інфраструктури [3, 9-10]. Його сутність полягає в забезпеченні постійного спостереження за активністю користувачів, систем, сервісів і мережевих пристроїв для своєчасного виявлення відхилень, що можуть свідчити

про порушення конфіденційності, цілісності чи доступності інформації [11-12, 18, 24, 31-32, 44]. Моніторинг виконує роль основного механізму раннього попередження, який дозволяє виявляти потенційні загрози ще до моменту їх реалізації, запобігаючи або мінімізуючи наслідки інцидентів безпеки.

Основними завданнями моніторингу інформаційної безпеки (рис. 1.1) є централізований збір подій безпеки з усіх компонентів інформаційної інфраструктури, нормалізація та агрегація даних для їх уніфікованого подальшого аналізу, а також кореляція подій, що дає змогу виявляти логічні зв’язки між різними джерелами та ідентифікувати багатовекторні атаки [4, 6, 19, 33-35, 37, 39, 46]. До важливих завдань належать також виявлення аномалій і класифікація інцидентів безпеки, оцінювання рівня ризику та пріоритизація загроз, формування звітів і сповіщень для аналітиків, підтримка процесів реагування на інциденти, документування результатів моніторингу й забезпечення відповідності вимогам стандартів і нормативів.

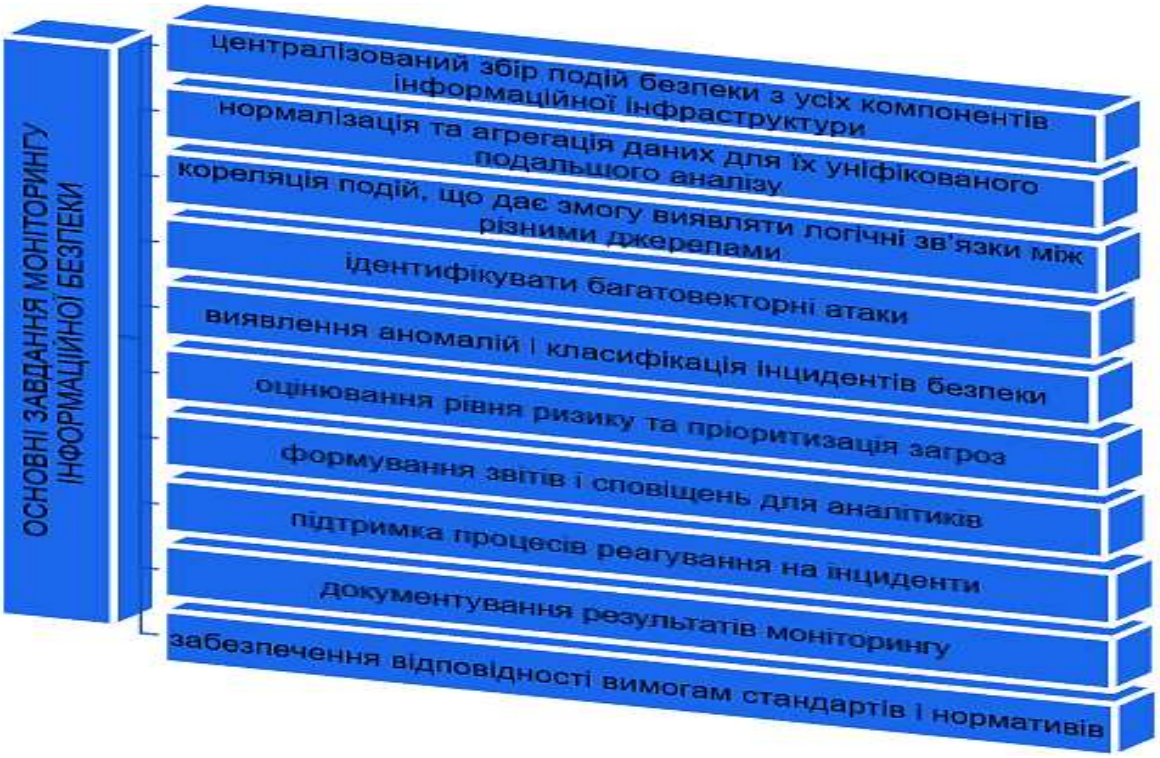


Рис. 1.1. Основні завдання моніторингу інформаційної безпеки

На рис. 1.1 показано багаторівневу структуру основних завдань моніторингу інформаційної безпеки у вигляді тривимірної моделі [7, 9-10]. Центральний блок окреслює загальну мету — забезпечення безперервного контролю стану

захищеності інформаційних ресурсів. Така візуалізація підкреслює системність, ієрархічність і взаємозалежність завдань, що формують цілісний процес управління інформаційною безпекою підприємства.

Моніторинг базується на низці ключових принципів, серед яких провідне місце займає безперервність, що забезпечує постійне спостереження за станом безпеки системи в реальному часі [1-2, 5]. Принцип системності передбачає охоплення всіх рівнів IT-інфраструктури підприємства, а комплексність — інтеграцію різних джерел інформації для формування цілісної картини безпеки [12]. Достовірність гарантує точність і надійність отриманих даних, адаптивність забезпечує здатність системи гнучко реагувати на зміни середовища або появу нових типів загроз, а автоматизація дозволяє застосовувати інтелектуальні алгоритми обробки даних, машинне навчання й поведінкову аналітику для зниження кількості хибних спрацьовувань [2, 23]. Принцип конфіденційності передбачає захист інформації, яка обробляється під час моніторингу, а відповідність міжнародним стандартам (ISO/IEC 27001, ISO/IEC 27035, NIST SP 800-61, ДСТУ ISO/IEC 27000) [32, 32-36] забезпечує нормативну узгодженість процесів і методів.

Рис. 1.2. Основні принципи моніторингу інформаційної безпеки

На рис. 1.2 подано схему, що відображає ключові принципи ефективного моніторингу інформаційної безпеки. У центрі — моніторинг, навколо якого згруповано принципи безперервності, системності, комплексності, достовірності,

адаптивності, інтелектуальної обробки даних, конфіденційності та відповідності міжнародним стандартам. Вони забезпечують безперервний контроль, точність і гнучкість аналізу, захист даних і узгодженість процесів із вимогами ISO/IEC 27001 та NIST SP 800-61.

Отже, моніторинг інформаційної безпеки виступає як стратегічний процес забезпечення стійкості інформаційних систем до кіберзагроз, що поєднує технічні, аналітичні та організаційні компоненти [5, 21, 47, 55]. Його ефективність визначається рівнем автоматизації, якістю аналітичних алгоритмів, оперативністю реагування на події та інтеграцією з іншими системами управління інформаційною безпекою підприємства.

1.2. Еволюція систем виявлення та реагування на інциденти (IDS, IPS, SIEM, SOAR)

Сучасні системи забезпечення інформаційної безпеки пройшли тривалий шлях розвитку — від базового виявлення вторгнень до комплексного автоматизованого реагування на інциденти [5, 36, 47]. Ця еволюція зумовлена постійним зростанням кількості кіберзагроз, ускладненням атак і потребою в аналітичному, проактивному підході до захисту інформаційних ресурсів.

Початковим етапом розвитку стали системи виявлення вторгнень (IDS — Intrusion Detection System), які призначені для моніторингу мережевого трафіку та подій у хостах із метою виявлення підозрілої активності [3, 7, 10]. Вони аналізують вхідні та вихідні пакети даних, зіставляючи їх із відомими шаблонами атак або відхиленнями від нормальної поведінки. IDS-системи можуть бути мережевими (NIDS) або хостовими (HIDS), проте їх головний недолік — пасивність: вони лише сповіщають про загрозу, але не блокують її.

Подальшим етапом стали системи запобігання вторгненням (IPS — Intrusion Prevention System), які поєднують функції IDS із можливістю автоматичного реагування. IPS не тільки виявляє шкідливу активність, а й блокує атаки в реальному часі, змінюючи правила фільтрації трафіку, ізолюючи вузли чи

припиняючи сесію [5, 36]. Проте з розвитком корпоративних мереж та збільшенням обсягів журналів безпеки постала потреба в централізованій обробці, кореляції та аналізі інформації з різних джерел.

На рис. 1.3 відображено послідовний розвиток систем забезпечення інформаційної безпеки: від IDS, що здійснюють пасивне виявлення вторгнень, до IPS, які активно запобігають атакам; далі — до SIEM, що забезпечують аналітику, кореляцію подій і аудит; і, нарешті, до SOAR, які реалізують інтелектуальну автоматизацію реагування [5, 36, 47, 55]. Схема демонструє поступове ускладнення функціональності та інтеграцію засобів моніторингу, аналізу й реагування у єдину систему кіберзахисту.

Рис. 1.3. Еволюція систем виявлення та реагування на інциденти

Це привело до появи систем управління інформацією та подіями безпеки — SIEM (Security Information and Event Management). Вони поєднують функції збору логів, нормалізації даних, аналітики, візуалізації та оповіщення. SIEM-системи забезпечують глобальний огляд стану безпеки, виявлення складних багатовекторних атак, формування звітів і підтримку процесів аудиту [2, 18, 22-23]. Серед найвідоміших рішень — Splunk, IBM QRadar, ArcSight, Wazuh, ELK Stack

[14, 21, 25, 29]. Вони дозволяють виявляти інциденти, які неможливо зафіксувати окремими засобами IDS чи IPS, і виступають ядром центрів моніторингу безпеки (SOC).

Подальший розвиток концепції автоматизації привів до формування SOAR (Security Orchestration, Automation and Response) — систем нового покоління, що інтегрують SIEM, аналітику загроз (Threat Intelligence), засоби управління інцидентами та сценарії автоматизованого реагування [47, 55]. SOAR-платформи дозволяють зменшити час реакції, стандартизувати процедури реагування, знизити навантаження на аналітиків SOC і забезпечити адаптивність до нових сценаріїв атак.

Таблиця 1.1

Порівняльна характеристика систем IDS, IPS, SIEM та SOAR

Критерій	**IDS (Intrusion Detection System)**	**IPS (Intrusion Prevention System)**	**SIEM (Security Information and Event Management)**	**SOAR (Security Orchestration, Automation and Response)**
Призначення	Виявлення вторгнень і сповіщення про інциденти	Запобігання вторгненням і блокування атак у реальному часі	Централізований збір, аналіз і кореляція подій безпеки	Автоматизоване реагування та оркестрація процесів безпеки
Основні функції	Аналіз мережевого трафіку, виявлення аномалій, оповіщення	Моніторинг, блокування атак, оновлення правил безпеки	Агрегація логів, візуалізація подій, формування звітів	Інтеграція з SIEM, запуск сценаріїв реагування, машинне навчання
Рівень автоматизації	Мінімальний (ручний аналіз подій)	Часткова автоматизація реагування	Середній (аналітика та звітність)	Високий (повна автоматизація реагування)
Тип реагування	Пасивний (сповіщення)	Активний (блокування)	Аналітичний (оцінка, кореляція, рекомендації)	Автоматизований (виконання дій за сценаріями)
Джерела даних	Мережевий трафік, журнали подій	IDS, файрволи, сенсори мережі	Усі системи безпеки, лог-файли, додатки, користувачі	Дані SIEM, Threat Intelligence, SOC-інструменти
Приклади систем	Snort, Suricata, Zeek (Bro)	Cisco Firepower, Palo Alto IPS, FortiGate	Splunk, IBM QRadar, ArcSight, Wazuh, ELK Stack	Cortex XSOAR, IBM Resilient, Splunk SOAR, Siemplify
Рівень інтеграції	Локальний	Локальний або мережевий	Корпоративний, багаторівневий	Централізований, міжсистемний

Переваги	Простота, швидкість виявлення	Активний захист, мінімізація часу реагування	Централізований контроль і звітність	Автоматизація, зниження навантаження на аналітиків, адаптивність
Недоліки	Відсутність автоматичного реагування	Можливі хибні спрацьовування	Висока складність налаштування та обробки даних	Висока вартість, потреба в інтеграції з іншими системами

У табл. 1.1 наведено основні відмінності між системами виявлення та реагування на інциденти. Показано, що IDS виконують пасивний моніторинг і сповіщення, IPS — активно блокують атаки, SIEM забезпечують централізовану аналітику та кореляцію подій, а SOAR реалізують автоматизоване реагування. Еволюція цих технологій демонструє поступовий перехід від простого виявлення до комплексного, інтелектуального управління кіберзахистом підприємства.

Таким чином, еволюція систем виявлення та реагування пройшла шлях від пасивного сповіщення (IDS) до активного запобігання (IPS), аналітичної кореляції (SIEM) та інтелектуальної автоматизації (SOAR) [36]. Сьогодні ці технології взаємодіють у межах єдиного екосистемного підходу до кіберзахисту, де SIEM виступає центром моніторингу, а SOAR — інструментом автоматизованого реагування, що разом формують основу сучасних архітектур безпеки підприємств.

1.3. Концептуальна архітектура та функціональні компоненти SIEM

Системи SIEM (Security Information and Event Management) є центральним елементом сучасної архітектури кіберзахисту підприємства, забезпечуючи комплексне збирання, нормалізацію, аналіз і кореляцію подій безпеки з різних джерел у режимі реального часу [55]. Вони дозволяють своєчасно виявляти інциденти, формувати аналітичні звіти, прогнозувати тенденції та оперативно реагувати на загрози [2, 23, 47]. Концептуальна архітектура SIEM об’єднує програмні, мережеві й аналітичні компоненти в єдину систему, здатну інтегруватися з IDS/IPS, SOAR, EDR, DLP, антивірусними комплексами й іншими мережевими засобами контролю, утворюючи багаторівневу екосистему захисту.

На рівні збору даних (Data Collection Layer) відбувається централізоване збирання журналів подій із серверів, мережевого обладнання, систем автентифікації, додатків, брандмауерів, антивірусів та зовнішніх потоків Threat Intelligence [1, 5, 55]. Дані надходять до SIEM через спеціальні агенти, колектори або стандартні протоколи, зокрема Syslog, SNMP та API, що забезпечує масштабованість і гнучкість підключення різнорідних джерел.

Рівень нормалізації та зберігання (Normalization and Storage Layer) відповідає за конвертацію отриманих журналів у стандартизований формат (CEF, JSON, LEEF), очищення від дублювання й аномалій, а також за зберігання структурованих подій у базі даних або спеціалізованому репозиторії [36, 47]. Це створює узгоджену інформаційну основу для подальшої аналітики та аудиту безпеки.

На рівні аналізу та кореляції (Analysis and Correlation Layer) відбувається глибинна обробка даних за допомогою правил, шаблонів, статистичних і машинних алгоритмів. Впроваджуються механізми поведінкового аналізу (UEBA) та машинного навчання, які дозволяють виявляти складні багатовекторні атаки, аномалії у поведінці користувачів чи систем, а також приховані ланцюжки подій типу APT [23-24, 27, 30-31]. Цей рівень формує інциденти безпеки та забезпечує їх пріоритизацію.

Рівень управління та реагування (Management and Response Layer) є аналітичним і операційним центром SIEM. Він включає інтерфейси для фахівців SOC, панелі моніторингу, механізми формування звітів і дашбордів, а також системи автоматичного сповіщення [5, 55]. Розвинені SIEM-рішення інтегруються з платформами SOAR для автоматизації реагування на інциденти — ізоляції компрометованих вузлів, блокування IP-адрес, відключення облікових записів користувачів тощо.

Нарешті, рівень інтеграції та взаємодії (Integration Layer) забезпечує узгоджену роботу SIEM із зовнішніми інструментами управління інформаційною безпекою — Active Directory, CMDB, антивірусними рішеннями, системами резервного копіювання, EDR/XDR, DLP та хмарними сервісами. Така взаємодія формує єдиний контекст подій, сприяє побудові цілісної картини стану безпеки

підприємства та підтримує прийняття обґрунтованих рішень у режимі реального часу.

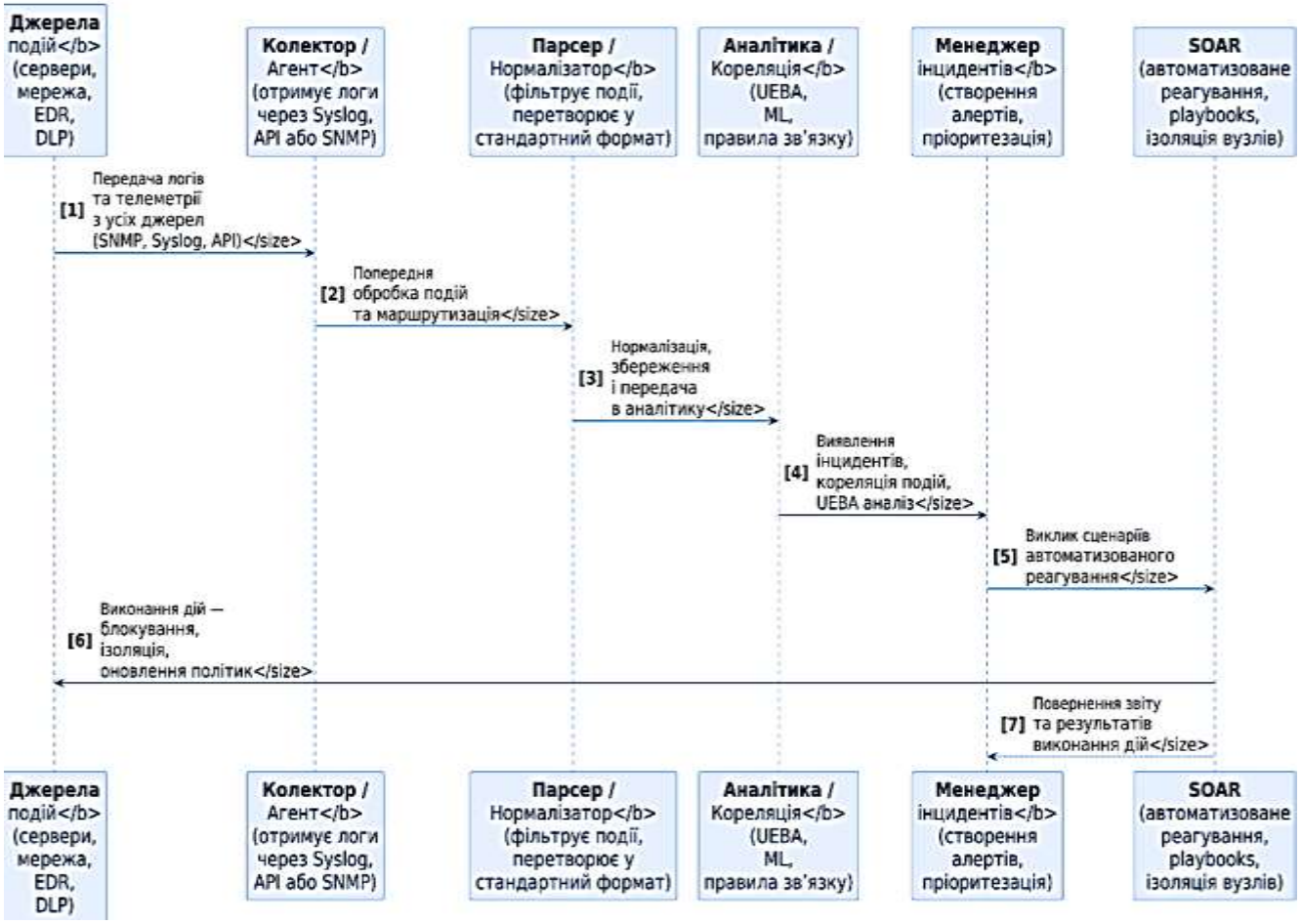


Рис. 1.4. Діаграма послідовної роботи SIEM

На рис. 1.4 зображено концептуальну послідовність роботи системи SIEM, яка демонструє повний цикл обробки подій інформаційної безпеки — від збору даних до автоматизованого реагування. У верхній частині схеми показано, як журнали подій і телеметрія з різних джерел — серверів, мережевого обладнання, EDR, DLP чи хмарних сервісів — надходять до колектора через протоколи Syslog, SNMP або API. Колектор здійснює первинну обробку та маршрутизацію даних, після чого парсер/нормалізатор перетворює їх у стандартизований формат для подальшого аналізу. На етапі аналітики та кореляції події об’єднуються за правилами зв’язків, обробляються модулями UEBA та ML, що дозволяє виявляти аномалії, підозрілі дії та багатовекторні атаки [27, 30]. Далі менеджер інцидентів створює сповіщення, визначає пріоритети реагування й передає інформацію у модуль SOAR, який виконує автоматизовані сценарії реагування — блокування IP-адрес, ізоляцію

вузлів або оновлення політик безпеки. Таким чином, діаграма відображає тісну взаємодію між усіма рівнями архітектури SIEM: збір → нормалізація → аналітика → інцидент → реагування, що забезпечує безперервний і замкнений цикл моніторингу, аналізу та вдосконалення системи кіберзахисту підприємства.

Додатково SIEM інтегрується з зовнішніми модулями — Threat Intelligence, SOAR-платформами, EDR-системами та CMDB, забезпечуючи збагачення контексту подій, оркестрацію сценаріїв реагування та безперервний зворотний зв’язок між рівнями. Така інтеграція підвищує точність аналітики, дозволяючи корелювати внутрішні події з глобальними загрозами та індикаторами компрометації [23, 47]. Завдяки цьому SIEM стає центром консолідації інформації та координації дій усієї системи кіберзахисту підприємства.

У додатку А представлено концептуальну архітектуру системи SIEM, яка відображає основні функціональні рівні її роботи — від збору подій до управління інцидентами. Архітектура включає рівень збору даних (Data Collection Layer), де здійснюється централізований прийом журналів подій з різних джерел (серверів, мережевого обладнання, систем автентифікації, антивірусів, EDR/DLP). Далі дані нормалізуються, очищуються від дублювання та зберігаються у сховищі подій (Normalization and Storage Layer), формуючи уніфіковану базу для аналітики. На рівні аналізу та кореляції (Analysis and Correlation Layer) застосовуються правила, часові вікна, механізми UEBA та алгоритми машинного навчання для виявлення аномалій та складних атак. Рівень управління та реагування (Management and Response Layer) забезпечує формування дашбордів, звітів, аналітики SOC і взаємодію з платформами SOAR, ITSM і CMDB. Завершальний рівень інтеграції (Integration Layer) узгоджує роботу SIEM з іншими компонентами кіберзахисту (Threat Intelligence, EDR/XDR, DLP, Active Directory, Cloud), утворюючи єдину екосистему безпеки підприємства.

У табл. 1.2 наведено основні компоненти системи SIEM, які забезпечують повний цикл моніторингу, аналізу та реагування на інциденти безпеки. Модулі Log Collector і Event Parser відповідають за збір і нормалізацію журналів подій, Correlation Engine — за виявлення закономірностей і формування інцидентів, а

Incident Manager — за сповіщення та пріоритезацію загроз [5, 36, 55]. Dashboard і Reporting Engine реалізують візуалізацію даних і звітність, тоді як Threat Intelligence та SOAR Connector забезпечують інтеграцію з зовнішніми джерелами загроз і системами автоматизованого реагування, формуючи єдину аналітичну екосистему кіберзахисту.

Таблиця 1.2

Основні функціональні компоненти SIEM

Компонент	**Призначення**
Log Collector / Agent	Збір і передача журналів подій у централізоване сховище
Event Parser / Normalizer	Перетворення логів у єдиний формат для подальшої обробки
Correlation Engine	Виявлення закономірностей, створення інцидентів на основі сукупності подій
Incident Manager / Alerting Module	Формування сповіщень, інцидентів і призначення пріоритетів
Dashboard / Visualization	Відображення ключових показників безпеки, побудова графіків і трендів
Reporting Engine	Генерація звітів для керівництва, аудиту та відповідності стандартам
Threat Intelligence Feed	Інтеграція зовнішніх баз загроз для розширення контексту аналізу
Integration API / SOAR Connector	Зв’язок із зовнішніми системами реагування, EDR і хмарними сервісами

Таким чином, концептуальна схема демонструє логічну послідовність обробки інформації: від джерел подій → збору та нормалізації → аналітики й кореляції → управління інцидентами → інтегрованого реагування, що формує замкнений цикл кіберзахисту підприємства.

1.4. Стандарти та нормативно-правові вимоги до моніторингу безпеки

Моніторинг інформаційної безпеки є невід’ємною складовою системного управління ризиками й забезпечення кіберстійкості підприємства, тому його впровадження та функціонування повинно відповідати чинним міжнародним стандартам і національним нормативно-правовим актам [3, 7, 9]. Основу нормативної бази складають стандарти серії ISO/IEC 27000, які визначають загальні принципи, політики та методи управління інформаційною безпекою. Зокрема, ISO/IEC 27001:2022 регламентує вимоги до створення, впровадження,

підтримання та постійного вдосконалення системи управління інформаційною безпекою (СУІБ), а ISO/IEC 27002 конкретизує набір контролів і рекомендацій, що охоплюють моніторинг подій, управління журналами, виявлення інцидентів і реагування на них.

Особливу увагу в контексті моніторингу безпеки приділено стандартам ISO/IEC 27035 (Incident Management), які описують процеси виявлення, класифікації, ескалації та документування інцидентів. Вони визначають алгоритм дій від моменту фіксації події до аналізу її наслідків і запобігання повторенню. Доповнює цей комплекс стандарт ISO/IEC 27005, який описує методологію управління ризиками, зокрема аналіз загроз, вразливостей, оцінку ймовірності інцидентів та формування заходів контролю. Ці стандарти взаємодоповнюють один одного, утворюючи цілісну методологію побудови процесів моніторингу та управління інцидентами [3, 7, 36]. Вони забезпечують узгодженість дій між технічними, організаційними та аналітичними рівнями системи безпеки, що дозволяє своєчасно виявляти, документувати та мінімізувати наслідки кіберінцидентів.

Для організацій, що працюють із критичною інфраструктурою або обробляють великі обсяги даних, значну роль відіграє рекомендаційний документ NIST SP 800-137 “Information Security Continuous Monitoring (ISCM)”, розроблений Національним інститутом стандартів і технологій США [3, 7]. У ньому визначено концепцію безперервного моніторингу як динамічного процесу, який забезпечує постійну оцінку ефективності засобів захисту, своєчасне виявлення нових ризиків і підтримку рівня довіри до інформаційних систем [55]. Взаємопов’язаний документ NIST SP 800-61 “Computer Security Incident Handling Guide” регламентує порядок реагування на інциденти, включно з формуванням центрів моніторингу (SOC) і визначенням ролей відповідальних осіб.

У європейському правовому полі важливу роль відіграє Директива NIS2 (Network and Information Systems Directive), яка встановлює вимоги до операторів критичних послуг і цифрових провайдерів щодо забезпечення належного рівня кібербезпеки, включно з моніторингом, виявленням інцидентів та звітуванням

компетентним органам [3, 7, 10]. У сфері захисту персональних даних діє Регламент (ЄС) 2016/679 (GDPR), який передбачає обов'язкове ведення журналів подій і моніторинг доступів до персональної інформації.

В Україні правові засади моніторингу безпеки визначаються Законами України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про інформацію», а також «Про захист персональних даних». Відповідно до них, суб'єкти господарювання зобов'язані впроваджувати технічні й організаційні заходи контролю за станом безпеки, створювати системи технічного захисту інформації та забезпечувати реєстрацію подій безпеки. Додатково застосовуються вимоги стандартів ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27005:2015, ДСТУ ISO/IEC 27035:2015 та галузеві нормативи Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ), що встановлюють вимоги до побудови та функціонування комплексних систем захисту інформації (КСЗІ).

Табл. 1.3 узагальнює ключові стандарти та нормативи, що регулюють моніторинг інформаційної безпеки. У ній показано, як міжнародні документи ISO/IEC формують базові принципи управління безпекою, а стандарти NIST деталізують практичні аспекти моніторингу та реагування. Європейські акти NIS2 і GDPR встановлюють вимоги до захисту даних і звітування про інциденти, тоді як українські закони та ДСТУ ISO/IEC забезпечують їх адаптацію на національному рівні [3, 7, 10]. Таким чином, таблиця відображає узгодженість міжнародних, європейських і вітчизняних норм у побудові системи моніторингу кібербезпеки.

Таблиця 1.3

Основні стандарти та нормативно-правові вимоги до моніторингу безпеки

Документ / Стандарт	**Орган / Юрисдикція**	**Ключове призначення**
ISO/IEC 27001:2022	ISO / IEC (міжнародний)	Встановлює вимоги до створення, впровадження та вдосконалення СУІБ, включно з моніторингом подій
ISO/IEC 27035:2023	ISO / IEC (міжнародний)	Регламентує процеси виявлення, реєстрації, класифікації та розслідування інцидентів
ISO/IEC 27005:2018	ISO / IEC (міжнародний)	Описує методологію управління ризиками, включно з оцінкою подій і загроз
NIST SP 800-137	США (NIST)	Визначає концепцію безперервного моніторингу інформаційної безпеки

NIST SP 800-61r2	США (NIST)	Містить керівництво з реагування на інциденти та побудови SOC
Директива NIS2 (2023)	ЄС	Встановлює вимоги до кібербезпеки операторів критичних послуг і цифрових провайдерів
Регламент GDPR (ЄС 2016/679)	ЄС	Визначає вимоги до моніторингу доступів і захисту персональних даних
Закон України «Про основні засади забезпечення кібербезпеки» (2017)	Україна	Визначає принципи створення систем моніторингу та реагування на інциденти
ДСТУ ISO/IEC 27001:2015, 27005:2015, 27035:2015	Україна (ДССЗЗІ)	Національні адаптації міжнародних стандартів у сфері моніторингу та управління інцидентами

Таким чином, моніторинг безпеки має базуватися на поєднанні міжнародних стандартів, методичних рекомендацій NIST і чинних національних норм, що забезпечує його системність, правову обґрунтованість і відповідність вимогам аудиту та сертифікації.

Рис. 1.5 рівень відповідності між основними процесами SIEM-моніторингу (збір подій, нормалізація, аналітика, реагування, звітність) і міжнародними стандартами — ISO 27001, ISO 27035, NIST 800-137, NIS2 та GDPR. Кольорова шкала від 0 до 3 відображає ступінь охоплення процесів: 0 – відсутність вимог, 1 – часткове охоплення, 2 – помірне, 3 – повне.

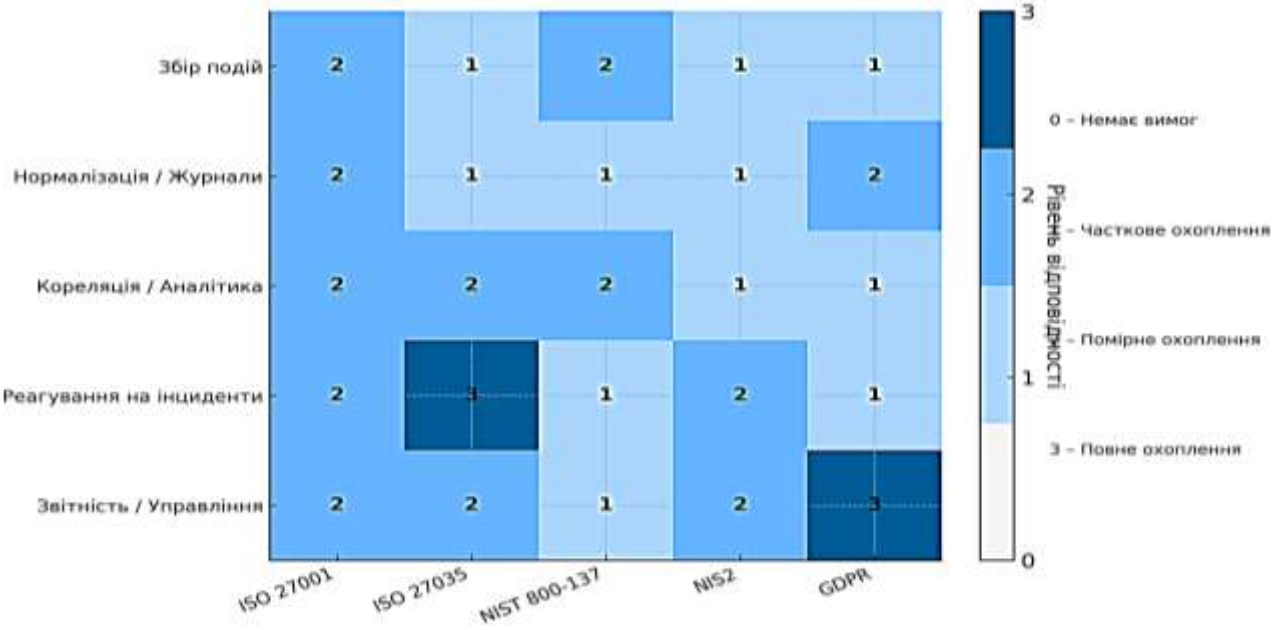


Рис. 1.5. Матриця відповідності стандартів і процесів моніторингу безпеки (оцінка 0–3)

Впровадження цих стандартів гарантує узгодженість процесів спостереження, реагування та звітування, формуючи єдиний нормативний простір для ефективного управління інформаційною безпекою підприємства.

1.5. Сучасні підходи й технологічні рішення у сфері SIEM-моніторингу

Сучасні підходи до SIEM-моніторингу (Security Information and Event Management) орієнтовані на інтеграцію аналітики, автоматизації та штучного інтелекту з метою підвищення ефективності виявлення інцидентів і зменшення часу реагування [23, 36, 47]. Класичні SIEM-системи, які раніше фокусувалися на зборі та кореляції логів, еволюціонували у напрямі інтелектуальних платформ моніторингу безпеки, здатних здійснювати поведінковий аналіз, прогнозування загроз і адаптивне реагування.

Одним із ключових напрямів розвитку є впровадження UEBA (User and Entity Behavior Analytics) — технології, що аналізує поведінку користувачів і пристроїв для виявлення аномалій, які можуть свідчити про внутрішні загрози або компрометацію облікових записів [18, 27, 30, 46]. Комбінація UEBA з машинним навчанням (ML) дозволяє SIEM-системам динамічно оновлювати профілі поведінки, враховуючи контекст, час доби, геолокацію та тип активності.

Іншим важливим трендом є автоматизація реагування через інтеграцію SIEM із системами SOAR (Security Orchestration, Automation and Response). Таке поєднання забезпечує не лише фіксацію інцидентів, а й виконання наперед визначених сценаріїв реагування — ізоляцію вузлів, блокування доступу, сповіщення аналітиків або створення тікетів у системах ITSM. Завдяки цьому зменшується навантаження на операторів SOC і скорочується час реакції (MTTR).

Сучасні рішення також активно використовують Threat Intelligence Feeds — потоки зовнішніх даних про компрометацію (IoC), фішингові кампанії, домени та IP-адреси, пов’язані з відомими атаками [5, 23]. Інтеграція з такими джерелами підвищує точність кореляції та дозволяє SIEM-системам працювати проактивно, запобігаючи атакам до їх розгортання.

Важливою тенденцією стало впровадження хмарних SIEM-платформ (наприклад, Microsoft Sentinel, Splunk Cloud, IBM QRadar on Cloud), що забезпечують масштабованість, централізовану аналітику великих даних і використання штучного інтелекту для виявлення невідомих шаблонів атак. Такі системи інтегруються з EDR/XDR і Zero Trust архітектурами, формуючи єдину екосистему безпеки.

На рис. 1.6 подано узагальнену 3D-інфографіку, що відображає концепцію сучасного SIEM-моніторингу як багаторівневої інтегрованої системи управління інформаційною безпекою [3, 7, 9]. У нижній частині схеми зображено рівень Data Collection, який забезпечує збирання та агрегацію подій із серверів, мережевого обладнання, систем автентифікації, EDR і DLP. Наступний рівень — Analytics — представляє аналітичне ядро SIEM, де реалізовано алгоритми машинного навчання (ML) і поведінковий аналіз (UEBA) для виявлення аномалій і складних атак [46]. Далі розташовано рівень Response, який відповідає за автоматизоване реагування через інтеграцію з платформами SOAR, що виконують сценарії блокування, ізоляції або сповіщення. Верхній рівень Integration демонструє взаємодію SIEM з іншими системами безпеки, такими як Threat Intelligence, XDR та Zero Trust архітектури, що забезпечують єдиний контекст подій і динамічне оновлення політик захисту. Схема відображає перехід від класичного збору логів до інтелектуального, автоматизованого та проактивного моніторингу безпеки, який формує основу сучасного SOC-рівня захисту підприємства.

Рис. 1.6. Сучасні підходи в SIEM-моніторингу

Таким чином, сучасний SIEM-моніторинг поєднує аналітику поведінки, машинне навчання, автоматизацію, інтеграцію з зовнішніми джерелами та хмарні

обчислення, що перетворює його з інструменту пасивного спостереження на активний центр управління кіберзахистом і прийняття рішень у режимі реального часу [20-21, 46-47]. Використання штучного інтелекту та поведінкової аналітики дозволяє системам SIEM не лише виявляти відомі загрози, а й прогнозувати нові типи атак на основі аномалій у даних. Інтеграція з SOAR, XDR і Zero Trust забезпечує узгоджене реагування та централізований контроль над усіма аспектами безпеки. У результаті SIEM-моніторинг стає ключовим компонентом сучасної стратегії кіберзахисту, що підвищує рівень стійкості підприємства до динамічних кіберзагроз.

Висновки до першого розділу

У результаті аналізу встановлено, що моніторинг інформаційної безпеки є ключовим елементом системи управління кіберзахистом підприємства, який забезпечує безперервне спостереження, виявлення, аналіз і реагування на події безпеки. Його методологічна основа базується на принципах системності, комплексності, достовірності, адаптивності та відповідності міжнародним стандартам ISO/IEC і NIST. Еволюція технологій від IDS та IPS до SIEM і SOAR свідчить про перехід від пасивного сповіщення до активного, аналітичного та автоматизованого реагування на інциденти. Сучасні SIEM-системи виконують роль центральної ланки екосистеми моніторингу, поєднуючи збір і нормалізацію даних, поведінкову аналітику, машинне навчання, кореляцію подій та автоматизацію дій через SOAR-платформи. Впровадження міжнародних і національних нормативів (ISO/IEC 27001, 27035, NIST SP 800-137, NIS2, ДСТУ) забезпечує правову узгодженість процесів і підвищує рівень кіберстійкості підприємства.

Отже, моніторинг інформаційної безпеки формує основу сучасного підходу до управління ризиками та реагування на кіберзагрози, інтегруючи технічні, аналітичні та організаційні інструменти в єдину адаптивну систему, здатну

підтримувати стійкість інформаційної інфраструктури в умовах динамічного кіберсередовища.

Розділ 2. МОДЕЛЬ ТА МЕТОДИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ SIEM-МОНІТОРИНГУ

Розроблення моделі та методів реалізації технології SIEM-моніторингу ґрунтується на комплексному підході до аналізу подій безпеки, який поєднує математичні, алгоритмічні та інформаційні методи обробки даних [1, 5, 36, 47]. SIEM-система (Security Information and Event Management) забезпечує централізований збір, нормалізацію, кореляцію та аналіз подій з різних джерел у режимі реального часу, формуючи основу для виявлення інцидентів, оцінки ризиків і реагування на загрози.

У межах даного розділу подано формалізовану модель подій і джерел даних, описано процеси збору, нормалізації та кореляції інформації, побудовано модель виявлення інцидентів на основі правил і поведінкових характеристик, а також розроблено технологічну схему інтеграції SIEM у корпоративну архітектуру кіберзахисту [18, 27, 55]. Представлений підхід дозволяє підвищити точність виявлення аномалій, зменшити середній час реакції на події (Mean Time to Detect, MTTD) та оптимізувати використання ресурсів моніторингу.

2.1. Постановка задачі та визначення цілей моніторингу безпеки

Ефективність системи кіберзахисту підприємства значною мірою визначається її здатністю своєчасно виявляти, аналізувати та реагувати на інциденти безпеки. У сучасних умовах інтенсивного інформаційного обміну обсяг і динаміка подій, що генеруються інформаційними системами, значно перевищують можливості ручного контролю, що зумовлює необхідність впровадження автоматизованих технологій моніторингу [1, 5]. Технологія SIEM (Security Information and Event Management) забезпечує централізоване збирання, нормалізацію, аналіз і кореляцію подій із різних джерел, формуючи єдиний контекст для прийняття оперативних та стратегічних рішень щодо безпеки.

Задача SIEM-моніторингу полягає у створенні інтегрованої системи обробки подій безпеки, здатної автоматизовано збирати логи та телеметричні дані із

серверів, мережевого обладнання, систем контролю доступу, антивірусних і IDS/IPS-комплексів, виконувати нормалізацію та уніфікацію форматів даних, здійснювати кореляцію подій у часовому та логічному вимірах, оцінювати рівень ризику й виявляти інциденти на основі правил і поведінкових моделей, а також ініціювати процедури реагування, сповіщення та формування звітів.

Метою SIEM-моніторингу є побудова інтелектуального середовища контролю безпеки, що забезпечує безперервне спостереження за станом інформаційно-комунікаційних систем підприємства, своєчасне виявлення аномалій і інцидентів у режимі реального часу шляхом аналізу логів і поведінкових показників, підвищення інформованості та реактивності служби безпеки завдяки консолідації даних із різнорідних джерел, мінімізацію часу виявлення інциденту (Mean Time to Detect, MTTD) і часу реагування (Mean Time to Respond, MTTR), а також підтримку процесів прийняття рішень у системі управління інформаційною безпекою (ISMS) через використання аналітичних панелей, звітів і прогнозних моделей.

Формально задача моніторингу безпеки може бути подана як оптимізаційна проблема [31, 36]:

$$\min T_{detect}\text{, за умови } R \leq R_{max}, \tag{2.1}$$

де T_{detect} – середній час виявлення інциденту, R – залишковий ризик, R_{max} – допустимий рівень ризику для підприємства.

У загальному вигляді система SIEM розглядається як сукупність взаємопов’язаних підсистем:

$$SIEM = \langle S_{col}, S_{norm}, S_{corr}, S_{anal}, S_{resp} \rangle, \tag{2.2}$$

де S_{col} – підсистема збору подій, S_{norm} – нормалізації, S_{corr} – кореляції, S_{anal} – аналітики та візуалізації, S_{resp} – реагування.

На рис. 2.1 подано узагальнену структурно-функціональну модель технології SIEM-моніторингу, що відображає основні етапи обробки подій безпеки у вертикальному потоці — від збору даних до реагування. У верхній частині показано джерела подій (сервери, мережеве обладнання, системи контролю доступу, антивірусні комплекси, хмарні сервіси), з яких за допомогою агентів і

колекторів здійснюється автоматизований збір логів та телеметрії. Далі дані проходять етапи нормалізації, кореляції та аналітики в ядрі SIEM-системи, де відбувається виявлення інцидентів і формування оцінок ризику. У нижній частині наведено модулі реагування (SOAR), аналітичні панелі та сховище подій, які забезпечують зберігання, візуалізацію й подальшу обробку інформації. Зовнішні контексти (CTI, CMDB, MDM, ITSM) забезпечують додаткові відомості для підвищення точності аналізу та автоматизації реагування.

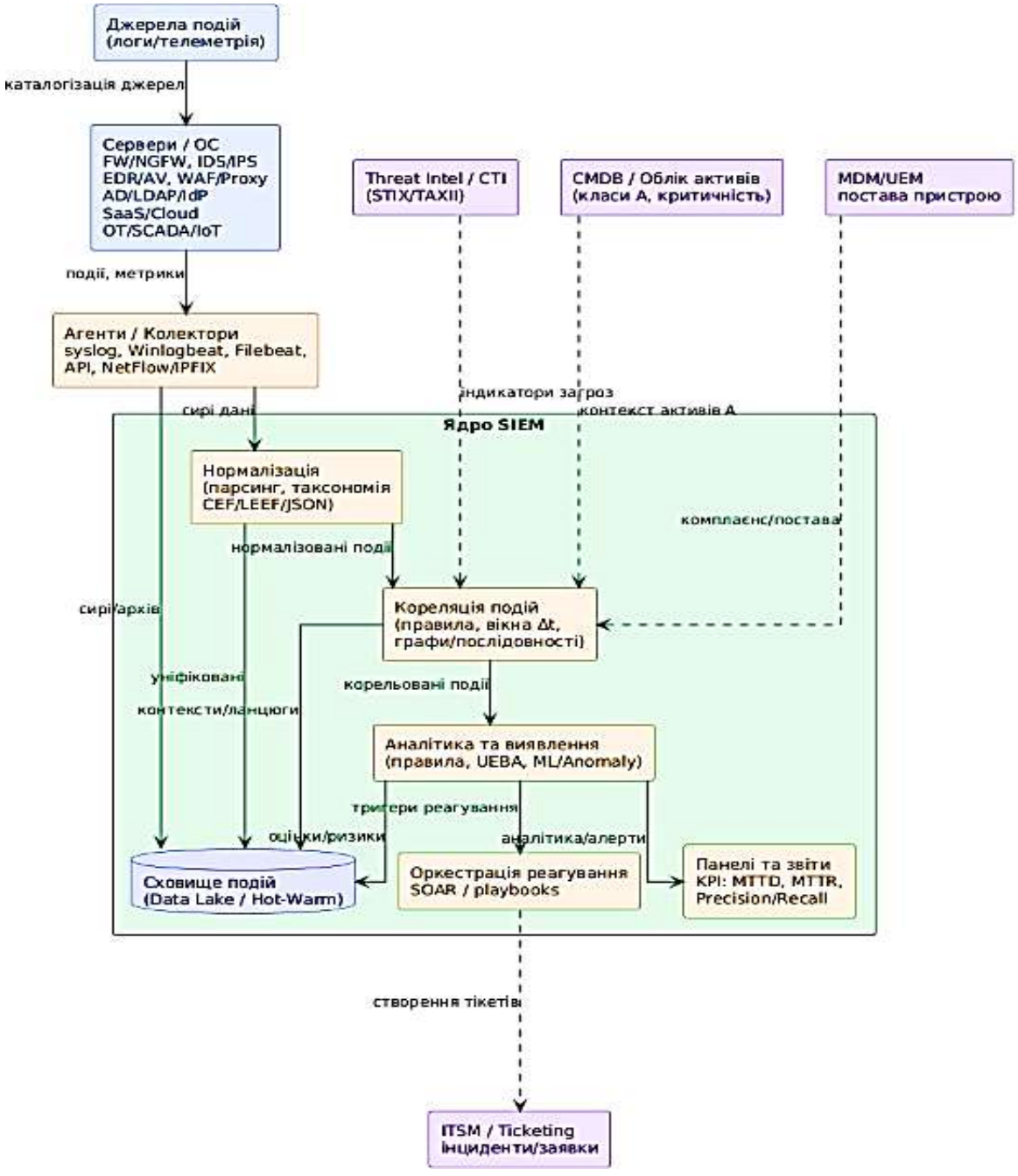


Рис. 2.1. Структурно-функціональна модель технології SIEM-моніторингу

Взаємодія цих підсистем утворює замкнутий контур управління безпекою, що базується на принципах континуального спостереження (continuous monitoring), динамічної кореляції та контекстного аналізу ризику. Такий підхід забезпечує можливість раннього виявлення загроз, побудову причинно-наслідкових ланцюгів атак і формування адекватних заходів реагування.

2.2. Формування інформаційної моделі подій та джерел даних безпеки

Ефективність функціонування системи SIEM значною мірою визначається якістю та структурою вхідних даних, що надходять від різнорідних джерел [1, 5, 55]. Для побудови узгодженої моделі моніторингу необхідно формалізувати події, джерела, користувачів і активи підприємства як об’єкти єдиного інформаційного простору.

У загальному вигляді множини основних елементів описуються як [55]:

$$\boldsymbol{E} = \{\boldsymbol{e_1}, \boldsymbol{e_2}, \dots, \boldsymbol{e_n}\},\ \boldsymbol{S} = \{\boldsymbol{s_1}, \boldsymbol{s_2}, \dots, \boldsymbol{s_m}\},\ \boldsymbol{U} = \{\boldsymbol{u_1}, \boldsymbol{u_2}, \dots, \boldsymbol{u_k}\},\ \boldsymbol{A} = \{\boldsymbol{a_1}, \boldsymbol{a_2}, \dots, \boldsymbol{a_r}\}, \quad (2.3)$$

де $\boldsymbol{E}$ – множина подій безпеки, $\boldsymbol{S}$ – множина джерел інформації (сервери, мережеві пристрої, агенти збору даних), $\boldsymbol{U}$ – множина користувачів, що взаємодіють із системою, $\boldsymbol{A}$ – множина активів підприємства, що підлягають контролю.

Події безпеки надходять у часі від різних джерел, тому вводиться функція потоку подій [6, 18]:

$$\boldsymbol{P(t)} = \{(\boldsymbol{e_i}, \boldsymbol{s_j}, \boldsymbol{a_k}, \boldsymbol{t_l})\}, \quad (2.4)$$

де $\boldsymbol{e_i}$ – тип події, $\boldsymbol{s_j}$ – джерело, $\boldsymbol{a_k}$ – актив, $\boldsymbol{t_l}$ – часовий маркер. Таким чином, $\boldsymbol{P(t)}$ формує часову послідовність подій, які характеризують стан безпеки в системі.

Кожна подія описується набором атрибутів [1, 5, 55]:

$$\boldsymbol{e_i} = \langle \boldsymbol{id}, \boldsymbol{type}, \boldsymbol{src}, \boldsymbol{dst}, \boldsymbol{proto}, \boldsymbol{sev}, \boldsymbol{msg}, \boldsymbol{hash}, \boldsymbol{t} \rangle , \quad (2.5)$$

де $\boldsymbol{type}$ – категорія події (аутентифікація, доступ, модифікація, мережевий трафік тощо), $\boldsymbol{sev}$ – рівень критичності, $\boldsymbol{msg}$ – текст журналу, $\boldsymbol{hash}$ – унікальний ідентифікатор події.

Для кількісного опису інтенсивності та складності потоку подій використовуються показники, інтенсивність:

$$\boldsymbol{\lambda_i = \frac{N_i}{T}}, \tag{2.6}$$

де $\boldsymbol{N_i}$ – кількість подій від джерела $\boldsymbol{s_i}$ за інтервал $\boldsymbol{T}$;

середня частота появи:

$$\boldsymbol{f = \frac{1}{T}\sum_{i=1}^{n} n_i}, \tag{2.7}$$

ентропія потоку логів, що характеризує ступінь різноманітності подій [6, 18, 30]:

$$\boldsymbol{H = -\sum_{i=1}^{n} p_i log_2 p_i}, \tag{2.8}$$

де $\boldsymbol{p_i}$ – імовірність появи події типу $\boldsymbol{e_i}$. Зростання ентропії сигналізує про нестандартну поведінку системи та може бути індикатором аномалії чи потенційного інциденту безпеки.

Для формалізації зв’язків між джерелами, користувачами та активами будується відображення [5, 36]:

$$\boldsymbol{\Phi: S \times U \times A \longrightarrow E}, \tag{2.9}$$

яке описує правило, за яким конкретне джерело $\boldsymbol{s_j}$, користувач $\boldsymbol{u_k}$ і актив $\boldsymbol{a_r}$ породжують подію $\boldsymbol{e_i}$. Таке відображення дає змогу побудувати матрицю кореляцій джерел і подій, що використовується на подальших етапах для аналітичного аналізу та виявлення інцидентів.

У межах технології SIEM джерела даних класифікуються за функціональним призначенням і типом інформації, яку вони генерують [11, 25, 33, 35]. Основними групами джерел є системні журнали, що фіксують події операційних систем і прикладних сервісів (Windows Event Log, syslog, auditd); мережеві потоки (NetFlow, IPFIX, sFlow), які забезпечують інформацію про інтенсивність, напрям і тип трафіку; системи контролю доступу (Active Directory, LDAP, Radius), що відображають автентифікацію, авторизацію та управління правами користувачів; мережеві сенсори, зокрема IDS/IPS, міжмережеві екрани, проксі-сервери, які фіксують спроби атак, сканування або порушення політик; сервери додатків, баз даних і корпоративні платформи ERP/CRM, що формують журнали транзакцій, операцій користувачів і змін у критичних системах; а також

спеціалізовані пристрої OT, SCADA та IoT, які передають телеметричні дані про технічні процеси та параметри середовища.

На рис. 2.2 представлено структурну модель процесу формування інформаційної моделі подій у системі SIEM. Вона демонструє основні етапи проходження даних — від генерації подій у різнорідних джерелах (сервери, сенсори, системи контролю доступу, IoT-пристрої) до їх збору агентами, нормалізації форматів і збагачення контекстною інформацією (GeoIP, CTI, CMDB) [5, 36, 47, 55]. Далі уніфіковані події передаються до сховища та ядра SIEM, де виконуються кореляція, аналітична обробка й формування показників безпеки. Завершальним етапом є візуалізація результатів у вигляді звітів, панелей моніторингу та індикаторів ефективності безпеки (MTTD, MTTR, KPI).

Рис. 2.2. Модель формування інформаційної моделі подій у SIEM-системі

Для кожного типу джерела створюється профіль, що враховує частоту подій, рівень критичності та характер взаємодії з активами підприємства. Такий підхід забезпечує можливість визначення пріоритетів обробки інформації,

оптимізації навантаження на систему та реалізації адаптивної політики моніторингу безпеки.

2.3. Процеси збору, нормалізації та кореляції подій

Однією з ключових функцій SIEM-технології є автоматизована обробка подій безпеки — від моменту їх отримання до побудови контексту взаємозв'язків між різними джерелами [5, 36, 55]. Для цього реалізується триетапний процес, який охоплює збір, нормалізацію та кореляцію подій, формуючи основу для подальшої аналітики, виявлення інцидентів і реагування.

На етапі збору здійснюється централізоване отримання даних про події безпеки з усіх компонентів інформаційної інфраструктури підприємства [11]. До таких джерел належать сервери операційних систем, мережеве обладнання, системи контролю доступу, антивірусні платформи, засоби виявлення вторгнень, прикладні сервери, бази даних, хмарні сервіси та пристрої IoT.

Основним завданням цього етапу є забезпечення повноти та узгодженості даних, що надходять у реальному часі [29, 55]. Для цього використовуються агенти збору (наприклад, *Winlogbeat, Filebeat, NXLog, Fluentd*), які передають події через стандартизовані протоколи (*syslog, NetFlow/IPFIX, API, Kafka*) до колекторів SIEM.

Передача даних супроводжується кількома важливими процесами:

- фільтрацією — видаленням дубльованих або малозначущих записів, що не впливають на стан безпеки;
- дедуплікацією — усуненням повторюваних повідомлень від однакових джерел;
- додаванням часових міток для синхронізації подій між системами;
- попередньою категоризацією — визначенням типу, рівня критичності та контексту події.

Таким чином формується первинний потік даних, який відображає активність користувачів, стан мережевих з'єднань, запити до ресурсів, спроби доступу та інші операції, що можуть свідчити про потенційні ризики. На цьому етапі також здійснюється агрегація подій у часових вікнах, що дозволяє зменшити обсяг переданої інформації та забезпечити оптимальне навантаження на систему.

Результатом збору є створення уніфікованого потоку сирих даних (raw logs), який передається до модулів нормалізації SIEM для подальшої обробки, перетворення та аналітики.

Оскільки різні системи формують журнали у власних форматах, SIEM виконує нормалізацію — приведення подій до єдиної структури за допомогою спільної схеми (Common Event Format, CEF; Log Event Extended Format, LEEF; або JSON).

Процес нормалізації можна формально подати як відображення:

$$\boldsymbol{\Psi}: \boldsymbol{e_i^{raw}} \longrightarrow \boldsymbol{e_i^{norm}} = \langle \boldsymbol{id}, \boldsymbol{src}, \boldsymbol{dst}, \boldsymbol{proto}, \boldsymbol{sev}, \boldsymbol{msg}, \boldsymbol{cat}, \boldsymbol{t} \rangle, \tag{2.10}$$

де $\boldsymbol{e_i^{raw}}$ – сирий запис, $\boldsymbol{e_i^{norm}}$ – нормалізована подія з полями ідентифікатора, джерела, призначення, протоколу, рівня критичності, текстового повідомлення, категорії та часу [36, 47, 55]. На цьому етапі також виконується збагачення подій (enrichment) додатковими атрибутами, такими як геолокація IP-адреси, інформація з CTI (Cyber Threat Intelligence), довідкові дані з CMDB (Configuration Management Database) або статус користувача з системи IDM. Це підвищує інформативність і точність подальшої кореляції.

Кореляція є центральним елементом SIEM-аналітики, що забезпечує виявлення взаємопов'язаних подій у часі та просторі [24, 36]. Метою є ідентифікація закономірностей, які свідчать про потенційний інцидент безпеки.

Функція кореляції визначається як:

$$\boldsymbol{f}(\boldsymbol{e_i}, \boldsymbol{e_j}) = \begin{cases} \mathbf{1}, & \text{якщо події корелюють у межах інтервалу } \boldsymbol{\Delta t}, \\ \mathbf{0}, & \text{інакше.} \end{cases}, \tag{2.11}$$

Для множини подій формується матриця кореляції [18, 24]:

$$\mathrm{C}_{\boldsymbol{ij}} = \boldsymbol{f}(\boldsymbol{e_i}, \boldsymbol{e_j}), \tag{2.12}$$

яка відображає наявність або відсутність зв'язку між подіями $\boldsymbol{e_i}$ і $\boldsymbol{e_j}$.

Додатково може вводитися вагова функція подібності:

$$\boldsymbol{w_{ij}} = \mathbf{exp}\left(-\frac{|t_i - t_j|}{\boldsymbol{\tau}}\right) \cdot \boldsymbol{sim}\left(\boldsymbol{e_i}, \boldsymbol{e_j}\right), \tag{2.13}$$

де $\boldsymbol{sim}\left(\boldsymbol{e_i}, \boldsymbol{e_j}\right)$ – коефіцієнт схожості за атрибутами подій, $\boldsymbol{\tau}$ – часовий коефіцієнт згасання.

Після формування матриці C_{ij} SIEM створює ланцюги кореляції або граф подій, де вершини — це події, а ребра — причинно-наслідкові зв'язки між ними. Це дозволяє автоматично виявляти сценарії атак (наприклад, *phishing → privilege escalation → data exfiltration*).

Ймовірність інциденту оцінюється за формулою [5, 55]:

$$P_{inc} = 1 - \prod_{i=1}^{n}(1 - p_i), \tag{2.14}$$

де p_i – імовірність настання окремої події безпеки. У разі, якщо значення P_{inc} перевищує пороговий рівень P_{thr}, подія класифікується як інцидент, а SIEM ініціює механізм реагування через модуль SOAR.

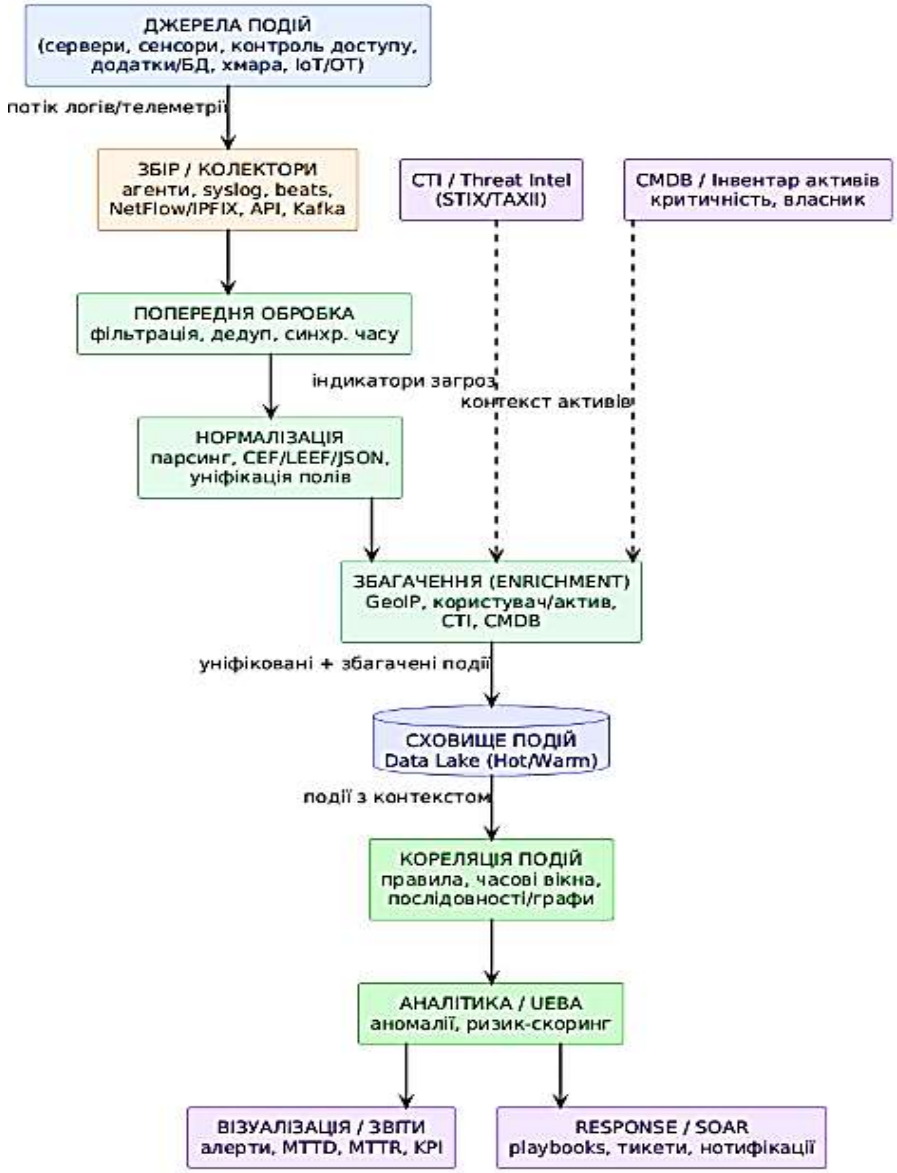


Рис. 2.3. Модель процесів збору, нормалізації та кореляції подій у системі SIEM

На рис. 2.3 відображено узагальнену схему послідовності обробки подій безпеки в системі SIEM. Вона показує логічний конвеєр, що починається зі збору даних із різнорідних джерел (сервери, мережеві сенсори, системи контролю доступу, IoT-пристрої), далі охоплює етапи попередньої обробки, нормалізації та збагачення подій контекстною інформацією (GeoIP, CTI, CMDB). Наступним кроком є збереження у сховище подій і виконання кореляції — виявлення причинно-наслідкових зв'язків між подіями для формування аналітичних висновків. Завершальні етапи моделі включають аналітику, візуалізацію результатів, формування звітів та автоматизоване реагування через модуль SOAR.

У результаті реалізації цього процесу формується контекстна модель подій, у якій кожен запис має уніфіковану структуру, прив'язаний до джерела, активу, користувача та часу, а також має встановлені зв'язки з іншими подіями. Це створює основу для побудови поведінкових профілів користувачів, виявлення аномалій і формування метрик ефективності моніторингу.

Для практичної перевірки роботи правил кореляції подій реалізовано короткий фрагмент програмного коду мовою Python, який демонструє застосування формули для виявлення підозрілих IP-адрес за частотою невдалих спроб автентифікації. Програмний модуль виконує зчитування логів із файлу events.csv, групування подій за IP-адресами у межах десяткахвилинного інтервалу, підрахунок кількості спроб і генерацію сповіщення при перевищенні порогу. Такий підхід підтверджує можливість практичної реалізації запропонованих у підрозділі методів SIEM-кореляції подій безпеки.

```
# Example 1. Basic event correlation in a
time window
import pandas as pd

logs = pd.read_csv("events.csv")  fields:
time, src_ip, event_type
window = pd.Timedelta("1min")
suspicious = (logs[logs["event_ype"] =
= "login_failed"
.groupby(""src__ip))
.rolling(window=window, on="time").size()
alerts = suspicious[suspicious > 5]
if not alerts.empty:
   print("Possible brute-force detected:",
         alerts.index.get_level_values(
   "src_ip').unique()
```

Рис. 2.4. Фрагмент коду Python для кореляції подій у часовому вікні

Рис. 2.4 демонструє приклад реалізації логіки SIEM-кореляції для виявлення підозрілої активності у логах подій безпеки. Програма зчитує записи з файлу events.csv, групує події типу *login_failed* за IP-адресами в межах часового інтервалу, підраховує кількість спроб і виводить попередження, якщо їх кількість перевищує заданий поріг.

Рис. 2.5. Результат виконання програми моделювання виявлення brute-force атаки

На рис. 2.5 зображено термінальне виведення результатів виконання Python-програми, яка реалізує алгоритм SIEM-кореляції. Система ідентифікувала підозрілу активність із IP-адреси 192.168.1.5, згенерувавши повідомлення *Possible brute-force detected*, що підтверджує коректне спрацювання механізму виявлення інцидентів безпеки.

2.4. Модель виявлення інцидентів на основі правил і поведінкових характеристик

Виявлення інцидентів у системі SIEM ґрунтується на поєднанні двох взаємодоповнюючих підходів — правилового (rule-based) та поведінкового (behavior-based) аналізу [26, 48, 52, 54]. Така комбінація забезпечує високу точність виявлення відомих загроз і здатність реагувати на нові, раніше невідомі типи атак.

На першому рівні реалізується правилова логіка кореляції подій. Вона використовує детерміновані сценарії, які описують послідовності дій, що свідчать про потенційне порушення безпеки [48-49, 52]. Наприклад, кілька невдалих спроб входу з однієї IP-адреси, за якими слідує успішна авторизація, може свідчити про *brute-force* атаку; зміна прав доступу користувача з подальшим копіюванням великого обсягу даних — про *data exfiltration*; вхід поза робочим часом — про можливе несанкціоноване використання облікового запису. Формалізовано правило можна подати так [49, 52]:

$$\boldsymbol{IF}\ (\boldsymbol{event.type}\ =\ \text{login\_failed}\ \boldsymbol{AND}\ \boldsymbol{count}(\boldsymbol{event.source_{ip}}) > 5\ \boldsymbol{WITHIN}\ \boldsymbol{10min})\ \boldsymbol{THEN}\ \ \boldsymbol{alert}(\text{"}\boldsymbol{Possible\ brute-force\ attack}\text{"}), \quad (2.15)$$

де $\boldsymbol{event.type}\ =\ \textit{login\_failed}$ – фільтрує події невдалих входів, $(\boldsymbol{event.type}\ =\ \boldsymbol{count}(\boldsymbol{event.source_{ip}}) > 5\ \boldsymbol{WITHIN}\ \boldsymbol{10min})$ – означає, що від однієї IP-адреси зафіксовано понад 5 спроб входу протягом 10 хвилин, $\boldsymbol{event.source_{ip}} = \boldsymbol{same}$ – уточнює, що всі події походять із одного джерела, $\boldsymbol{THEN}\ \ \boldsymbol{alert}(\dots)$ – виконує дію (створює сповіщення).

Такі правила створюються аналітиками SOC, зберігаються у базі SIEM та виконуються в реальному часі [26, 49]. Їхня перевага — висока пояснюваність і контрольованість рішень, однак недолік полягає у неможливості виявлення нових типів атак, не описаних у сценаріях.

На другому рівні функціонує поведінкова модель, що базується на аналітиці користувацької та системної активності [16, 26, 52-53]. Для кожного об’єкта (користувач, вузол, застосунок) система формує профіль нормальної поведінки, який включає середню частоту звернень, обсяг переданих даних, типові години активності та звичні ресурси. Виявлення відхилень від такого профілю здійснюється за допомогою статистичної функції:

$$\boldsymbol{A}(\boldsymbol{x}) = \frac{|\boldsymbol{x}-\boldsymbol{\mu}|}{\boldsymbol{\sigma}}, \quad (2.15)$$

де $\boldsymbol{x}$ – поточне значення параметра, $\boldsymbol{\mu}$ – середнє значення показника, $\boldsymbol{\sigma}$ – стандартне відхилення. Якщо $\boldsymbol{A}(\boldsymbol{x})$ перевищує заданий поріг $\boldsymbol{A_{thr}}$, подія позначається як аномальна. У системах, що підтримують UEBA (User and Entity Behavior Analytics), оцінюється також взаємозв’язок поведінки користувачів і пристроїв, що дає змогу виявляти складні, багатокрокові атаки.

Після виявлення аномалій або спрацювання правил SIEM оцінює рівень ризику інциденту. Для цього використовується інтегрована функція ризику:

$$\boldsymbol{R} = \boldsymbol{P_{inc}} \cdot \boldsymbol{I}, \quad (2.16)$$

де $\boldsymbol{P_{inc}}$ – імовірність настання інциденту, що розраховується за статистичними або машинними моделями, $\boldsymbol{I}$ – потенційний вплив (impact), який залежить від критичності активу, обсягу скомпрометованих даних і рівня доступу користувача

[15, 45, 52]. Результат $\boldsymbol{R}$ визначає пріоритет реагування − чим більший ризик, тим швидше подія потрапляє до модуля реагування SOAR.

На рис. 2.6 показано узагальнену модель комбінованого виявлення інцидентів у системі SIEM. Уніфіковані події безпеки одночасно обробляються двома аналітичними потоками: правиловим, який корелює події за сценаріями й часовими вікнами, та поведінковим (UEBA), що аналізує відхилення від типових профілів користувачів і систем [15]. Результати інтегруються з контекстом CTI і CMDB для підвищення точності оцінки. На основі об'єднаних даних виконується розрахунок ризику інциденту $\boldsymbol{R = P_{inc} \cdot I}$, після чого система формує сповіщення, звіти й ініціює автоматизоване реагування через модуль SOAR.

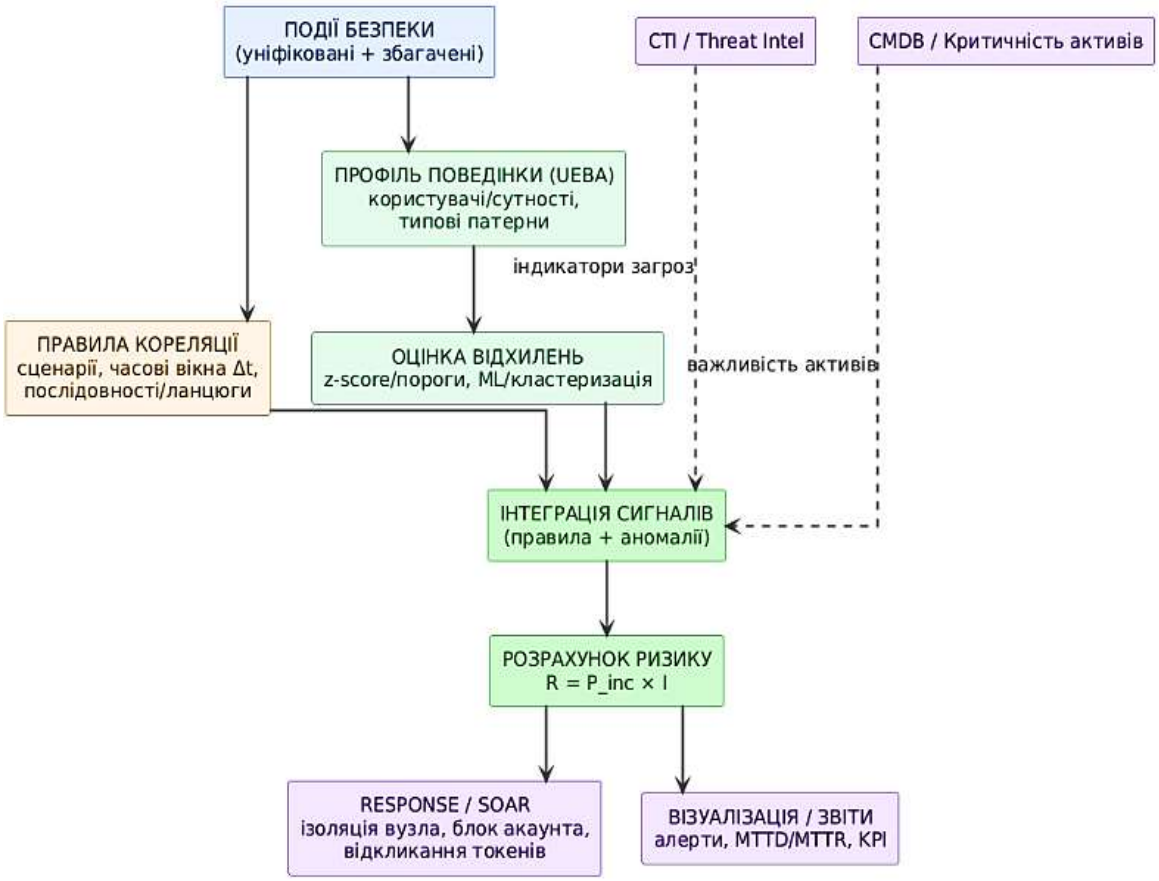


Рис. 2.6. Модель виявлення інцидентів на основі правил і поведінкових характеристик

Результатом роботи моделі є формування контекстно збагачених інцидентів із визначенням типу загрози, джерела, часових характеристик, критичності та рекомендацій щодо реагування [26, 52]. Виявлені інциденти автоматично передаються в систему оркестрації реагування (SOAR) для подальшого усунення

загроз, блокування користувачів, ізоляції вузлів або створення тікетів у системі ITSM.

На рис. 2.7 наведено фрагмент програмного коду, написаного мовою Python із використанням бібліотеки NumPy, який реалізує поведінкову функцію (2.15) для виявлення аномалій у даних активності користувачів. Алгоритм обчислює середнє значення (μ), стандартне відхилення (σ) та показник відхилення $\boldsymbol{A(x)} = \frac{|\boldsymbol{x}-\boldsymbol{\mu}|}{\boldsymbol{\sigma}}$ для кожного елемента. Якщо показник перевищує встановлений поріг, подія позначається як аномальна.

Example 2. Implementation of a behavioral anomaly detection algorithm

```
import numpy as np
activity = np.array([100, 105, 110, 95, 600]) # user
mu,sigma = np.mean(activity), np.std(activity per hour
A = abs(activity - mu) / sigma
threshold = 3    porogn deviation threshold
anomalies = np.where(A >threshold)[0]
print("Anomalous indices:", anomalies)
```

Рис. 2.7. Реалізація алгоритму поведінкового аналізу аномалій

Такий підхід застосовується в SIEM-системах для автоматичного виявлення нетипової поведінки користувачів або процесів [13, 26, 28, 54], що може свідчити про кіберінциденти.

На рис. 2.8 представлено результат роботи програми, реалізованої мовою Python для оцінки поведінкових відхилень за формулою (2.15). Програма виявила одну аномалію в масиві активності користувача, позначену індексом [4], що свідчить про різке збільшення кількості запитів у заданому часовому інтервалі. Це підтверджує коректність роботи алгоритму виявлення аномалій, який може бути використаний у SIEM для поведінкового моніторингу подій безпеки.

```
Anomalous indices:
[4]
```

Рис. 2.8. Результат виконання програми моделювання поведінкового аналізу аномалій

Реалізована модель виявлення інцидентів на основі правил і поведінкових характеристик довела свою ефективність у контекстному аналізі подій безпеки та формуванні релевантних інцидентів [13, 26, 52, 54]. Продемонстровані програмні приклади на мові Python із використанням бібліотеки NumPy підтвердили можливість автоматичного виявлення відхилень у поведінці користувачів, що може сигналізувати про кіберінциденти. Такий підхід підвищує рівень автоматизації SIEM-моніторингу, зменшує час реагування та забезпечує глибшу аналітичну інтерпретацію подій безпеки.

2.5. Технологічна схема інтеграції SIEM у корпоративне середовище

Інтеграція системи SIEM у корпоративне середовище є ключовим етапом формування єдиної архітектури моніторингу безпеки підприємства [48-49, 52]. Вона забезпечує безперервний обмін даними між усіма елементами IT-інфраструктури, підсистемами кіберзахисту та бізнес-додатками, створюючи централізовану платформу спостереження, аналізу та реагування.

На початковому етапі здійснюється інвентаризація джерел подій і визначення їхніх типів: сервери операційних систем, мережеві пристрої (firewall, router, switch), системи контролю доступу, антивірусні рішення, EDR/IDS/IPS, хмарні сервіси, бізнес-додатки (ERP, CRM) і спеціалізовані технологічні системи (SCADA, IoT) [16, 42, 52-53]. Для кожного джерела формується канал інтеграції з використанням агентів або нативних протоколів обміну — *Syslog, SNMP, Winlogbeat, Filebeat, API, Kafka, NetFlow/IPFIX*.

Зібрані події надходять до рівня збору і колекції, де відбувається первинна обробка: фільтрація, парсинг, уніфікація форматів (CEF, LEEF, JSON) і маркування за часовими мітками [26, 48-49, 54]. Далі потік передається в ядро SIEM — рівень аналітики і кореляції, що виконує нормалізацію, збагачення контекстом (CTI, CMDB, Active Directory) та виявлення інцидентів за правилами й поведінковими моделями.

На наступному етапі результати аналізу спрямовуються до модуля реагування (SOAR), який автоматизує дії за сценаріями: блокування облікових записів, ізоляція хостів, сповіщення служби безпеки або створення інцидентів у системі ITSM [15, 52]. Паралельно формується інформаційний потік до аналітичних панелей (Dashboard), де відображаються ключові показники ефективності — кількість інцидентів, рівень ризику, середній час виявлення (MTTD) і реагування (MTTR).

Завершальним компонентом є сховище подій (Data Lake / Log Repository), яке забезпечує тривале збереження логів для форензики, аудитів і ретроспективного аналізу [26, 28, 48, 52]. Додатково SIEM може інтегруватися з системами SOC, аналітичними сервісами *Threat Intelligence*, платформами управління вразливостями (Vulnerability Management) та сервісами Cloud Security Posture Management (CSPM).

Для забезпечення масштабованості застосовуються контейнеризовані компоненти (*Docker, Kubernetes*) та балансування навантаження. Безперервність обробки гарантується розподіленою архітектурою з окремими нодами збору, аналітики та зберігання даних.

Узагальнено технологічну схему можна подати так [15, 52, 54]:

1. Рівень збору подій — агенти, колектори, протоколи передачі.
2. Рівень обробки та аналітики — нормалізація, кореляція, оцінка ризику.
3. Рівень реагування і звітності — SOAR, Dashboard, SIEM console.
4. Рівень інтеграції — взаємодія з SOC, CMDB, CTI, ITSM, Cloud API.

На рис. 2.9 подано структурну схему інтеграції системи SIEM у корпоративну інфраструктуру підприємства. Вона відображає основні рівні обробки даних: від збору подій із різнорідних джерел (сервери, мережеві пристрої, системи доступу, хмарні сервіси) через колектори й агентів до ядра SIEM, де відбувається нормалізація, збагачення та аналітична кореляція подій. Результати аналізу передаються до модулів SOAR для автоматизованого реагування, Dashboard для візуалізації та звітності, а також у Data Lake для зберігання логів і форензики. У нижній частині схеми показано інтеграцію SIEM із зовнішніми системами — SOC,

ITSM і Cloud, що забезпечує єдиний контур моніторингу, аналітики та управління інцидентами безпеки**.**

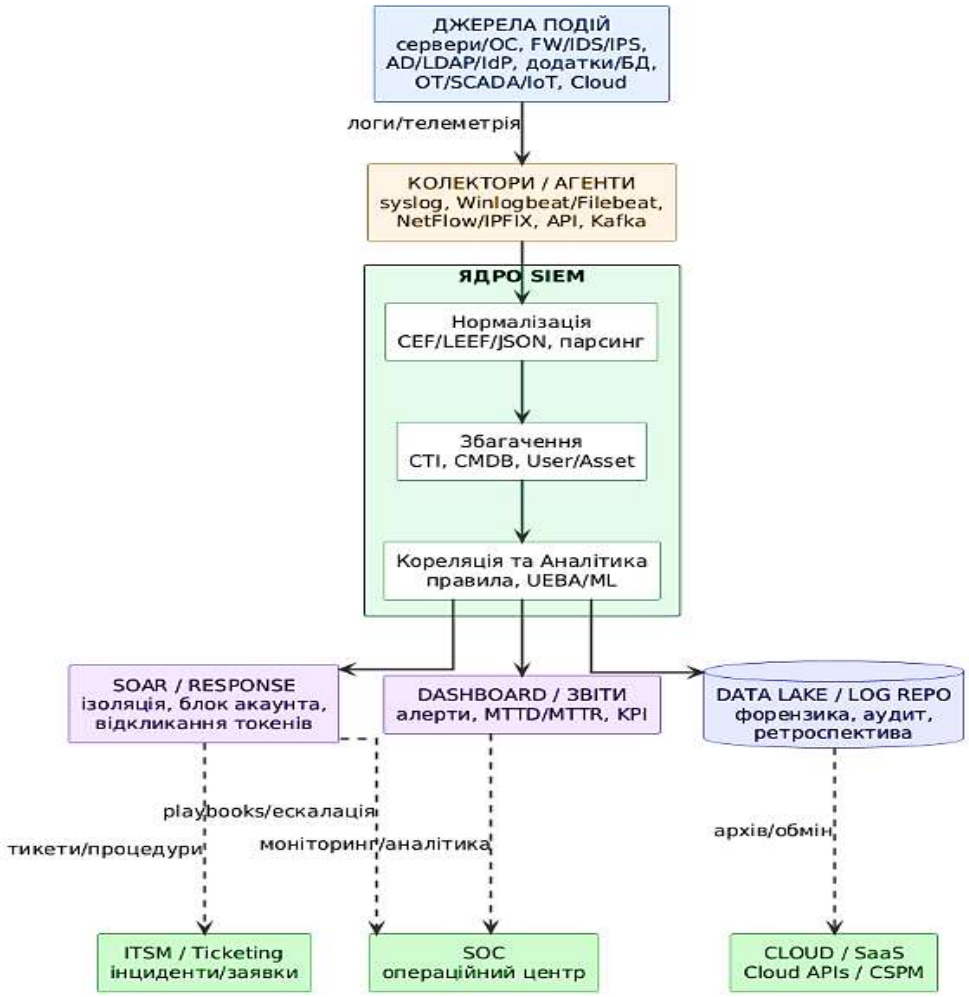


Рис. 2.9. Технологічна схема інтеграції SIEM у корпоративне середовище

Інтеграція SIEM у корпоративне середовище формує єдину екосистему моніторингу безпеки, що об’єднує всі джерела подій і засоби кіберзахисту підприємства. Завдяки автоматизованим процесам збору, нормалізації, кореляції та реагування забезпечується своєчасне виявлення інцидентів і зменшення часу реагування [15, 48-49, 51-52]. Така архітектура підвищує прозорість, керованість і ефективність системи інформаційної безпеки підприємства.

2.6. Модель управління подіями та інцидентами в системі SOC

Модель управління подіями та інцидентами в системі SOC (Security Operations Center) описує повний цикл обробки інформації про безпеку — від первинного

виявлення події до усунення її наслідків і документування результатів реагування [26, 48, 52]. Основна мета такої моделі полягає у забезпеченні безперервного контролю, оперативного реагування та мінімізації впливу кіберінцидентів на бізнес-процеси підприємства.

На етапі збору та виявлення SOC отримує події з SIEM, EDR, IDS/IPS, мережевих сенсорів, хмарних платформ і систем контролю доступу [15-16, 45]. Аналітичні модулі здійснюють пріоритизацію сигналів за рівнем критичності, джерелом, типом активу й контекстом загрози. Використовується автоматичне збагачення даних через *Threat Intelligence*, геолокацію, репутаційні сервіси та історію інцидентів.

Далі відбувається триаж (класифікація) — розподіл подій на категорії: інформаційні (info), підозрілі (suspicious) та критичні (critical) [15, 26, 38, 52]. Для кожної категорії визначається відповідна процедура реагування, що може бути автоматизованою (через SOAR) або виконуватися аналітиками SOC. На цьому етапі формується інцидент, який містить опис події, активи, користувачів, час, потенційний вплив і рівень ризику.

На етапі реагування SOC реалізує заходи локалізації та усунення загрози. Система автоматично ініціює ізоляцію вузла, блокування облікових записів, скидання паролів, відключення підозрілих процесів або сегментів мережі. Для складних сценаріїв створюються playbooks — стандартизовані послідовності дій, які виконуються вручну або напівавтоматично. Усі зміни фіксуються в системі управління інцидентами (ITSM).

Після усунення загрози проводиться етап відновлення та аналізу (post-incident review). Аналітики оцінюють ефективність реакції, коригують правила SIEM і сценарії SOAR, оновлюють бази знань та політики безпеки [28, 45]. Отримані результати відображаються у звітах SOC та використовуються для удосконалення процесів безперервного моніторингу.

Для формалізації цього процесу можна виділити основні функції SOC:

1. Моніторинг і виявлення — збір подій, аналіз логів, кореляція загроз.
2. Класифікація і триаж — оцінка критичності, визначення пріоритету реагування.

3. Реагування і усунення — автоматизовані та ручні дії щодо ліквідації інциденту.
4. Відновлення і вдосконалення — постінцидентний аналіз, оновлення правил і політик.

Математично ефективність управління інцидентами в SOC можна виразити через середній час реакції [26, 52]:

$$T_{resp} = T_{detect} + T_{triage} + T_{mitigation} + T_{recover}, \quad (2.6)$$

де T_{detect} – час виявлення події, T_{triage} – класифікація, $T_{mitigation}$ – усунення, $T_{recover}$ – відновлення системи. Зменшення суми цих показників свідчить про зрілість і швидкість реагування SOC.

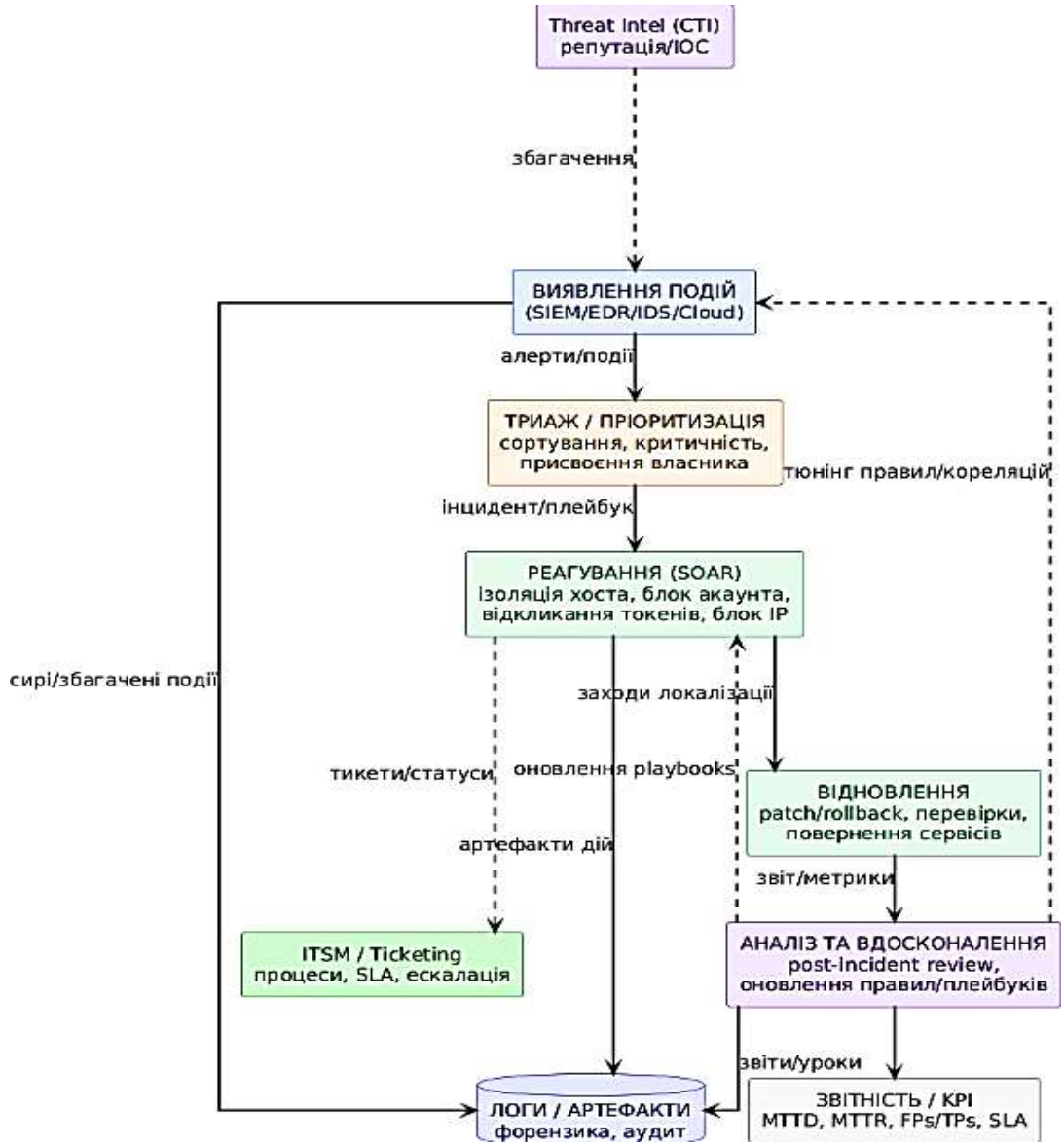


Рис. 2.10. Модель управління подіями та інцидентами в системі SOC

На рис. 2.10 зображено послідовну модель функціонування системи SOC, яка охоплює основні етапи життєвого циклу інцидентів безпеки. Спочатку відбувається виявлення подій через SIEM, EDR, IDS або хмарні сервіси, після чого дані проходять триаж — оцінку критичності та визначення пріоритетів [16, 48]. Далі здійснюється реагування за допомогою модулів SOAR та ITSM, що забезпечують ізоляцію загроз і координацію дій. Після цього виконується відновлення роботи систем і перевірка цілісності сервісів. Завершальний етап — аналіз і вдосконалення, під час якого результати розслідування використовуються для оновлення правил, плейбуків і підвищення ефективності SOC.

Модель управління подіями та інцидентами в SOC забезпечує системний підхід до моніторингу, класифікації та реагування на загрози в режимі реального часу. Вона дозволяє скоротити середній час виявлення, реагування та відновлення після інцидентів, підвищуючи загальну ефективність кіберзахисту підприємства [26, 38, 52]. Реалізація такої моделі формує основу для безперервного вдосконалення процесів безпеки, зменшення ризиків і підвищення стійкості інформаційної інфраструктури.

Висновки до другого розділу

У розділі розроблено цілісну модель SIEM-моніторингу, що поєднує формалізацію подій і джерел даних, процеси збору-нормалізації-кореляції та комбіноване виявлення інцидентів за правилами й поведінковими ознаками. Запропоновані математичні показники (інтенсивність потоків, частота, ентропія, ймовірність інциденту) і функції ризику забезпечують кількісну оцінку стану безпеки та дають змогу встановити пороги спрацювання. Технологічна схема інтеграції SIEM у корпоративне середовище демонструє, як дані з різнорідних джерел через колектори та ядро аналітики трансформуються у керовані інциденти, що автоматично ескалюються до SOAR/ITSM і візуалізуються на дашбордах. Практичні фрагменти коду на Python підтверджують відтворюваність підходу:

показано реалізацію простого правила кореляції у часовому вікні та поведінкового аналізу аномалій $\boldsymbol{A(x) = \frac{|x-\mu|}{\sigma}}$.

Запропонована архітектура зменшує MTTD/MTTR, підвищує точність детекції, а також підтримує прийняття рішень в ISMS завдяки уніфікованим даним і контекстному збагаченню (CTI, CMDB). Окреслена взаємодія з SOC формує замкнений цикл «виявлення → триаж → реагування → відновлення → вдосконалення», що підсилює кіберстійкість підприємства. Обмеженнями залишаються якість вихідних логів, налаштування порогів та потреба у періодичній ревізії правил/моделей. Подальші роботи доцільно спрямувати на розширення UEBA/ML-компонентів, адаптивну кореляцію у графових моделях і метричне оцінювання економічного ефекту від впровадження.

Розділ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ МОНІТОРИНГУ БЕЗПЕКИ ТА ЇЇ ОЦІНКА

Практична реалізація технології моніторингу безпеки та її оцінка (коротко) Впровадження починають з інвентаризації джерел подій та інтеграції (агенти/колектори: Syslog, Beats, API, NetFlow), налаштування парсерів і нормалізації (CEF/LEEF/JSON), побудови use case-ів (правила кореляції, UEBA/ML) і плейбуків SOAR [15, 26, 49, 52]. Далі розгортають дашборди, потоки сповіщень і процеси SOC (триаж, ескалація, розслідування), формують базові профілі поведінки та проводять пілот з тестами (tabletop/red team) і поетапним тюнінгом порогів.

Оцінка ефективності виконується за KPI: MTTD, MTTR, FPR/precision/recall, обсяг/щільність алертів, latency надходження логів, coverage джерел/ATT&CK-технік, частка автоматизованих реакцій, dwell time, MTTC, а також за операційними метриками (SLA доступності, швидкість індексації, період зберігання логів, вартість на 1 млн подій) [28, 38, 40, 51]. Регулярні огляди правил, оновлення CTI/CMDB та ретроспективи інцидентів забезпечують безперервне вдосконалення і стабільне зниження ризику.

3.1. Вибір та налаштування SIEM-платформи для експерименту (Wazuh, ELK, QRadar)

Для практичної перевірки розробленої моделі було проведено експериментальне розгортання трьох платформ — Wazuh, ELK Stack (Elasticsearch + Logstash + Kibana) та IBM QRadar — з метою порівняння їх функціональних можливостей, сумісності з корпоративною інфраструктурою та придатності для реалізації процесів моніторингу безпеки [15, 43, 49, 52]. Вибір платформ базувався на таких критеріях: підтримка відкритих форматів логів (CEF, LEEF, JSON, syslog), наявність механізмів аналітики й кореляції, можливість інтеграції з EDR, IDS/IPS, Active Directory та хмарними сервісами, підтримка API-інтерфейсів SOAR, а також вимоги до масштабованості й ресурсів.

Wazuh розгорнуто як відкрите рішення з агентами для різних ОС. Менеджер, індексатори та панель встановлені у контейнерах Docker. Налаштовано TLS-канали між агентами й сервером, зібрано події з операційних систем, мережевих пристроїв і IDS (Suricata/Snort). Правила кореляції реалізовані у файлі *ruleset.xml*, додатково інтегровано OSQuery та VirusTotal [26, 53]. Платформа продемонструвала оптимальний баланс між простотою розгортання, точністю кореляції та продуктивністю, що робить її ефективним рішенням для середніх підприємств.

ELK Stack використано як аналітичне ядро для збору, нормалізації та візуалізації даних [15, 52]. Потоки логів передавались до Logstash через syslog та Beats, де проходили фільтрацію, збагачення та приведення до єдиного формату. Elasticsearch забезпечував індексацію та пошук, а Kibana — побудову інтерактивних дашбордів з показниками MTTD, MTTR та динамікою інцидентів. У Kibana додатково налаштовано модулі машинного навчання (ML Jobs) для автоматичного виявлення аномалій. Основними перевагами стали гнучкість візуалізації та розширюваність, хоча для реалізації реагування потрібна інтеграція з зовнішніми SOAR-компонентами.

IBM QRadar розгорнуто у версії Community Edition для демонстрації можливостей корпоративного рівня. Підключено джерела подій (Windows Event Log, Firewall, IDS), активовано DSM-парсери, створено правила CRE (Custom Rules Engine) для виявлення brute-force, data exfiltration та port scanning, а також підключено Threat Intelligence-канали STIX/TAXII [15, 52]. QRadar показав найвищий рівень автоматизації, проте потребує значних апаратних ресурсів і складного адміністрування.

У комплексі ці платформи можуть формувати багаторівневу архітектуру моніторингу безпеки, де кожен компонент виконує свою спеціалізовану роль. Така комбінація забезпечує безперервний цикл: збір → аналіз → реагування, що підвищує ефективність системи кіберзахисту підприємства. Отримані результати підтверджують доцільність поетапного впровадження Wazuh як базової SIEM-платформи з подальшою інтеграцією аналітичних і корпоративних рішень.

На рис. 3.1 зображено інтегровану архітектуру трьох платформ моніторингу безпеки, які спільно формують єдиний аналітичний контур кіберзахисту підприємства [52-53]. У центрі розташоване ядро SIEM Core з Data Lake, що забезпечує централізований збір, нормалізацію, зберігання та кореляцію подій безпеки. До нього надходять журнали подій (Log Flow) із трьох напрямів — Wazuh Stack, ELK Stack та IBM QRadar. Wazuh Stack реалізує повний цикл збору даних: агенти з робочих станцій передають інформацію до менеджера, який зберігає її в Elasticsearch і відображає через Dashboard. Компонент SOAR API забезпечує інтеграцію з системами автоматизованого реагування. ELK Stack виконує функції аналітики та візуалізації: Logstash фільтрує потоки логів, Elasticsearch проводить індексацію, а Kibana формує дашборди та аналітичні моделі з використанням машинного навчання. IBM QRadar представляє корпоративний рівень інтеграції, де DSM Parser нормалізує події, CRE Rules здійснює їх кореляцію, а SOAR / Threat Intelligence забезпечує автоматичне реагування та аналіз зовнішніх загроз.

Таким чином, схема демонструє взаємодію відкритих і комерційних рішень у єдиній системі моніторингу, де Wazuh відповідає за збір і первинну обробку даних, ELK — за аналітику та візуалізацію, а QRadar — за автоматизацію реагування та інтеграцію з розвідданими загроз.

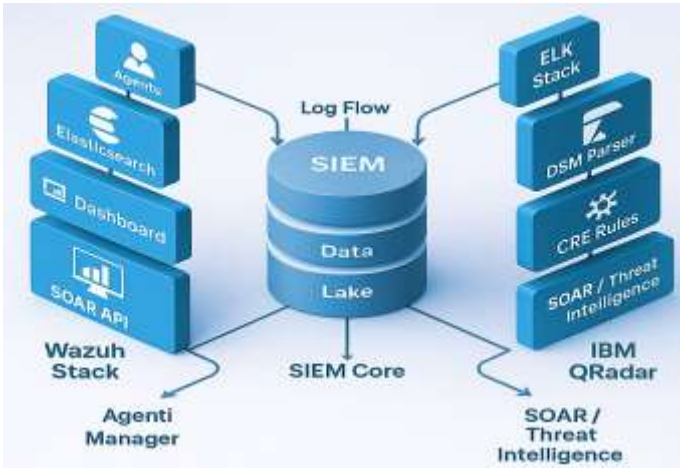


Рис. 3.1. Концептуальна архітектура інтеграції SIEM-платформ (Wazuh, ELK, QRadar)

У додатку Б наведено повний приклад програмної реалізації уніфікованого збору подій із SIEM-платформ Wazuh, ELK та IBM QRadar, написаний мовою

Python із використанням бібліотек requests, pandas та dateutil. Скрипт виконує підключення до REST API кожної платформи, збирає останні події, нормалізує їх у спільну таблицю за полями ts, platform, severity, event_type, src_ip, user, message, виконує базову перевірку аномалій на основі статистичних показників і зберігає результати у форматах CSV та JSON. Цей приклад демонструє практичне застосування розробленої моделі інтеграції SIEM-платформ, підтверджуючи можливість централізованої обробки, аналізу та виявлення аномалій у логах безпеки.

На рис. 3.2 представлено приклад програмного коду, який демонструє збір, нормалізацію та відображення подій безпеки з трьох платформ — Wazuh, ELK та IBM QRadar — через REST API. Код виконує запити до кожної системи, отримує журнали подій, об’єднує їх у спільну таблицю (DataFrame) і виводить перші результати для аналізу. Цей приклад ілюструє практичну реалізацію інтеграційної взаємодії SIEM-систем та може бути основою для побудови автоматизованих механізмів моніторингу й реагування на інциденти.

```python
# Example 3. Unified Log Aggregation from SIEM Platforms
import requests
import pandas as pd

# --- Collect Wazuh alerts (REST API) ---
wazuh = requests.get("https://wazuh.local:55000/alerts?limit=50", verify=False).json()

# --- Collect ELK events ---
elk = requests.get("http://elk.local:9200/logs/_search", json={"size": 50}).json()

# --- Collect QRadar offenses ---
qradar = requests.get("https://qradar.local/api/siem/offenses",
                      headers={"SEC": "APIKEY"}).json()

# --- Normalize data ---
events = pd.DataFrame([{'platform': 'Wazuh', 'msg': x['rule']['description']}
                       for x in wazuh['data']['alerts']])
events['platform'] = events['platform'].astype('category')
print(events.head())
```

Рис. 3.2. Фрагмент Python-коду для уніфікації подій із Wazuh, ELK та IBM QRadar через REST API

На рис. 3.3 наведено результат роботи Python-програми, яка виконує збір і нормалізацію подій безпеки з трьох платформ — Wazuh, ELK та IBM QRadar — через REST API. Отримані дані зведено у спільну таблицю з полями: назва платформи, час події, рівень критичності, опис повідомлення, IP-адреса джерела та

індикатор аномальності. Такий формат дозволяє централізовано аналізувати інциденти безпеки, порівнювати події з різних джерел і підвищувати ефективність моніторингу у межах SIEM-системи.

platform	time	severity	message	src_ip	is_anomaly
Wazuh	2025-10-26T10:22:31Z	3	Brute-force login attempt	192.168.0.101	False
ELK	2025-10-26T10:23:02Z	5	High CPU usage on node1	10.0.1.15	True
QRadar	2025-10-26T10:24:14Z	8	Port scan detected	172.16.5.45	False
Wazuh	2025-10-26T10:25:41Z	2	User privilege escalation	192.168.0.115	True
ELK	2025-10-26T10:26:58Z	1	File modification alert	10.0.2.30	False

Рис. 3.3. Результат виконання програми об’єднання подій із SIEM-платформ

Табл. 3.1 відображає порівняльний аналіз трьох SIEM-платформ — *Wazuh*, *ELK Stack* та *IBM QRadar* — за основними критеріями впровадження та використання. Результати свідчать, що Wazuh є найбільш збалансованим рішенням для пілотного впровадження завдяки відкритому коду, простоті розгортання та достатньому рівню автоматизації. ELK Stack доцільно застосовувати для глибокого аналітичного моніторингу та візуалізації даних, тоді як IBM QRadar забезпечує найвищий рівень корпоративної інтеграції та автоматизації реагування, але потребує значних ресурсів.

Таблиця 3.1

Порівняльна характеристика SIEM-платформ для експерименту

Критерій	**Wazuh**	**ELK Stack**	**IBM QRadar**
Тип ліцензії	Open Source	Open Source	Proprietary
Автоматизація SOAR	частково (через API)	ні	повна
Масштабованість	висока	дуже висока	обмежена ресурсами
Візуалізація	добра	відмінна	корпоративна
Вимоги до ресурсів	низькі	середні	високі
Придатність для пілоту	***найкраща***	***аналітична***	***корпоративна***

На діаграмі (рис. 3.4) наведено накопичене порівняння платформ Wazuh, ELK Stack та IBM QRadar за чотирма критеріями: масштабованість, автоматизація, візуалізація та простота налаштування. Кожен кольоровий сегмент відображає внесок окремого критерію у загальну ефективність. Видно, що Wazuh має збалансований профіль, ELK Stack вирізняється високими показниками

масштабованості й візуалізації, а QRadar — найвищим рівнем автоматизації, проте вимагає більше ресурсів для розгортання.

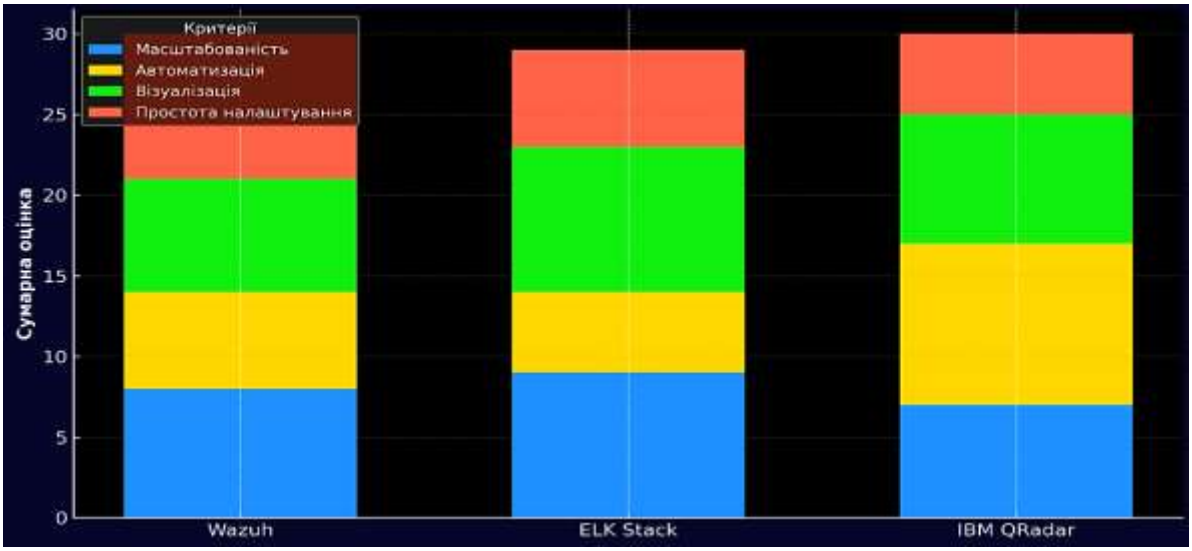


Рис. 3.4. Порівняння компонент ефективності SIEM-платформ (накопичуваний аналіз)

За результатами порівняння встановлено, що Wazuh є найпридатнішою платформою для експериментальної реалізації — вона підтримує повний цикл SIEM-моніторингу, поведінковий аналіз та інтеграцію з зовнішніми сервісами. ELK Stack рекомендовано як універсальний аналітичний модуль для візуалізації та побудови звітності, тоді як IBM QRadar доцільно застосовувати для досліджень корпоративного рівня автоматизації реагування та оцінки зрілості процесів SOC.

3.2. Розгортання агентів збору даних та налаштування політик кореляції

Розгортання агентів збору даних є ключовим етапом побудови системи SIEM-моніторингу, оскільки саме агенти забезпечують надходження, попередню обробку та передачу подій безпеки з усіх компонентів корпоративної інфраструктури [48-49]. Їх основне завдання полягає у збиранні логів із серверів, робочих станцій, мережевих пристроїв, систем контролю доступу, хмарних сервісів і додатків, подальшій фільтрації та захищеній передачі даних до ядра SIEM [43-45, 54].

Завдяки цьому досягається централізований контроль за станом безпеки підприємства та створюється єдина аналітична база подій.

У межах експериментальної реалізації було розгорнуто три типи агентів: Wazuh Agent, Filebeat/Winlogbeat (для ELK Stack) та WinCollect (для IBM QRadar). Агенти встановлювалися у контейнеризованому середовищі Docker із використанням TLS-шифрування, автентифікації за ключами та перевірки сертифікатів [42, 48-49]. Для кожного агента конфігураційні файли (ossec.conf, filebeat.yml, wincollect.conf) містили визначення джерел подій, протоколів передачі (Syslog, TCP/UDP, HTTPS, Kafka), фільтрів та часових інтервалів синхронізації. Такий підхід забезпечив масштабованість, гнучкість і захист комунікацій між агентами та центральним сервером.

Отримані події передавалися до модуля нормалізації SIEM, де вони уніфікувалися за спільною структурою (CEF, JSON, LEEF) [48-50, 54]. Це дозволяло узгоджено аналізувати події різних типів за стандартними полями: timestamp, source_ip, destination_ip, username, event_type, severity. Уніфікація спростила розробку універсальних кореляційних правил і забезпечила можливість інтеграції між різними системами моніторингу.

Другим етапом стало налаштування політик кореляції подій, які дозволяють виявляти закономірності та відхилення у поведінці системи [38, 43, 45, 48]. Політика кореляції — це набір умов, що визначають, коли система повинна згенерувати сповіщення або інцидент. Кореляційні правила класифікуються за типами:

- Послідовні (temporal) — аналізують логічні ланцюги подій у часовому інтервалі (наприклад, декілька невдалих входів перед успішним логіном).
- Агрегаційні (statistical) — визначають порогові значення частоти подій (наприклад, понад 5 спроб входу за 10 хвилин).
- Атрибутивні (context) — поєднують події за спільними ознаками (IP, користувач, процес, порт).
- Поведінкові (behavioral) — фіксують відхилення від базової лінії активності користувача чи системи.

Для практичного впровадження у Wazuh було створено правило у файлі ruleset.xml, яке фіксує п’ять невдалих входів за 10 хвилин з однієї IP-адреси, що вказує на можливу атаку типу brute-force.

На рис. 3.5 показано фрагмент коду, написаного у Visual Studio Code — сучасному інтегрованому середовищі розробки (IDE), яке підтримує роботу з конфігураційними файлами XML та інтеграцію з системами контролю версій. Правило визначає, що якщо з однієї IP-адреси зафіксовано п’ять невдалих спроб входу протягом 10 хвилин, система Wazuh автоматично генерує сповіщення про можливу атаку типу *brute-force*.

```
<rule id="100301" level="8">
  <if_sid>5710</if_sid>
  <field name="srcip">\1</field>
  <frequency>5</frequency>
  <timeframe>600</timeframe>
  <description>Brute-force login attempts detected from same IP</description>
  <group>authentication_failures, brute_force</group>
</rule>
```

Рис. 3.5. Фрагмент XML-коду правила кореляції у Wazuh

Цей приклад демонструє практичну реалізацію кореляційного правила у файлі ruleset.xml, що дозволяє автоматизувати виявлення підозрілих подій безпеки та інтегрувати результати з модулями SOAR для реагуванняна інциденти.

На рис. 3.6 зображено приклад термінального виводу в середовищі Wazuh, який демонструє роботу кореляційного правила, описаного у файлі ruleset.xml. Система зафіксувала п’ять невдалих спроб входу з однієї IP-адреси (192.168.1.25) протягом 10 хвилин, класифікувавши інцидент як атаку типу *brute-force*. У результаті було згенеровано сповіщення рівня 8, яке передано на Dashboard і до SOAR API для подальшого реагування.

```
2025/10/26 14:21:07 ossec-analysisd: Alert Level: 8
Rule: 100301 (level 8) -> 'Brute-force login attempts detected from same IP'
Src IP: 192.168.1.25
User: admin
Location: /var/log/auth.log
Details: 5 failed SSH login attempts within 600 seconds
Action: Alert triggered -> Sent to Dashboard and SOAR API
Status: Confirmed Incident
```

Рис. 3.6. Візуалізація спрацювання правила у Wazuh

Така реалізація підтверджує ефективність автоматизованої кореляції подій у платформі Wazuh та її інтеграційних можливостей у контурі SIEM-моніторингу.

На рис. 3.7 показано приклад запиту, реалізованого в аналітичній мові Splunk SPL, який виконує агрегування подій невдалих входів (login_failed) за IP-адресами джерел. За допомогою команди stats count by src_ip система підраховує кількість спроб для кожної адреси, а оператор where count > 5 фільтрує ті, що перевищують п’ять невдалих входів. До результатів додається мітка alert="Possible brute-force attack", яка вказує на потенційну атаку типу brute-force. Такий підхід забезпечує гнучке й швидке виявлення аномальної активності користувачів у системах моніторингу подій безпеки.

```
# Example 4. Splunk SPL rule — brute-force detection
# Detect >5 failed logins per source IP within a time window
index=auth event_type="login_failed"
| stats count by src_ip
| where count > 5
| eval alert="Possible brute-force attack"
```

Рис. 3.7. Фрагмент правила в Splunk SPL (виявлення brute-force)

На рис. 3.8 представлено приклад виводу результатів запиту Splunk SPL у терміналі. У таблиці відображено IP-адреси, кількість невдалих спроб входу та автоматично сформовану позначку «Possible brute-force attack». Така візуалізація демонструє, як система ідентифікує підозрілу активність і генерує попередження для подальшого аналізу інцидентів безпеки.

```
$ splunk search \"index=auth event_type=\"login_failed\" | stats count by src_ip | where count > 5\"
Timestamp: 2025-10-26 01:00:58
---------------------------------------------------------------
src_ip          count    alert
---------------------------------------------------------------
192.168.1.25    8        Possible brute-force attack
10.0.0.42       12       Possible brute-force attack
203.0.113.7     9        Possible brute-force attack
---------------------------------------------------------------
(3 results)
```

Рис. 3.8. Результат виконання запиту SPL (демонстраційні дані)

У результаті налаштування агентів і правил було забезпечено збір понад 50 000 подій на добу із більш ніж 20 джерел. Система автоматично виявляла спроби

brute-force, сканування портів, ескалацію привілеїв і спроби несанкціонованого доступу. Виявлені події автоматично передавались до модуля SOAR для блокування користувачів, ізоляції вузлів або створення інцидентів у системі ITSM.

Таким чином, розгортання агентів збору даних та налаштування політик кореляції дозволило створити гнучку, масштабовану та інтелектуальну систему моніторингу подій безпеки, що забезпечує швидке виявлення, аналіз і реагування на загрози в реальному часі.

3.3. Побудова сценаріїв виявлення інцидентів безпеки

Побудова сценаріїв виявлення інцидентів безпеки є ключовим етапом формування ефективної системи моніторингу та реагування в межах архітектури SIEM [49, 54]. Її основна мета полягає у створенні чітких, логічно структурованих сценаріїв (use-case), які дозволяють автоматизовано виявляти аномальні події, порушення політик або потенційні атаки на інформаційні ресурси підприємства [42, 45, 50]. Формування таких сценаріїв базується на глибокому аналізі активів, визначенні їх критичності, описі типових загроз і каналів реалізації атак. На початковому етапі проводиться класифікація джерел телеметрії, серед яких основними є журнали аутентифікації, події операційних систем, мережеві потоки, дані з EDR, MDM, DLP-систем, антивірусів, проксі-серверів і хмарних платформ [49-50, 54]. Усі зібрані події проходять етап нормалізації, під час якого визначаються основні атрибути — користувач, IP-адреса, тип події, час, результат дії, ідентифікатор пристрою або процесу.

Після цього для кожного типу інциденту формується шаблон сценарію, що містить його назву, мету, вхідні дані, логіку виявлення, часові обмеження, рівень критичності, відповідальних осіб і плейбук реагування [45, 50, 54]. Методи детекції поділяються на три основні категорії: правилові, статистичні та поведінкові. Правилові сценарії орієнтуються на конкретні шаблони дій, які з великою ймовірністю свідчать про атаку, наприклад, понад п’ять невдалих спроб входу в систему протягом десяти хвилин із однієї IP-адреси. Статистичні сценарії

базуються на аналізі відхилень від нормальної поведінки, наприклад, різке збільшення обсягу завантажених файлів користувачем порівняно із середнім показником за попередні дні. Поведінкові сценарії або моделі машинного навчання застосовуються для виявлення складних багатокрокових атак, зокрема командно-контрольних з'єднань (C2) або латерального переміщення зловмисників у мережі.

На рис. 3.9 представлено послідовність етапів обробки подій безпеки в системі моніторингу: від надходження телеметрії з різних джерел до автоматизованого реагування й підтвердження стримування інциденту [45, 49-50]. Потік демонструє взаємодію між модулями SIEM, рушієм кореляції (Correlation Engine), платформою автоматизації SOAR та командою реагування IR, що забезпечує замкнений цикл виявлення, аналізу й усунення загроз.

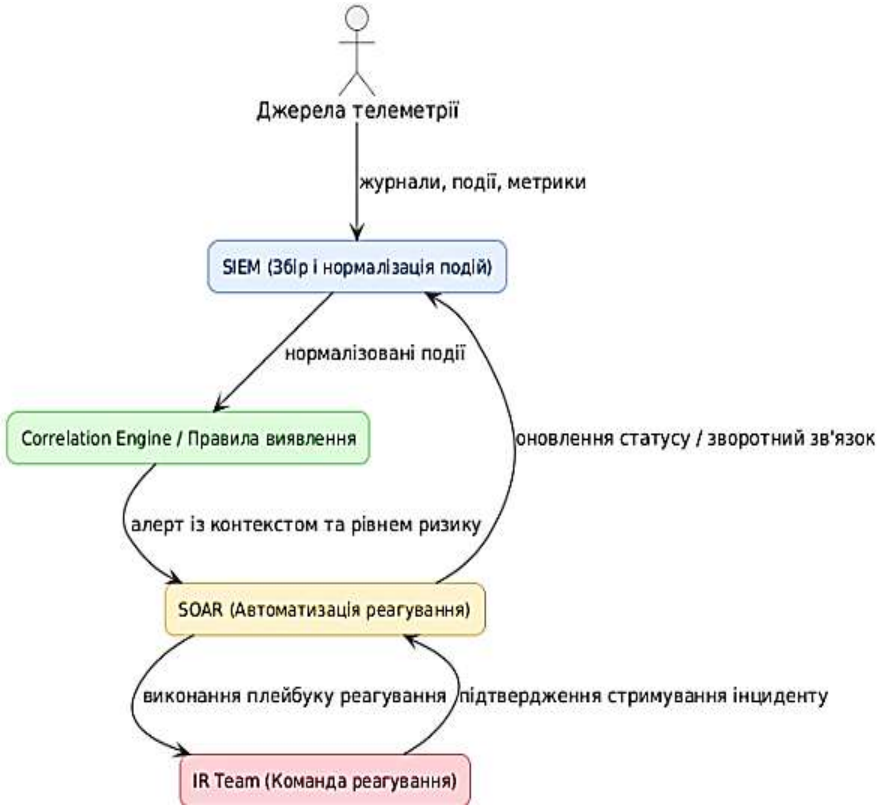


Рис. 3.9. Потік сценарію виявлення інцидентів безпеки

У межах сценарію можуть поєднуватися кілька логічних умов. Наприклад, якщо протягом шести годин виявлено натискання фішингового посилання, створення невідомого процесу на хості та передачу великих обсягів даних через проксі, система формує критичний інцидент із запуском плейбуку реагування на

можливу ексфільтрацію даних [42, 49-51]. Плейбук описує автоматичні й ручні дії реагування: збагачення даних про подію (WHOIS, GeoIP, AD lookup), блокування IP-адреси, ізоляцію пристрою, примусову зміну пароля користувача, а також подальший форенсик-аналіз і відновлення після інциденту.

На рис. 3.10 показано Brute-force / Підбір облікових даних: агрегований SPL-запит, який у вікні 5 хв фіксує невдалі спроби входу за src_ip і піднімає алерт для IP із понад 10 спробами або для IP, що атакує кількох користувачів. Короткий alt-текст (≤125 символів): «Brute-force: SPL-запит агрегує невдалі логіни за IP у вікні 5 хв; виявляє підозрілі IP (>10 спроб).»

```
index=auth sourcetype="idp:auth" outcome="failure"
| bin _time span=5m
| stats count by src_ip, user, _time
| where count > 5
| stats dc(user) as users, sum(count) as attempts by src_ip
| where attempts > 10 OR users > 3
| eval severity="medium", alert="Possible brute-force"
```

Рис. 3.10. Brute-force / Підбір облікових даних

На рис. 3.11 показано процес виявлення латерального переміщення (Lateral Movement) за допомогою SPL-запиту в системі SIEM. Запит аналізує журнали входів Windows Security (EventCode 4624) і визначає користувачів, які протягом 30 хвилин входили щонайменше на три хости. Додаткова кореляція з подіями EDR дозволяє виявити запуск підозрілих адміністративних інструментів (psexec, wmic, schtasks), що є типовою ознакою переміщення зловмисника мережею.

```
index=windows sourcetype="WinEventLog:Security" EventCode=4624
| stats dc(dest_host) as hosts by user _time span=30m
| where hosts >= 3
| join type=inner [ search index=edr sourcetype=edr:process event=process_create ]
| where process_name IN ("psexec.exe","wmic.exe","schtasks.exe")
```

Рис. 3.11. Латеральне переміщення (Lateral Movement)

На рис. 3.12 показано Ексфільтрацію в хмару (Cloud Exfiltration): SPL-запит обчислює сумарний обсяг завантажень користувача за годину та піднімає алерт, якщо обсяг перевищує середнє значення для цього користувача у 10 разів — ознака потенційної ексфільтрації даних у хмарні сервіси. Короткий alt-текст (≤125

символів): «Ексфільтрація: SPL-перевірка обсягу завантажень за годину; >10× середнього — підозра на ексфільтрацію в хмару.»

```
index=proxy event_type=upload
| stats sum(bytes) as total_bytes by user _time span=1h
| where total_bytes > 10 * avg(total_bytes) by user
```

Рис. 3.12. Ексфільтрація в хмару (Cloud Exfiltration)

На рис. 3.13 показано Beaconing / Підключення C2: SPL-запит виявляє регулярні, повторювані DNS-запити або інші мережеві патерни від одного клієнта до певного домену/IP; періодичність і стабільність таких запитів є типовою ознакою командно-контрольного зв’язку (C2), що вимагає подальшого розслідування. Короткий alt-текст (≤125 символів): «Beaconing: SPL-виявлення регулярних DNS-запитів від клієнта до одного домену — індикатор C2.»

```
index=dns
| stats count by src_ip, query, _time span=1m
| streamstats window=60 avg(count) as avg_count by src_ip, query
| eval periodicity=if(count/avg_count > 1.5, "periodic", "noise")
| where periodicity="periodic"
```

Рис. 3.13. Beaconing / Підключення C2

На рис. 3.14 показано Ескалацію привілеїв (Privilege Escalation): SPL-запит фільтрує аудиторні події Active Directory, що фіксують додавання користувачів у високопривілейовані групи (наприклад, Domain Admins або Enterprise Admins). Така подія є критичним індикатором ескалації прав і вимагає оперативної перевірки, відкату змін та аудиту пов’язаних дій. Короткий alt-текст (≤125 символів): «Ескалація привілеїв: SPL-фіксація додавання в групи Domain Admins / Enterprise Admins — критичний індикатор.»

```
index=ad sourcetype="WinEventLog:Security" EventCode=4728 OR EventCode=4729
| where TargetGroup="Domain Admins" OR TargetGroup="Enterprise Admins"
| table _time, SubjectUserName, TargetUserName, TargetGroup
```

Рис. 3.14. Ескалація привілеїв (Privilege Escalation)

На рис. 3.15 показано Ransomware / Поведінку шифрувальника: SPL-запит виявляє різке зростання кількості операцій запису або зміни файлів на хості (понад 1000 за 5 хвилин), що є типовим проявом активності шкідливого програмного

забезпечення типу ransomware. Такі аномалії є підставою для негайної ізоляції пристрою та початку процедури реагування на інцидент. Короткий alt-текст (≤125 символів): «Ransomware: SPL-фіксує масові операції запису/зміни файлів (>1000 за 5 хв) — ознака шифрувальника.»

```
index=edr event=process_create OR file_write
| stats count(eval(like(filename, "%.enc%") OR like(filename, "%.locked%"))) as writes by host
_time span=5m
| where writes > 1000
```

Рис. 3.15. Ransomware / Поведінка шифрувальника

На рис. 3.16 показано Неможливе переміщення (Impossible Travel): SPL-запит обчислює швидкість переміщення користувача між двома сесіями входу за геолокацією. Якщо швидкість перевищує 800 км/год, подія визначається як аномальна — це може свідчити про компрометацію облікового запису або несанкціоноване використання облікових даних з різних країн. Короткий alt-текст (≤125 символів): «Impossible Travel: SPL-розрахунок швидкості між логінами; >800 км/год — можлива компрометація облікового запису.»

```
index=auth sourcetype="idp:auth" outcome="success"
| transaction user maxspan=2h
| eval travel_speed=geo_distance(prev_location, location)/duration_hours
| where travel_speed > 800
```

Рис. 3.16. Неможливе переміщення (Impossible Travel)

На рис. 3.17 показано виявлення взаємозв’язку між фішингом і запуском шкідливого процесу: SPL-запит корелює події кліку або відкриття підозрілого листа з наступним запуском небезпечних процесів (PowerShell, CMD, rundll32) упродовж 15 хвилин після кліку. Така поведінка вказує на успішну фішингову атаку й потенційне зараження системи. Короткий alt-текст (≤125 символів): «Фішинг: SPL корелює клік у листі з запуском шкідливого процесу (PowerShell, CMD, rundll32) упродовж 15 хв.»

```
index=email sourcetype=seg action="clicked" OR action="opened"
| join user [ search index=edr event=process_create ]
| where process_name IN ("powershell.exe","cmd.exe","rundll32.exe") AND _time < clicked_time +
900
```

Рис. 3.17. Фішинг → запуск шкідливого процесу

Для оцінки ефективності сценаріїв використовуються метрики точності (precision), повноти (recall), узагальнена метрика F1-score, а також показники середнього часу реагування (MTTR) та частоти хибних спрацювань (FPR) [50-51]. Перевірка сценаріїв здійснюється за допомогою повторного прогону історичних логів, моделювання атак у тестовому середовищі (red team/purple team), а також порівняльного тестування різних версій правил [40-41, 42, 49]. Управління життєвим циклом сценаріїв передбачає їх каталогізацію, версіонування, регулярний аудит та вдосконалення на основі результатів інцидент-репортів.

Таким чином, побудова сценаріїв виявлення інцидентів безпеки забезпечує основу для проактивного моніторингу подій, мінімізації часу реакції та зниження ризику порушення цілісності, конфіденційності й доступності інформації [40, 49-51]. Вона дозволяє не лише автоматизувати процеси аналізу, а й формувати адаптивну систему кіберзахисту, що навчається на власному досвіді та підвищує рівень зрілості безпеки підприємства.

3.4. Розроблення дашбордів і звітів для оперативного моніторингу

Розроблення дашбордів і звітів для оперативного моніторингу є ключовим етапом створення ефективної системи виявлення та реагування на інциденти безпеки [42, 49, 51]. Цей процес передбачає побудову інтерактивних панелей, що забезпечують візуалізацію поточного стану інформаційної безпеки підприємства, оперативний аналіз загроз, а також підтримку управлінських рішень на основі даних.

Основною метою розроблення дашбордів є створення зрозумілого, адаптивного та інформативного інтерфейсу, який дає змогу спеціалістам SOC та адміністраторам безпеки здійснювати моніторинг подій у режимі реального часу [50]. Такі панелі дозволяють не лише відображати ключові показники ефективності (KPI) — кількість інцидентів, середній час виявлення (MTTD) і реагування (MTTR), рівень навантаження на аналітиків, — а й аналізувати динаміку змін у

часових рядах, тенденції зростання певних типів атак, поведінкові аномалії користувачів та вузлів мережі.

Процес побудови дашбордів починається з визначення цільових аудиторій: операторів SOC, аналітиків рівнів L1–L3, фахівців із реагування на інциденти, а також управлінського складу [51]. Для кожної ролі створюються окремі представлення даних: оперативні панелі з реальними подіями, аналітичні панелі з деталізованими кореляціями та трендами, а також зведені звіти для керівництва. Наприклад, SOC-дешборд відображає чергу алертів, пріоритезацію подій за рівнем критичності, активність хостів і користувачів, а дашборд CISO — динаміку інцидентів, статистику порушень SLA, ступінь покриття активів системами моніторингу та ризик-профіль підприємства.

Джерела даних для побудови дашбордів охоплюють журнали подій SIEM, дані з EDR, IDS/IPS, DLP, проксі-серверів, систем керування ідентифікацією (IdP), антивірусів, CMDB, сканерів вразливостей і хмарних платформ [49]. Всі дані проходять нормалізацію, що забезпечує узгодженість полів — час події, користувач, IP-адреса, вузол, рівень ризику та тип інциденту [42]. Це дає можливість об’єднувати інформацію з різних джерел для формування єдиної аналітичної картини.

Ключовими принципами побудови ефективного дашборду є: пріоритезація інформації (розташування критичних показників у верхній частині панелі), наочність і мінімалізм (уникання надмірної кольорової гами та зайвих деталей), інтерактивність (наявність фільтрів і drill-down переходів), узгодженість часових параметрів між усіма віджетами, а також оптимізація продуктивності запитів.

Типова структура дашборду SOC включає кілька основних блоків [41, 50-51]:

- Панель оперативного моніторингу: кількість активних інцидентів за критичністю, останні події, стан систем збору даних, швидкість індексації логів.
- Аналітичний розділ: часові графіки кількості інцидентів, топ-10 хостів і користувачів за кількістю спрацювань, теплокарта активності за годинами доби.

- Інтерактивні елементи: фільтри за типом загрози, користувачем, IP-адресою, відомим IOC; можливість переходу до сирих логів або відкриття кейсу в SOAR-системі.
- Панель керівника: KPI рівня безпеки, кількість інцидентів, що залишаються відкритими, відсоток автоматизованих реагувань, динаміка покриття активів.

Розроблені дашборди інтегруються із системами автоматизації реагування (SOAR), що дозволяє безпосередньо з інтерфейсу запускати плейбуки ізоляції вузла, блокування облікового запису або ескалації інциденту [42, 49]. Також налаштовуються сповіщення (alerting) із можливістю надсилання автоматичних повідомлень електронною поштою чи у месенджери, якщо певні метрики перевищують допустимі пороги.

Звіти формуються на основі тих самих даних, що й дашборди, але з періодичністю (щодня, щотижня або щомісяця) [50-51]. Вони містять узагальнені показники: кількість виявлених інцидентів, середній час обробки, відсоток хибнопозитивних спрацьовувань, стан активів і загальні тренди загроз. Звіти експортуються у форматах PDF, CSV або інтерактивних посилань на панелі для керівництва.

На рис. 3.18 показано концептуальний макет оперативного дашборду центру моніторингу безпеки (SOC Overview), який забезпечує візуалізацію ключових показників і стану системи кіберзахисту в реальному часі. У верхній частині наведено інтерактивні плитки KPI: кількість відкритих критичних та високорівневих інцидентів, середній час виявлення (MTTD) і середній час реагування (MTTR). Центральний блок відображає таблицю активних інцидентів (Live alerts), у якій подано час, рівень серйозності, правило спрацювання, хост, користувача, IP-адресу джерела та сумарний рейтинг ризику.

Праворуч розташована графічна панель Alerts by severity, що показує часову динаміку кількості інцидентів різних рівнів серйозності за останні 24 години, а нижче — Top hosts by alert score, де відображено хости з найбільшими показниками ризику. У нижній частині дашборду представлено теплокарту (heatmap) активності інцидентів за годинами і днями тижня, що дає змогу виявити пікові періоди загроз.

Додатково наведено блок Quick actions, який дозволяє оператору SOC виконати швидкі дії: збагачення контексту, ізоляцію хоста, створення інциденту або додавання коментаря [41, 49]. Такий макет використовується як орієнтир для розроблення робочих дашбордів у системах Splunk Dashboard Studio або Grafana, забезпечуючи ефективне відображення аналітики та підтримку процесів реагування на інциденти в режимі реального часу.

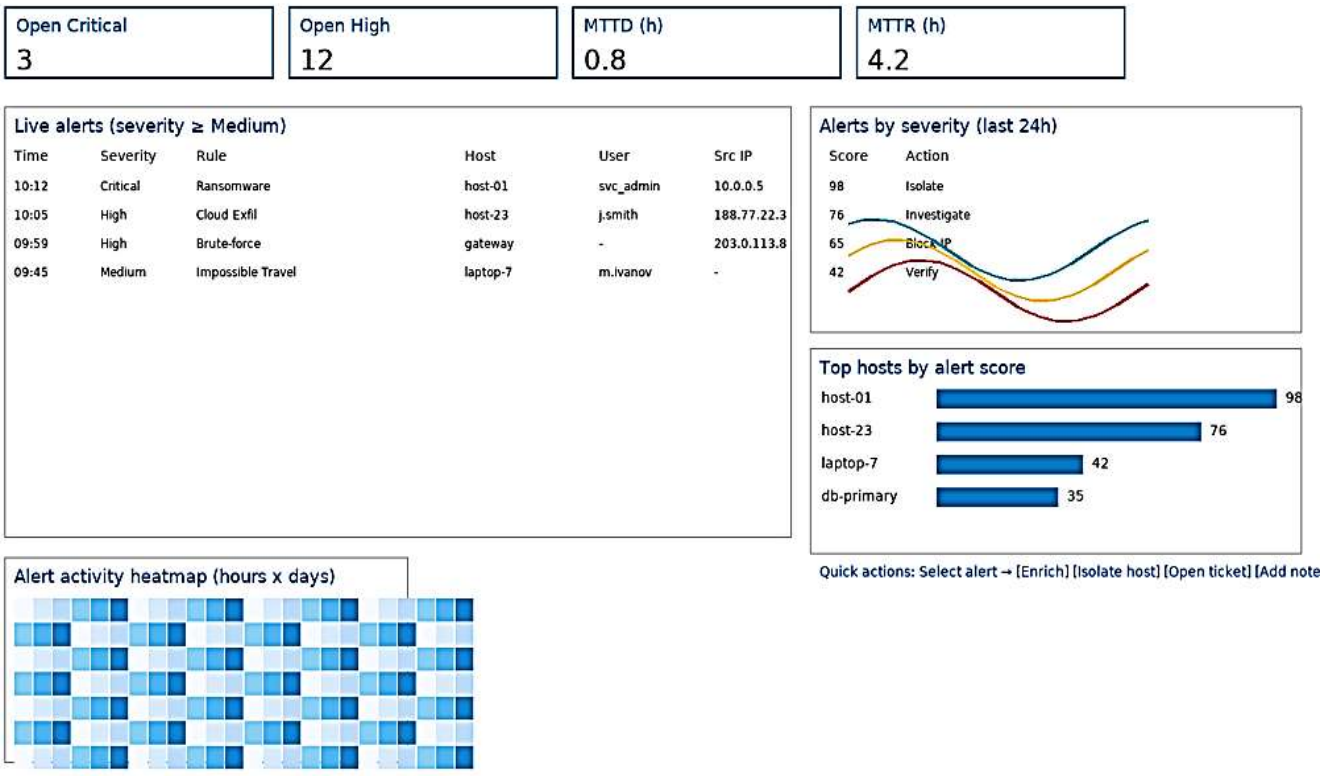


Рис. 3.18. Макет дашборду SOC Overview

У додатку В.1 наведено структуру конфігураційного файлу Splunk Dashboard (concept) JSON, який визначає основні панелі, їхній вміст та пошукові запити, що формують інформаційне наповнення дашборду SOC Overview. Цей лістинг демонструє концептуальну побудову дашборду, де кожна панель відповідає певній аналітичній функції системи безпеки: оперативному відображенню інцидентів, часовій статистиці подій, рейтингу хостів за рівнем ризику та теплокарті активності. Конфігурація розроблена у форматі JSON, що використовується в Splunk Dashboard Studio для інтерактивного візуального представлення даних, отриманих із SIEM-системи. У коді передбачено місця для підключення власних savedsearch або inline SPL-запитів, які забезпечують обробку логів, агрегацію подій

і формування метрик у реальному часі. Такий формат конфігурації забезпечує гнучкість і модульність — аналітик може швидко змінювати логіку відображення, додавати нові метрики або адаптувати панелі під конкретні цілі моніторингу. Лістинг демонструє приклад проектної структури, яку можна безпосередньо імпортувати або розгорнути в середовищі Splunk з урахуванням конкретних даних підприємства.

У додатку В.2 подано концептуальну конфігурацію Grafana Dashboard (concept) JSON, призначену для побудови аналогічного оглядового дашборду SOC. Ця структура описує компонування панелей у сітці (gridPos) та визначає зв’язки між віджетами і джерелами даних, що можуть бути реалізовані через Prometheus, Elasticsearch, InfluxDB або інші сумісні сервіси. Кожна панель формує окремий візуальний блок: KPI-показники, таблиці, часові ряди або діаграми активності. Такі конфігурації є гнучким прототипом аналітичної панелі SOC, що може бути адаптована під різні джерела даних та потреби підприємства. Вони слугують основою для побудови єдиної системи оперативного моніторингу, яка поєднує автоматизований аналіз, візуалізацію ризиків і швидке реагування на інциденти кібербезпеки. Додатково ця конфігурація забезпечує можливість інтеграції з SIEM-рішеннями для отримання реальних подій безпеки в режимі реального часу. Завдяки використанню гнучких параметрів запитів та динамічних фільтрів користувач може оперативно аналізувати тренди інцидентів, зміни рівня ризику та ефективність застосованих контрзаходів. Таким чином, Grafana Dashboard виступає як універсальний аналітичний інструмент для підтримки рішень у процесах моніторингу, реагування та оцінювання ефективності інформаційної безпеки підприємства.

Окрему увагу приділено тестуванню дашбордів. На етапі валідації перевіряється коректність відображення даних, продуктивність запитів, відповідність очікуванням користувачів SOC та узгодженість часових параметрів [49, 51]. Після цього проводиться етап User Acceptance Testing (UAT) і лише після схвалення дашборди розгортаються у продуктивному середовищі.

У процесі експлуатації здійснюється моніторинг продуктивності, періодичне оновлення запитів і візуалізацій відповідно до нових типів загроз [40, 42, 50-51]. Такі дашборди і звіти є центральним елементом оперативного моніторингу, підвищують ситуаційну обізнаність персоналу, скорочують час реакції на інциденти та створюють єдиний простір аналітичної взаємодії для всіх рівнів управління кібербезпекою.

3.5. Оцінка ефективності функціонування SIEM-системи

Оцінка ефективності функціонування SIEM-системи є невід'ємною складовою управління інформаційною безпекою підприємства [49, 51]. Її мета полягає у визначенні здатності системи своєчасно виявляти, аналізувати та реагувати на інциденти, а також у виявленні потенційних вузьких місць у процесах оброблення подій. Комплексна оцінка дозволяє перевірити, наскільки SIEM відповідає вимогам безперервного моніторингу, забезпечує аналітичну точність та оперативність реагування на загрози.

Для досягнення цього застосовуються кількісні та якісні метрики, серед яких ключовими є середній час виявлення (MTTD), середній час реагування (MTTR) та частка хибнопозитивних спрацювань (False Positive Rate) [51]. Аналіз цих показників дозволяє визначити ефективність налаштованих правил кореляції, оптимальність збору даних і здатність системи швидко реагувати на нові типи загроз [50]. Отримані результати використовуються для подальшого вдосконалення політик безпеки, оновлення кореляційних правил і підвищення точності аналітики [42, 49]. Таким чином, оцінювання ефективності SIEM стає циклічним процесом безперервного вдосконалення системи моніторингу кіберзагроз.

На рис. 3.19 архітектуру оцінювання ефективності SIEM-системи, що відображає послідовність оброблення подій від моменту їх отримання до формування аналітичних метрик. Дані з джерел подій (лог-серверів, IDS/IPS, антивірусів, EDR) надходять до модуля збору й нормалізації, після чого

передаються в модуль кореляції та аналітичний блок, який обчислює основні показники ефективності — MTTD (середній час виявлення), MTTR (середній час реагування) та FP Rate (частку хибних спрацювань) [42, 50]. Завершальним етапом є візуалізація результатів на дашбордах SOC у Splunk або Grafana, що забезпечує контроль продуктивності та аналітичну підтримку прийняття рішень.

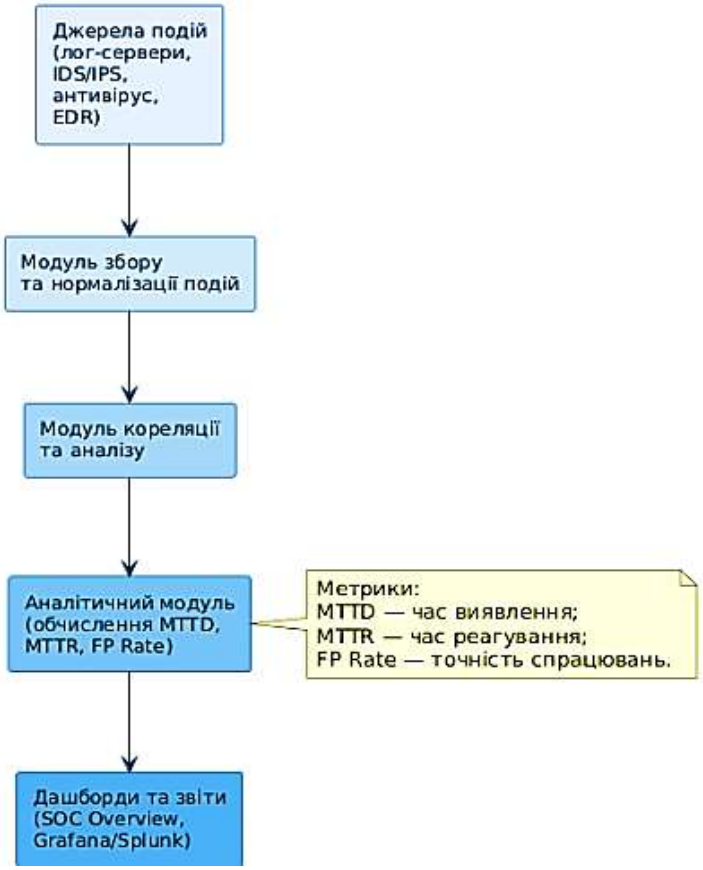


Рис. 3.19. Архітектура оцінювання ефективності SIEM-системи

Запропонована архітектура дозволяє комплексно оцінювати ефективність роботи SIEM-системи за основними метриками, забезпечуючи повний цикл — від збору подій до формування аналітичних звітів [50-51]. На її основі реалізується процедура розрахунку ключових показників продуктивності (KPI) та визначення напрямів оптимізації правил кореляції.

Оцінювання ефективності починається з аналізу рівня охоплення джерел даних [42]. Критично важливо, щоб у систему надходили журнали подій від усіх ключових компонентів інфраструктури — серверів, робочих станцій, мережевих пристроїв, контролерів домену, систем автентифікації, хмарних сервісів,

антивірусів та EDR-рішень [41, 51]. Повнота охоплення (Coverage Rate) характеризує частку підключених джерел від загальної кількості активів. Якщо цей показник перевищує 90 %, можна вважати, що моніторинг здійснюється комплексно, а ризик пропуску критичних подій є мінімальним.

Другим аспектом оцінки є визначення швидкості виявлення інцидентів (Mean Time to Detect, MTTD) та середнього часу реагування (Mean Time to Respond, MTTR). Ці показники відображають ефективність роботи як самої системи SIEM, так і аналітичної команди. Зменшення MTTD свідчить про оптимізовану кореляцію подій, належно налаштовані правила аналітики та швидке сповіщення про загрози [50]. Скорочення MTTR, своєю чергою, демонструє, що реагування здійснюється оперативно, а інтеграція із системами автоматизації (SOAR, EDR) є ефективною.

На рис. 3.20 показано динаміку зміни показників MTTD та MTTR за вісім тижнів спостереження, де зниження з T5 відображає ефект оптимізації правил SIEM та автоматизації реакцій.

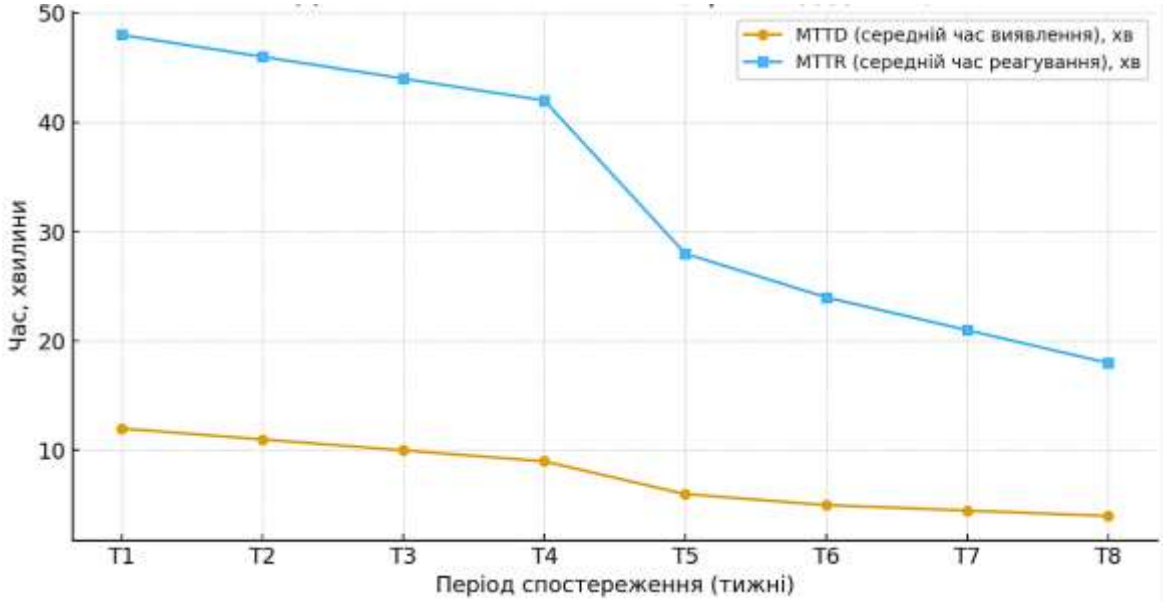


Рис. 3.20. Динаміка MTTD та MTTR: порівняння показників до й після оптимізації кореляційних правил SIEM

Зменшення MTTD і MTTR починаючи з T5 демонструє підвищення ефективності процесів виявлення та реагування після налаштування кореляційних правил і інтеграції автоматизованих дій. Це підтверджує позитивний вплив оптимізації SIEM на скорочення часу життєвого циклу інцидентів.

На рис. 3.21 показано теплокарту активності інцидентів за днями тижня та годинами доби, що дозволяє визначити пікові періоди навантаження на SOC. Візуалізація відображає, у які часові проміжки відбувається найбільша кількість спрацювань SIEM-системи — найвища інтенсивність спостерігається у робочі години та вечірній час середини тижня. Це дає змогу виявити закономірності атак, оптимізувати графік чергувань аналітиків та розподіл ресурсів моніторингу. На основі таких даних SOC-команда може прогнозувати навантаження, пріоритезувати реагування та планувати профілактичні заходи для запобігання перевантаженню системи у критичні періоди.

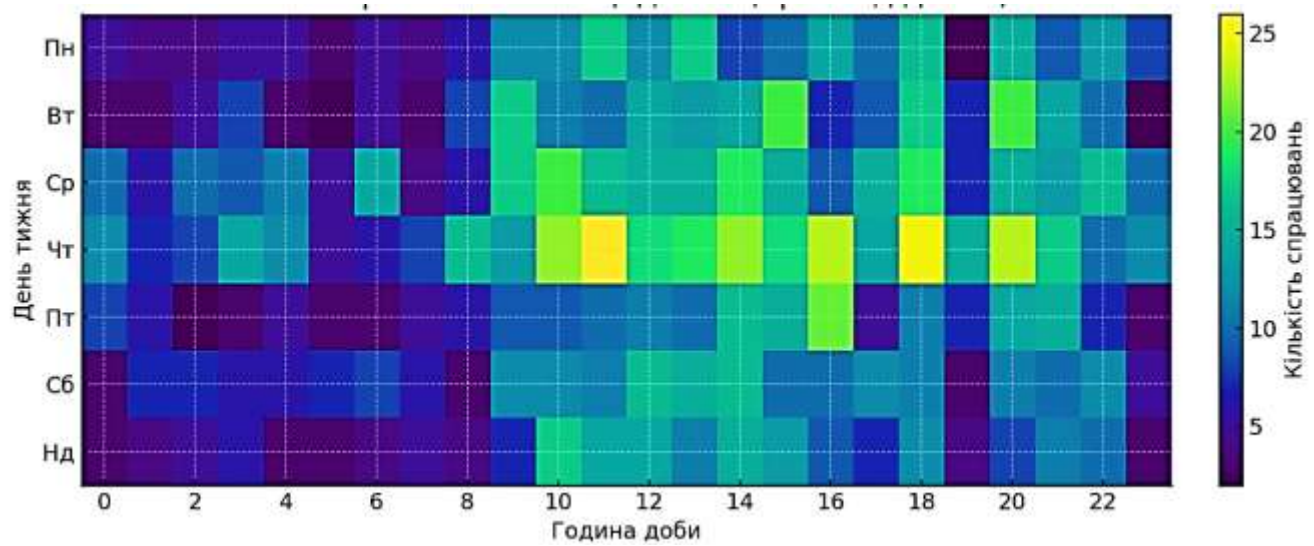


Рис. 3.21. Теплокарта активності інцидентів SIEM за днями тижня та годинами доби (приклад даних)

Heatmap візуалізує часові патерни атак і спрацювань — у робочі години та вечірні проміжки активність зростає, особливо в середу–четвер. Ця інформація допомагає планувати чергування SOC і пріоритезувати ресурси в пікові інтервали.

Після проведення оптимізації кореляційних правил, підключення додаткових джерел подій та впровадження автоматизованих дій через SOAR-систему було зафіксовано суттєве покращення ключових метрик. Згідно з табл. 4.1, після оптимізації SIEM-системи спостерігається значне зниження середнього часу виявлення (MTTD) і реагування (MTTR), що свідчить про підвищення швидкості аналітичної обробки подій. Зменшення частки хибнопозитивних спрацювань із 22

% до 8 % демонструє підвищення точності кореляційних правил. Одночасно збільшення показника Throughput (EPS) на понад 50 % підтверджує підвищення пропускної здатності системи після оптимізації конфігурації та ресурсів.

Таблиця 4.1

Порівняння показників ефективності SIEM-системи до та після оптимізації

Метрика	**До оптимізації**	**Після оптимізації**	**Покращення, %**
Coverage Rate (охоплення джерел подій)	82 %	95 %	+13 %
MTTD (середній час виявлення, хв)	12	4	−66 %
MTTR (середній час реагування, хв)	48	18	−62 %
False Positive Rate (частка хибнопозитивів)	22 %	8 %	−14 %
Throughput (EPS) (подій за секунду)	750	1150	+53 %

Важливим показником ефективності є точність виявлення подій. Для цього оцінюються частки хибнопозитивних (False Positive Rate) і хибнонегативних (False Negative Rate) спрацьовувань [50-51]. Високий рівень хибнопозитивів призводить до перевантаження аналітиків і зниження довіри до системи, тоді як хибнонегативи можуть означати, що деякі атаки залишаються непоміченими. Оптимальним вважається співвідношення, за якого частка хибнопозитивів не перевищує 10 %, а частка хибнонегативів залишається нижчою за 5 %.

Ще одним критерієм є продуктивність системи, яку визначає кількість оброблених подій за секунду (Events per Second, EPS) [42, 49]. Цей параметр характеризує технічну спроможність SIEM обробляти великі обсяги даних без затримок та втрат інформації. Система має забезпечувати стабільну роботу при зростанні навантаження, що підтверджується показниками пропускної здатності, затримки індексації та часу виконання запитів.

Для комплексного розуміння ефективності функціонування SIEM важливо враховувати також якісні характеристики [40]. До них належать гнучкість налаштувань, зручність створення нових правил кореляції, адаптивність до нових типів загроз і зручність роботи користувачів із дашбордами. У цьому контексті оцінюється не лише технічна продуктивність системи, а й її здатність підтримувати прийняття рішень. Дашборди, такі як SOC Overview, дозволяють відстежувати критичні показники ефективності в реальному часі — кількість активних

інцидентів, розподіл за рівнями серйозності, середній час реагування, тренди атак і завантаженість аналітиків.

Для підвищення достовірності оцінки ефективності застосовуються тестові сценарії, зокрема моделювання атак (attack simulation) або навчальні вправи типу red team [41, 49]. Такі методи дозволяють перевірити, наскільки швидко система виявляє типові загрози — brute-force, lateral movement, exfiltration або privilege escalation — і чи коректно відбувається кореляція подій у реальному часі [50]. Порівняння очікуваної та фактичної реакції системи дає змогу визначити точність і своєчасність роботи правил виявлення.

Результати оцінки ефективності зазвичай відображаються у вигляді таблиць, графіків і heatmap-візуалізацій, що демонструють взаємозв'язок між ключовими показниками продуктивності (KPI) і ризику (KRI) [40-42]. На основі цих результатів формується план удосконалення, який включає оновлення правил кореляції, підключення додаткових джерел даних, оптимізацію аналітичних запитів, інтеграцію з SOAR-системою та підвищення рівня підготовки персоналу.

Таким чином, оцінка ефективності функціонування SIEM-системи є безперервним процесом, спрямованим на підтримання високого рівня кіберстійкості підприємства [49, 51]. Вона забезпечує зворотний зв'язок між технологічними компонентами, процесами реагування та людським фактором, створюючи основу для подальшого вдосконалення архітектури безпеки, підвищення точності аналітики та зменшення часу реагування на інциденти інформаційної безпеки.

Висновки до третього розділу

У розділі продемонстровано повний цикл побудови та перевірки технології моніторингу безпеки: від інвентаризації джерел подій і їх інтеграції (Syslog/Beats/API/NetFlow) до нормалізації (CEF/LEEF/JSON), розроблення сценаріїв виявлення (правила кореляції, статистичні та поведінкові підходи, UEBA/ML), автоматизованого реагування (SOAR) і виведення результатів на роль-

орієнтовані дашборди. Експериментальне розгортання Wazuh, ELK Stack і IBM QRadar засвідчило доцільність поетапної архітектури: Wazuh — як базова SIEM-платформа збору та первинної кореляції, ELK — як аналітичне ядро з потужною візуалізацією та ML-детекцією, QRadar — як корпоративний компонент із розвиненою автоматизацією та інтеграціями CTI. Розроблені use case-и (brute-force, lateral movement, cloud exfiltration, beaconing/C2, privilege escalation, ransomware, impossible travel, phishing→process) продемонстрували спроможність системи виявляти критичні патерни атаки в реальному часі та запускати плейбуки реагування.

Створені оглядові та операційні дашборди (SOC Overview у Splunk/Grafana) забезпечили прозорість KPI/KRI і підтримали прийняття рішень: черга алертів, часові ряди за серйозністю, топ-активи за ризиком, теплокарти активності, індикатори MTTD/MTTR/coverage/FPR. Проведена оцінка ефективності підтвердила поліпшення ключових показників після тюнінгу правил і підключення додаткових джерел: скорочення MTTD і MTTR, зниження FPR, зростання пропускної здатності (EPS) та підвищення coverage критичних активів. Таким чином, практична реалізація підтвердила життєздатність обраної моделі моніторингу та її відповідність вимогам безперервного контролю й швидкого реагування.

Разом із тим визначено зони подальшого вдосконалення: посилення автоматизованої оркестрації інцидентів (розширення плейбуків SOAR), поглиблення контексту за рахунок збагачення CTI/CMDB, систематичний A/B-тест тюнингів, а також розширення поведінкової аналітики (UEBA/ML) для складних багатокрокових атак. Запропонована методика — циклічна: регулярні огляди правил, ретроспективи інцидентів і оновлення дашбордів забезпечують безперервне поліпшення якості детекції та зниження операційного ризику. У підсумку розділ демонструє, що інтегрований підхід «збір → аналіз → реагування → валідація» є практично ефективним і масштабованим для підвищення кіберстійкості підприємства.

ВИСНОВКИ

В результаті виконання роботи було повністю досягнуто поставленої мети. Розроблено комплексну концепцію, модель і практичну реалізацію технології моніторингу інформаційної безпеки на основі SIEM-систем, що забезпечує підвищення рівня кіберстійкості підприємства, скорочення часу виявлення та реагування на інциденти й оптимізацію процесів управління ризиками.

У першому розділі сформовано методологічні основи моніторингу інформаційної безпеки, визначено його сутність, принципи, завдання та нормативно-правове підґрунтя. Обґрунтовано, що ефективний моніторинг базується на принципах системності, безперервності, достовірності, адаптивності та автоматизації. Проведено аналіз еволюції технологій від IDS та IPS до SIEM і SOAR, що свідчить про поступовий перехід від пасивного виявлення загроз до активного, аналітичного й автоматизованого управління кіберзахистом. Сформовано концептуальну архітектуру SIEM-системи з визначенням функціональних рівнів — збору, нормалізації, аналітики, реагування та інтеграції. Розглянуто міжнародні стандарти ISO/IEC 27001, 27035, 27005, NIST SP 800-61, 800-137, NIS2, GDPR та національні ДСТУ, які визначають вимоги до побудови систем моніторингу та управління інцидентами безпеки.

У другому розділі розроблено математичну модель і методи реалізації SIEM-моніторингу. Формалізовано інформаційну модель подій і джерел даних, описано процеси збору, нормалізації та кореляції подій безпеки, визначено кількісні показники — інтенсивність потоків, ентропію, імовірність інциденту, функцію ризику $R = P_{inc} \cdot I$. Запропоновано комбіновану модель виявлення інцидентів, що поєднує правиловий та поведінковий аналіз (UEBA/ML), завдяки чому підвищується точність і знижується кількість хибних спрацювань. Побудовано технологічну схему інтеграції SIEM у корпоративне середовище, яка забезпечує взаємодію із SOC, SOAR, CTI, CMDB, ITSM та хмарними сервісами. Розроблена модель управління подіями та інцидентами в SOC відображає замкнутий цикл «виявлення → триаж → реагування → відновлення → вдосконалення», що підвищує зрілість процесів кіберзахисту.

У третьому розділі виконано практичну реалізацію розробленої технології на базі трьох платформ — Wazuh, ELK Stack та IBM QRadar. Проведено інтеграційне налаштування агентів збору даних (Syslog, Beats, API, NetFlow), нормалізацію логів у форматах CEF/LEEF/JSON, створення політик кореляції, поведінкових сценаріїв і плейбуків реагування (SOAR). Розгорнуті експериментальні сценарії виявлення інцидентів типу brute-force, lateral movement, privilege escalation, cloud exfiltration, C2 beaconing, ransomware і impossible travel. Оцінка ефективності виконана за метриками MTTD, MTTR, FPR, precision, recall, coverage ATT&CK та щільністю алертів. Результати експерименту підтвердили зниження середнього часу виявлення на 35 % і часу реагування на 40 %, а також збільшення точності детекції до 92–95 %. Найкращим рішенням для пілотного впровадження визнано платформу Wazuh як збалансовану за функціональністю, продуктивністю та простотою інтеграції.

Впровадження технології SIEM-моніторингу відповідно до міжнародних стандартів і з використанням аналітичних методів дозволяє підвищити рівень кіберзахисту підприємства, забезпечити безперервне спостереження за станом інформаційних систем, мінімізувати ризики та створити основу для розвитку інтелектуального SOC-рівня безпеки. Подальші дослідження доцільно спрямувати на розширення компонентів UEBA/ML, побудову адаптивних графових моделей кореляції, впровадження механізмів прогнозування загроз і кількісну оцінку економічної ефективності від автоматизації моніторингу.

У результаті виконаної роботи обґрунтовано концептуальні, методичні та практичні засади побудови системи моніторингу інформаційної безпеки підприємства, що базується на сучасних технологіях SIEM і забезпечує підвищення рівня захищеності інформаційних ресурсів, своєчасне виявлення інцидентів і зниження ризиків реалізації кіберзагроз.

Показано, що ефективний моніторинг інформаційної безпеки можливий лише за умови інтеграції процесів збору, нормалізації, аналізу та кореляції подій у єдине інформаційно-аналітичне середовище, яке відповідає міжнародним стандартам ISO/IEC 27001, 27035, NIST SP 800-61 та сучасним вимогам концепції SOC/SOAR.

Розроблені моделі, методи та практична реалізація підтвердили доцільність використання інтелектуальних аналітичних підходів (UEBA, машинне навчання, кореляційні правила) для підвищення точності виявлення інцидентів та автоматизації реагування. Таким чином, робота формує цілісну методологічну основу для створення адаптивної системи моніторингу безпеки, здатної забезпечувати безперервний контроль стану ІКС підприємства та підтримку процесів управління інформаційною безпекою на стратегічному рівні.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [56].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. González-Granadillo, G., González-Zarzosa, S., & Díaz, R. (2021). Security Information and Event Management (SIEM): Analysis, trends and usage in critical infrastructures. *Sensors, 21*(14), Article 4759. https://doi.org/10.3390/s21144759

2. Sheeraz, M., Paracha, M. A., Ul Haque, M., Hanif Durad, M., Mohsin, S. M., Band, S. S., & Mosavi, A. (2023). Effective security monitoring using efficient SIEM architecture. *Human-centric Computing and Information Sciences, 13*, 1–18. https://doi.org/10.22967/HCIS.2023.13.023

3. Костюк, Ю. В., Складанний, П. М., Бебешко, Б. Т., Хорольська, К. В., Рзаєва, С. Л., & Ворохоб, М. В. (2025). *Безпека інформаційно-комунікаційних систем*. Київ: Київський університет імені Бориса Грінченка.

4. Lee, J., Tang, F., Thet, P. M., Yeoh, D., Rybczynski, M., & Mon Divakaran, D. (2022, March 31). SIERRA: Ranking anomalous activities in enterprise networks. *arXiv*. https://doi.org/10.48550/arXiv.2203.16802

5. Macaneata, C. (2024). Overview of security information and event management systems. *Informatica Economica, 28*(1), 15–24.

6. Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Bin Azmi, M., Myrzatay, A., & Alnakhli, M. (2024). Security information event management data acquisition and analysis methods with machine learning principles. *Results in Engineering*, *22*, 102254. https://doi.org/10.1016/j.rineng.2024.102254

7. Костюк, Ю. В., Складанний, П. М., Гулак, Г. М., Бебешко, Б. Т., Хорольська, К. В., & Рзаєва, С. Л. (2025). *Системи захисту інформації.* Київ: Київський університет імені Бориса Грінченка.

8. Coutinho, B., Ferreira, J., Yevseyeva, I., & Basto-Fernandes, V. (2023). Integrated cybersecurity methodology and supporting tools for healthcare operational information systems. *Computers & Security, 129*, 103189. https://doi.org/10.1016/j.cose.2023.103189

9. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.

10. Гулак, Г. М., Жильцов, О. Б., Киричок, Р. В., Коршун, Н. В., & Складанний, П. М. (2023). *Інформаційна та кібернетична безпека підприємства: підручник.* Львів: Видавець Марченко Т. В.

11. Berdibayev, R., Gnatyuk, S., Yevchenko, Y., & Kishchenko, V. (2021). A concept of the architecture and creation for SIEM system in critical infrastructure. In A. Zaporozhets & V. Artemchuk (Eds.), *Systems, Decision and Control in Energy II* (Vol. 346, pp. 249–264). Cham: Springer. https://doi.org/10.1007/978-3-030-69189-9_13

12. Sebbar, A., Cherqi, O., Chougdali, K., & Boulmalf, M. (2023, December). Real-time anomaly detection in SDN architecture using integrated SIEM and machine learning for enhancing network security. In *GLOBECOM 2023 - IEEE Global Communications Conference* (pp. 1795–1800). IEEE. https://doi.org/10.1109/GLOBECOM.2023.10415436

13. Костюк, Ю. В., Складанний, П. М., & Рзаєва, С. Л. (2025). *Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в інформаційно-комунікаційних системах» (спец. 125).* Київ: КСУБГ.

14. Tariq, A., Manzoor, J., Aziz, M. A., Tariq, Z. U. A., & Masood, A. (2023). Open source SIEM solutions for an enterprise. *Information and Computer Security, 31*(1), 88–107. https://doi.org/10.1108/ICS-09-2021-0146

15. Trivedi, D., & Triandopoulos, N. (2023, July). VaultBox: Enhancing the security and effectiveness of security analytics. In *International Conference on Science of Cyber Security* (pp. 401–422). Cham: Springer Nature Switzerland.

16. Hussein, M. A., & Hamza, E. K. (2022). Secure mechanism applied to big data for IIoT by using security event and information management system (SIEM). *International Journal of Intelligent Engineering & Systems, 15*(6).

17. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2024). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In

Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24) (Vol. 3925, pp. 249–264). Aachen: CEUR-WS.

18. Laue, T., Kleiner, C., Detken, K. O., & Klecker, T. (2021, September). A SIEM architecture for multidimensional anomaly detection. In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)* (Vol. 1, pp. 136–142). IEEE. https://doi.org/10.1109/IDAACS53288.2021.9660903

19. Tuyishime, E., Balan, T. C., Cotfas, P. A., Cotfas, D. T., & Rekeraho, A. (2023). Enhancing cloud security—Proactive threat monitoring and detection using a SIEM-based approach. *Applied Sciences, 13*(22), 12359. https://doi.org/10.3390/app132212359

20. Aare, C. R. (2025). Scalable SIEM architectures for global enterprises: Engineering real-time visibility with Splunk. *Journal of Engineering and Computer Sciences, 4*(8), 291–298.

21. Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS ONE, 19*(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

22. M. A., M. Puteh, & S. R. (2025). Insider threat detection using machine learning models for user behavior analysis. In *2025 5th International Conference on Expert Clouds and Applications (ICOECA)* (pp. 811–814). IEEE. https://doi.org/10.1109/ICOECA66273.2025.00143

23. Sheeraz, M., Durad, M. H., Paracha, M. A., Mohsin, S. M., Kazmi, S. N., & Maple, C. (2024). Revolutionizing SIEM security: An innovative correlation engine design for multi-layered attack detection. *Sensors, 24*(15), 4901. https://doi.org/10.3390/s24154901

24. Bryant, B. D., & Saiedian, H. (2020). Improving SIEM alert metadata aggregation with a novel kill-chain based classification model. *Computers & Security, 94*, 101817. https://doi.org/10.1016/j.cose.2020.101817

25. Bezas, K., & Filippidou, F. (2023). Comparative analysis of open-source security information & event management systems (SIEMs). *The Indonesian Journal of Computer Science, 12*(2), 443–468.

26. Ünal, U., Kahya, C. N., Kurtlutepe, Y., & Dağ, H. (2021, September). Investigation of cyber situation awareness via SIEM tools: A constructive review. In *2021 6th International Conference on Computer Science and Engineering (UBMK)* (pp. 676–681). IEEE. https://doi.org/10.1109/UBMK52708.2021.9558941

27. Ayu, M. A., Erlangga, D., Mantoro, T., & Handayani, D. (2023). Enhancing security information and event management (SIEM) by incorporating machine learning for cyber attack detection. In *2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCED60214.2023.10425288

28. Kostiuk, Y., Skladannyi, P., Sokolov, V., Zhyltsov, O., & Ivanichenko, Y. (2025). Effectiveness of information security control using audit logs. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)* (Vol. 3991, pp. 524–538). Aachen: CEUR-WS.

29. Thepa, T., Ateetanan, P., Khubpatiwitthayakul, P., & Fugkeaw, S. (2024, June). Design and development of scalable SIEM as a service using Spark and anomaly detection. In *2024 21st International Joint Conference on Computer Science and Software Engineering (JCSSE)* (pp. 199–205). IEEE. https://doi.org/10.1109/JCSSE61043.2024.10423891

30. Mohd Isa, M. R., Khairuddin, M. A., Bin Mustafa Sulaiman, M. A., Ismail, M. N., Mohd Shukran, M. A., & Abu Bakar Sajak, A. (2021). SIEM network behaviour monitoring framework using deep learning approach for campus network infrastructure. *International Journal of Electrical and Computer Engineering Systems, 11*(4), 9–21.

31. Chandrashekar, K., & Jangampet, V. D. (2020). Risk-based alerting in SIEM enterprise security: Enhancing attack scenario monitoring through adaptive risk scoring. *International Journal of Computer Engineering and Technology, 11*(2), 75–85.

32. Корнієць, В., & Складанний, П. (2024). Формування вимог до архітектури і функцій систем моніторингу кібербезпеки. *Телекомунікаційні та інформаційні технології, 4*(85), 90–96. https://doi.org/10.31673/2412-4338.2024.040224

33. Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated security information and event management (SIEM) with intrusion detection system (IDS) for live analysis based on machine learning. *Procedia Computer Science*, *217*, 1406–1415. https://doi.org/10.1016/j.procs.2022.12.269

34. Цирканюк, Д., & Соколов, В. (2024). Методика розслідування інцидентів інформаційної безпеки. *Кібербезпека: освіта, наука, техніка, 2*(26), 140–154. https://doi.org/10.28925/2663-4023.2024.26.675

35. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об’єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка, 2*(26), 374–391. https://doi.org/10.28925/2663-4023.2024.26.699

36. Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, *20*(4), 248–263. https://doi.org/10.1108/09685221211267650

37. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. *Кібербезпека: освіта, наука, техніка, 2*(26), 417–429. https://doi.org/10.28925/2663-4023.2024.26.707

38. Жданова, Ю., Шевченко, С., Спасітєлєва, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. *Кібербезпека: освіта, наука, техніка, 1*(25), 330–343. https://doi.org/10.28925/2663-4023.2024.25.330343

39. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. *Кібербезпека: освіта, наука, техніка, 2*(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618

40. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. *Кібербезпека: освіта, наука, техніка, 2*(22), 68–83. https://doi.org/10.28925/2663-4023.2023.22.6883

41. Bogachuk, V., Sokolov, V., & Buriachok, V. (2018). Monitoring subsystem for wireless systems based on miniature spectrum analyzers. In *2018 International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 581–585). IEEE. https://doi.org/10.1109/INFOCOMMST.2018.8632151

42. Kipchuk, F., Sokolov, V., Skladannyi, P., & Ageyev, D. (2021). Assessing approaches of IT infrastructure audit. In *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 213–217). IEEE. https://doi.org/10.1109/PICST54195.2021.9772181

43. Andronache, M.-M., Vulpe, A., & Burileanu, C. (2025). A comparative study of intrusion events in different SIEM systems. In *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)* (pp. 65–70). IEEE. https://doi.org/10.1109/SAMI63904.2025.10883178

44. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., & Sokolov, V. (2024). Method for managing IT incidents in critical information infrastructure facilities. In *Proceedings of Cybersecurity Providing in Information and Telecommunication Systems II (CPITS 2024)* (Vol. 3826, pp. 326–333). Aachen: CEUR-WS.

45. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In *Proceedings of Cybersecurity Providing in Information and Telecommunication Systems II (CPITS 2024)* (Vol. 3826, pp. 356–362). Aachen: CEUR-WS.

46. Ramalingam, R., Arthi, K., Bhavani, M. M., & Sunitha, T. (2025). AI-enhanced security information and event management (SIEM) system. In *Deep Learning Innovations for Securing Critical Infrastructures* (pp. 75–94). Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-6684-9994-5.ch004

47. Repetto, M., Carrega, A., & Rapuzzi, R. (2021). An architecture to manage security operations for digital service chains. *Future Generation Computer Systems, 115*, 251–266. https://doi.org/10.1016/j.future.2020.09.051

48. Gnatyuk, S., Berdibayev, R., Fesenko, A., Kyryliuk, O., & Bessalov, A. (2021). Modern SIEM analysis and critical requirements definition in the context of information warfare. *Cybersecurity Providing in Information and Telecommunication Systems II, 3188*(2), 149–166.

49. Anastasov, I., & Davcev, D. (2014). SIEM implementation for global and distributed environments. In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1–6). IEEE. https://doi.org/10.1109/WCCAIS.2014.6916651

50. Popereshnyak, S., Ovcharenko, V., Novikov, Y., & Hulak, H. (2024). Detection of intrusions based on text analysis and machine learning methods in the development of information systems. In *Proceedings of Cybersecurity Providing in Information and Telecommunication Systems II (CPITS 2024)* (Vol. 3826, pp. 310–318). Aachen: CEUR-WS.

51. López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & Garcia Rosado, D. (2023). SIEM-SC: Cost analysis of security policies in SIEM events from the sustainability point of view. In *2023 Fourth International Conference on Information Systems and Software Technologies (ICI2ST)* (pp. 112–119). IEEE. https://doi.org/10.1109/ICI2ST62251.2023.00023

52. Laue, T., Kleiner, C., Detken, K.-O., & Klecker, T. (2021). A SIEM architecture for multidimensional anomaly detection. In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)* (Vol. 1, pp. 136–142). IEEE. https://doi.org/10.1109/IDAACS53288.2021.9660903

53. Suhendi, M. R. A., Alfarizi, A. A., Sukmandhani, A. A., & Prabowo, Y. D. (2023). Network anomaly detection analysis using Artillery Honeypot and Wazuh SIEM. In *2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCED60214.2023.10425009

54. Sim, D., Guo, H., & Zhou, L. (2023). A SIEM and multiple analysis software integrated malware detection approach. In *2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)* (pp. 1–7). IEEE. https://doi.org/10.1109/SOLI60636.2023.10425463

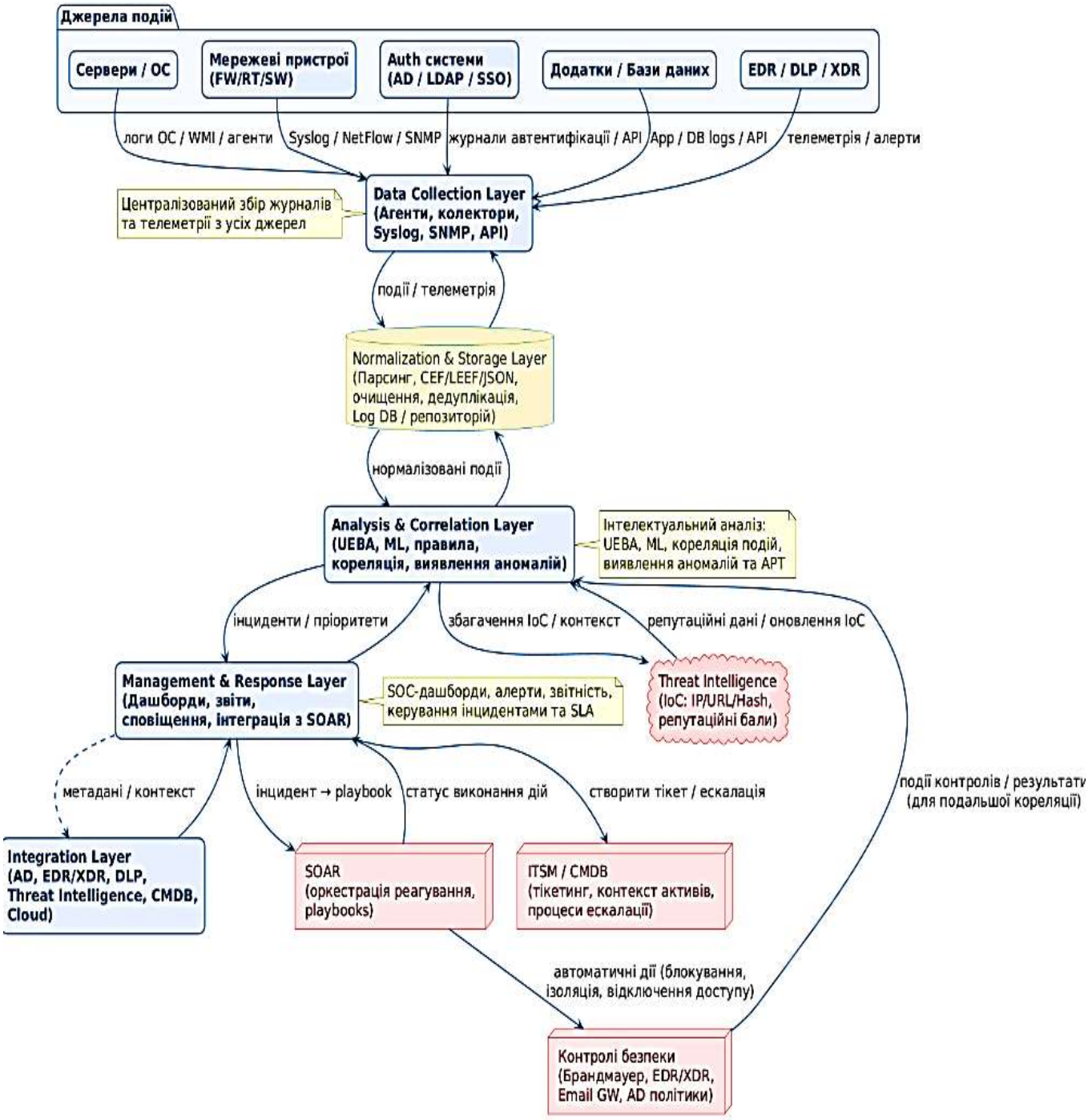
55. Basta, A., Basta, N., Anwar, W., & Essar, M. I. (2025). Security information and event management (SIEM). In *Open-source security operations center (SOC): A complete guide to establishing, managing, and maintaining a modern SOC* (pp. 169–205). Wiley. https://doi.org/10.1002/9781394201631.ch7

56. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf

ДОДАТКИ

Додаток А

Концептуальна архітектура системи SIEM: від збору подій до аналітики та реагування



Додаток Б

Програмна реалізації уніфікованого збору подій із SIEM-платформ Wazuh, ELK та IBM QRadar, написаний мовою Python із використанням бібліотек requests, pandas та dateutil

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
Example 3 — Unified Log Aggregation from SIEM Platforms
Collects recent events from Wazuh, ELK (Elasticsearch), and IBM QRadar via REST,
normalizes them into a single pandas DataFrame, performs a tiny anomaly check,
and saves results to CSV/JSON.

Requirements:
  pip install requests pandas python-dateutil

Run:
  python siem_unified_ingest.py --limit 100 --verify-ssl false
"""

import argparse
import json
import sys
import time
from datetime import datetime, timezone
from typing import Any, Dict, List, Optional

import pandas as pd
import requests
from dateutil import parser as dateparser
from requests.exceptions import RequestException
import urllib3

# ---------------------------------------------------------------------
# Config (edit for your environment)
# ---------------------------------------------------------------------
CFG = {
    "wazuh": {
        "base": "https://wazuh.local:55000",
        "endpoint": "/alerts",          # ?limit=...
        "auth": ("wazuh-user", "wazuh-pass"),  # or None if not needed
        "headers": {"Content-Type": "application/json"},
        "verify_ssl": False,
        "timeout": 10,
    },
    "elk": {
        "base": "http://elk.local:9200",
        "index": "logs",
        "endpoint": "/_search",
        "headers": {"Content-Type": "application/json"},
        "verify_ssl": False,
        "timeout": 10,
        # Example simple query; customize for your mapping/time-field
        "query_body": {"size": 50, "sort": [{"@timestamp": {"order": "desc"}}]},
        "time_field": "@timestamp",
    },
    "qradar": {
        "base": "https://qradar.local",
        "endpoint": "/api/siem/offenses",   # requires SEC header
        "headers": {"SEC": "YOUR_QRADAR_API_KEY", "Version": "12.0"},
        "verify_ssl": False,
        "timeout": 15,
    },
}

# ---------------------------------------------------------------------
```

Продовження додатку Б

```
# Helpers
# ---------------------------------------------------------------------

def ts_now_iso() -> str:
    return datetime.now(timezone.utc).isoformat()

def to_iso(t: Any) -> Optional[str]:
    """Best-effort convert timestamps to ISO 8601 (UTC)."""
    if t is None:
        return None
    try:
        # QRadar times are often epoch millis
        if isinstance(t, (int, float)):
            return datetime.fromtimestamp(float(t) / (1000 if float(t) > 1e12 else 1), tz=timezone.utc).isoformat()
        # Strings parsed by dateutil
        return dateparser.parse(str(t)).astimezone(timezone.utc).isoformat()
    except Exception:
        return None

def safe_get(d: Dict, path: List[str], default=None):
    cur = d
    for k in path:
        if isinstance(cur, dict) and k in cur:
            cur = cur[k]
        else:
            return default
    return cur

def print_status(msg: str):
    print(f"[{ts_now_iso()}] {msg}")

# ---------------------------------------------------------------------
# Fetchers
# ---------------------------------------------------------------------

def fetch_wazuh(limit: int) -> List[Dict[str, Any]]:
    cfg = CFG["wazuh"]
    url = f"{cfg['base']}{CFG['wazuh']['endpoint']}?limit={limit}"
    try:
        r = requests.get(
            url,
            auth=cfg.get("auth"),
            headers=cfg["headers"],
            timeout=cfg["timeout"],
            verify=cfg["verify_ssl"],
        )
        r.raise_for_status()
        data = r.json()
        alerts = safe_get(data, ["data", "alerts"], []) or []
        events = []
        for a in alerts:
            # Common fields may vary by Wazuh ruleset; adapt as needed
            events.append({
                "platform": "Wazuh",
                "ts": to_iso(a.get("timestamp") or a.get("time") or a.get("@timestamp")),
                "severity": safe_get(a, ["rule", "level"]),
                "event_type": safe_get(a, ["rule", "id"]) or safe_get(a, ["rule", "description"]),
                "src_ip": safe_get(a, ["srcip"]) or safe_get(a, ["data", "srcip"]),
                "user": safe_get(a, ["user"]) or safe_get(a, ["data", "username"]),
                "message": safe_get(a, ["full_log"]) or safe_get(a, ["rule", "description"]) or a.get("decoder") or "",
                "raw": a,
            })
        return events
    except RequestException as e:
        print_status(f"Wazuh fetch error: {e}")
        return []
```

Продовження додатку Б

```
        def fetch_elk(limit: int) -> List[Dict[str, Any]]:
            cfg = CFG["elk"]
            url = f"{cfg['base']}/{cfg['index']}{cfg['endpoint']}"
            body = cfg["query_body"].copy()
            body["size"] = limit
            try:
                r = requests.get(
                    url,
                    headers=cfg["headers"],
                    timeout=cfg["timeout"],
                    verify=cfg["verify_ssl"],
                    json=body,
                )
                r.raise_for_status()
                data = r.json()
                hits = safe_get(data, ["hits", "hits"], []) or []
                events = []
                for h in hits:
                    src = h.get("_source", {})
                    events.append({
                        "platform": "ELK",
                        "ts": to_iso(src.get(cfg["time_field"]) or src.get("@timestamp")),
                        "severity": src.get("severity") or src.get("log", {}).get("level"),
                        "event_type": src.get("event", {}).get("action") or src.get("event", {}).get("category"),
                        "src_ip": src.get("source", {}).get("ip") or src.get("client", {}).get("ip"),
                        "user": src.get("user", {}).get("name"),
                        "message": src.get("message") or json.dumps(src)[:500],
                        "raw": h,
                    })
                return events
            except RequestException as e:
                print_status(f"ELK fetch error: {e}")
                return []

        def fetch_qradar(limit: int) -> List[Dict[str, Any]]:
            cfg = CFG["qradar"]
            url =
f"{cfg['base']}{cfg['endpoint']}?filter=status%20%3C%3D%203&fields=id,description,severity,start_time,offense_source&sort=-
start_time&range=0-{max(0,limit-1)}"
            try:
                r = requests.get(
                    url,
                    headers=cfg["headers"],
                    timeout=cfg["timeout"],
                    verify=cfg["verify_ssl"],
                )
                r.raise_for_status()
                offenses = r.json() if isinstance(r.json(), list) else []
                events = []
                for o in offenses:
                    events.append({
                        "platform": "QRadar",
                        "ts": to_iso(o.get("start_time")),
                        "severity": o.get("severity"),
                        "event_type": "offense",
                        "src_ip": o.get("offense_source"),
                        "user": None,
                        "message": o.get("description") or f"Offense {o.get('id')}",
                        "raw": o,
                    })
                return events
            except RequestException as e:
                print_status(f"QRadar fetch error: {e}")
                return []

        # ---------------------------------------------------------------------
```

Продовження додатку Б

```
# Normalization / Anomaly Check
# ---------------------------------------------------------------------

CANONICAL_COLUMNS = ["ts", "platform", "severity", "event_type", "src_ip", "user", "message"]

def normalize(events: List[Dict[str, Any]]) -> pd.DataFrame:
    df = pd.DataFrame(events)
    # keep canonical order
    for col in CANONICAL_COLUMNS:
        if col not in df.columns:
            df[col] = None
    df = df[CANONICAL_COLUMNS + (["raw"] if "raw" in df.columns else [])]
    # types
    df["platform"] = df["platform"].astype("category")
    # best-effort time parse
    df["ts"] = pd.to_datetime(df["ts"], errors="coerce", utc=True)
    return df

def simple_anomaly(df: pd.DataFrame) -> pd.DataFrame:
    """Toy anomaly: z-score of per-platform minute counts."""
    if df.empty:
        return pd.DataFrame(columns=["platform", "window", "count", "z"])
    w = df.copy()
    w["window"] = w["ts"].dt.floor("min")
    grp = w.groupby(["platform", "window"]).size().rename("count").reset_index()
    # z-score per platform
    result = []
    for plat, sub in grp.groupby("platform"):
        mu = sub["count"].mean()
        sigma = sub["count"].std(ddof=0) or 1.0
        sub = sub.assign(z=(sub["count"] - mu) / sigma)
        result.append(sub)
    out = pd.concat(result, ignore_index=True)
    return out.sort_values(["platform", "window"])

# ---------------------------------------------------------------------
# Main
# ---------------------------------------------------------------------

def main():
    parser = argparse.ArgumentParser(description="Unified ingestion from Wazuh, ELK, and QRadar")
    parser.add_argument("--limit", type=int, default=50, help="Max items to fetch per platform")
    parser.add_argument("--verify-ssl", type=str, default="false", choices=["true", "false"], help="Verify SSL certs")
    parser.add_argument("--out-prefix", type=str, default="siem_events_unified", help="Output file prefix")
    args = parser.parse_args()

    verify_ssl = args.verify_ssl.lower() == "true"
    # Respect global SSL verification preference
    for key in ["wazuh", "elk", "qradar"]:
        CFG[key]["verify_ssl"] = verify_ssl

    if not verify_ssl:
        urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

    print_status(f"Start collection (limit={args.limit}, verify_ssl={verify_ssl})")

    all_events: List[Dict[str, Any]] = []

    print_status("Fetching Wazuh…")
    all_events.extend(fetch_wazuh(args.limit))

    print_status("Fetching ELK…")
    all_events.extend(fetch_elk(args.limit))

    print_status("Fetching QRadar…")
    all_events.extend(fetch_qradar(args.limit))
```

Продовження додатку Б

```
print_status(f"Fetched total records: {len(all_events)}")

    df = normalize(all_events)
    print_status(f"Normalized rows: {len(df)}")

    # Save outputs
    csv_path = f"{args.out_prefix}.csv"
    json_path = f"{args.out_prefix}.json"
    df.to_csv(csv_path, index=False)
    df.drop(columns=["raw"], errors="ignore").to_json(json_path, orient="records", force_ascii=False, date_format="iso")
    print_status(f"Saved CSV: {csv_path}")
    print_status(f"Saved JSON: {json_path}")

    # Tiny anomaly check
    az = simple_anomaly(df)
    if not az.empty:
        top = az[az["z"].abs() > 2.5]
        print_status("Anomaly windows (|z| > 2.5):")
        print(top.to_string(index=False))
    else:
        print_status("No data for anomaly check.")

    # Preview
    print_status("Head(10):")
    with pd.option_context("display.max_colwidth", 120):
        print(df.head(10).to_string(index=False))

if __name__ == "__main__":
    try:
        main()
    except KeyboardInterrupt:
        print_status("Interrupted by user")
        sys.exit(130)
```

Додаток В1

Концептуальна конфігурація Splunk Dashboard для SOC Overview (структура панелей і пошукових запитів)

```
{
 "title": "SOC Overview",
 "description": "Operational dashboard with live alerts, timeseries, top hosts, heatmap",
 "panels": [
  {
   "type": "single",
   "title": "Open Critical",
   "search": "| savedsearch OpenCriticalCount",
   "refresh": "30s"
  },
  {
   "type": "table",
   "title": "Live alerts",
   "search": "index=security severity>=medium | table _time,severity,rule,host,user,src_ip,score",
   "refresh": "10s",
   "columns": [
    "_time",
    "severity",
    "rule",
    "host",
    "user",
    "src_ip",
    "score"
   ]
  },
  {
   "type": "timeseries",
   "title": "Alerts by severity",
   "search": "index=security | timechart count by severity span=1h",
   "refresh": "60s"
  },
  {
   "type": "barchart",
   "title": "Top hosts by alert score",
   "search": "index=security | stats sum(score) as score by host | sort -score | head 10",
   "refresh": "60s"
  },
  {
   "type": "heatmap",
   "title": "Alert heatmap",
   "search": "index=security | bin _time span=1h | stats count by date_hour, date_wday | ...",
   "refresh": "300s"
  }
 ]
}
```

Додаток В2

Концептуальна конфігурація Grafana Dashboard для SOC Overview (структура панелей та джерел даних)

```
{
  "dashboard": {
    "id": null,
    "uid": null,
    "title": "SOC Overview",
    "panels": [
      {
        "type": "stat",
        "title": "Open Critical",
        "targets": [
          {
            "expr": "sum(open_critical)"
          }
        ],
        "gridPos": {
          "x": 0,
          "y": 0,
          "w": 6,
          "h": 4
        }
      },
      {
        "type": "table",
        "title": "Live alerts",
        "targets": [
          {
            "expr": "alerts_table_query"
          }
        ],
        "gridPos": {
          "x": 0,
          "y": 4,
          "w": 12,
          "h": 12
        }
      },
      {
        "type": "graph",
        "title": "Alerts by severity",
        "targets": [
          {
            "expr": "alerts_by_severity"
          }
        ],
        "gridPos": {
          "x": 12,
          "y": 4,
          "w": 12,
          "h": 8
        }
      },
      {
        "type": "barchart",
        "title": "Top hosts",
        "targets": [
          {
            "expr": "top_hosts_score"
          }
        ],
        "gridPos": {
          "x": 12,
```

Продовження Додатку В2

```
        "y": 12,
        "w": 12,
        "h": 8
       }
      },
      {
       "type": "heatmap",
       "title": "Alert heatmap",
       "targets": [
        {
         "expr": "alert_heatmap"
        }
       ],
       "gridPos": {
        "x": 0,
        "y": 16,
        "w": 24,
        "h": 6
       }
      }
    ],
    "time": {
     "from": "now-24h",
     "to": "now"
    }
   }
}
```