НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОДИКА ЗАСТОСУВАННЯ SIEM-СИСТЕМИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Старіченко Денис Павлович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.т.н., доцент
Бойко Віктор Дмитрович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Старіченку Денису Павловичу

1. Тема роботи: «Методика застосування SIEM-системи вінформаційній системі організації»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «16» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Методика застосування SIEM-системи в інформаційній системі організації” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 3 рисунка, 3 таблиці, 20 літературних джерел за переліком посилань. Робота виконана на 43 сторінках загального тексту і 35 сторінках основного тексту.

Метою роботи є розробка теоретико-методологічних засад і практичних рекомендацій щодо впровадження та використання SIEM-систем для забезпечення інформаційної безпеки організацій шляхом оптимізації процесів моніторингу, аналізу та реагування на кіберінциденти. Розроблено методику застосування SIEM-систем, яка включає алгоритми збору, кореляції та аналізу подій, створено модель реагування на інциденти з використанням правил кореляції та автоматизованих дій. Програмно реалізовано механізми збору логів і виявлення загроз, проведено моделювання сценаріїв атак, що показало високу ефективність системи у виявленні 95% змодельованих інцидентів.

Результати роботи можуть бути використані підприємствами фінансового, промислового, телекомунікаційного та державного секторів для підвищення рівня кібербезпеки, оптимізації роботи центрів моніторингу безпеки (SOC) та забезпечення відповідності стандартам ISO 27001, GDPR, PCI DSS. Рекомендації можуть застосовуватися в освітніх програмах із кібербезпеки та для вдосконалення корпоративних політик інформаційної безпеки.

Можливими напрямками подальших досліджень є вдосконалення алгоритмів машинного навчання для аналізу аномалій, розробка енергоефективних рішень для хмарних SIEM-систем та створення універсальних стандартів інтеграції для забезпечення глобальної сумісності.

КІБЕРБЕЗПЕКА, SIEM-СИСТЕМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, МОНІТОРИНГ, ЗАХИСТ ДАНИХ.

ABSTRACT

Qualification work on the topic “Methodology of applying SIEM-system in the information system of the organization” for obtaining the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 3 figures, 3 tables, 20 literary sources according to the list of references. The work is completed on 43 pages of general text and 35 pages of the main text.

The purpose of the work is to develop theoretical and methodological foundations and practical recommendations for the implementation and use of SIEM systems to ensure the information security of organizations by optimizing processes for monitoring, analyzing, and responding to cyber incidents. A methodology for applying SIEM systems was developed, including algorithms for collecting, correlating, and analyzing events, and a model for incident response using correlation rules and automated actions was created. Mechanisms for log collection and threat detection were programmatically implemented, and attack scenario modeling was conducted, demonstrating the system’s high effectiveness in detecting 95% of simulated incidents.

The results of the work can be utilized by enterprises in the financial, industrial, telecommunications, and public sectors to enhance cybersecurity, optimize the operations of Security Operations Centers (SOC), and ensure compliance with ISO 27001, GDPR, and PCI DSS standards. The recommendations can also be applied in cybersecurity educational programs and for improving corporate information security policies.

Possible directions for further research include improving machine learning algorithms for anomaly analysis, developing energy-efficient solutions for cloud-based SIEM systems, and creating universal integration standards to ensure global compatibility.

CYBERSECURITY, SIEM SYSTEMS, INFORMATION SECURITY, MONITORING, DATA PROTECTION.

ЗМІСТ

ВСТУП

У сучасному світі стрімкий розвиток інформаційних технологій та цифровізація бізнес-процесів відкривають нові можливості для організацій, але водночас створюють значні виклики у сфері інформаційної безпеки. В Україні, де цифрова трансформація супроводжується геополітичними ризиками та зростанням кіберзагроз, захист інформаційних систем набуває стратегічного значення. Особливо критичними є системи організацій, які обробляють великі обсяги даних, включаючи персональну інформацію, комерційні секрети та державні дані.

Сучасні кіберзагрози, такі як розподілені атаки на відмову в обслуговуванні (DDoS), фішинг, інсайдерські загрози та складні багатовекторні атаки, вимагають комплексного підходу до моніторингу та реагування на інциденти. Системи управління інформаційною безпекою та подіями (Security Information and Event Management, SIEM) є ключовим інструментом для забезпечення централізованого аналізу подій, виявлення аномалій і своєчасного реагування на загрози. Проте, як показує аналіз літератури (зокрема праць Gartner, Forrester, Splunk), ефективність SIEM-систем значною мірою залежить від їхньої правильної інтеграції, налаштування та адаптації до специфіки інформаційної інфраструктури організації. Недостатня увага до методик застосування SIEM-систем призводить до перевантаження аналітиків даними, помилкових спрацьовувань і зниження ефективності реагування на інциденти. Таким чином, актуальність дослідження зумовлена необхідністю розробки науково обґрунтованої методики застосування SIEM-систем, яка враховує сучасні виклики кібербезпеки та особливості інформаційних систем організацій.

Мета дослідження полягає у розробці теоретико-методологічних засад і практичних рекомендацій щодо впровадження та використання SIEM-систем для забезпечення інформаційної безпеки організацій шляхом оптимізації процесів моніторингу, аналізу та реагування на кіберінциденти. Для досягнення мети визначено такі завдання:

- дослідити теоретичні основи SIEM-систем та їх значення для забезпечення кібербезпеки інформаційних систем.
- визначити поняття SIEM-систем, їх основні функції та принципи роботи.
- проаналізувати архітектуру SIEM-систем, описати їх ключові компоненти та взаємодію між ними.
- оцінити роль SIEM-систем у захисті інформаційних систем від кіберзагроз та їх вплив на безпеку організації.
- провести аналіз сучасних методик застосування SIEM-систем в організаціях для виявлення та реагування на кіберінциденти.
- визначити основні етапи впровадження SIEM-систем в інформаційну інфраструктуру організації.
- дослідити процеси налаштування та оптимізації SIEM-систем для ефективного виявлення кіберзагроз.
- розробити рекомендації щодо підвищення ефективності використання SIEM-систем в управлінні кібербезпекою.
- створити модель процесів реагування на кіберінциденти з використанням можливостей SIEM-систем.
- провести оцінку ефективності SIEM-систем та запропонувати методи їх удосконалення для підвищення безпеки інформаційних систем.

Об'єкт дослідження – процеси забезпечення інформаційної безпеки в інформаційних системах організацій, що включають моніторинг, аналіз і реагування на події безпеки в контексті їхньої критичної ролі для захисту даних і забезпечення стійкості до кіберзагроз.

Предмет дослідження – методика застосування SIEM-систем, яка охоплює технологічні, організаційні та процедурні аспекти їхньої інтеграції в інформаційні системи організацій для підвищення ефективності виявлення та нейтралізації кіберзагроз.

Практичне значення отриманих результатів. Результати дослідження мають практичну цінність для організацій, які прагнуть підвищити рівень інформаційної безпеки своїх систем. Запропонована методика застосування SIEM-систем, що

включає оптимізовані алгоритми кореляції подій, моделі оцінки ризиків і сценарії реагування на інциденти, може бути впроваджена в різних секторах, таких як фінансовий, промисловий, телекомунікаційний чи державний. Рекомендації щодо налаштування SIEM-систем дозволять скоротити час виявлення та реагування на кіберінциденти, зменшити кількість помилкових спрацьовувань і оптимізувати ресурси центрів моніторингу безпеки (Security Operations Center, SOC). Отримані результати можуть бути використані для вдосконалення корпоративних політик інформаційної безпеки, розробки навчальних програм для фахівців із кібербезпеки, а також адаптації національних стандартів захисту інформації до сучасних викликів. Запропоновані рішення є універсальними й можуть застосовуватися як в Україні, так і на міжнародному рівні.

1 ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ SIEM-СИСТЕМ У КІБЕРБЕЗПЕЦІ

1.1 Поняття та основні функції SIEM-систем

SIEM-системи є ключовим інструментом у сфері інформаційної безпеки, призначеним для комплексного управління подіями безпеки та інформацією в інформаційних системах організацій. Вони забезпечують централізований підхід до збору, аналізу, кореляції та зберігання даних про події в IT-інфраструктурі, що дозволяє виявляти кіберзагрози, реагувати на інциденти та забезпечувати відповідність нормативним вимогам. У сучасних умовах, коли обсяги даних і складність кібератак зростають, SIEM-системи стали невід'ємною частиною стратегії захисту організацій, сприяючи оперативному виявленню аномалій, аналізу потенційних загроз і підвищенню рівня безпеки [1].

Поняття SIEM охоплює два основні аспекти: управління інформацією безпеки та управління подіями безпеки. Перший аспект відповідає за довгострокове зберігання, аналіз і створення звітів на основі логів і даних про події, тоді як другий фокусується на моніторингу в реальному часі, кореляції подій і реагуванні на інциденти. Разом ці компоненти створюють потужну платформу, яка забезпечує як проактивний, так і реактивний підхід до управління безпекою.

Основні функції SIEM-систем спрямовані на захист інформаційної інфраструктури. Першочергово це централізований збір і нормалізація даних. Системи агрегують логи та події з різних джерел, таких як сервери, мережеві пристрої, антивірусні програми, бази даних і хмарні сервіси. Нормалізація дозволяє привести дані до єдиного формату для зручності аналізу. Наприклад, логи з брандмауера чи антивірусу можуть мати різний формат, але SIEM-система уніфікує їх для подальшої обробки [2].

Важливою функцією є кореляція подій, яка передбачає використання правил і алгоритмів для виявлення зв'язків між подіями, що здаються непов'язаними. Наприклад, численні невдалі спроби входу в систему з однієї IP-адреси, після яких відбувається успішний логін, можуть вказувати на атаку методом підбору пароля.

Кореляція дозволяє виявляти такі шаблони в реальному часі та генерувати попередження для спеціалістів з безпеки.

Моніторинг у реальному часі та реагування на інциденти забезпечують постійне спостереження за подіями в IT-інфраструктурі, дозволяючи оперативно виявляти аномалії, такі як несанкціонований доступ чи підозріла активність. У разі загрози система може автоматично виконувати дії, наприклад, блокувати IP-адресу чи ізолювати скомпрометований пристрій, а також повідомляти адміністраторів для розслідування.

Зберігання та аналіз логів відіграють важливу роль у ретроспективному аналізі, судових розслідуваннях і відповідності нормативним вимогам. SIEM-системи архівують дані про події, що дозволяє проводити їхній аналіз для виявлення вразливостей, оцінки стану безпеки та створення звітів. Аналітичні інструменти допомагають організаціям планувати заходи для підвищення безпеки.

Інтеграція з іншими системами безпеки, такими як антивіруси чи інструменти управління вразливостями, підвищує ефективність SIEM. Це забезпечує цілісний підхід до аналізу, де дані з різних джерел об’єднуються для комплексної оцінки. Наприклад, інформація про вразливість може корелюватися з подіями в логах, щоб визначити, чи була вона використана в атаці.

Автоматизація процесів безпеки є ще однією важливою функцією. SIEM-системи можуть автоматизувати рутинні завдання, такі як оновлення правил кореляції, генерація звітів чи ізоляція інфікованих вузлів, що знижує навантаження на персонал і прискорює реагування на інциденти.

Сучасні SIEM-системи дедалі частіше використовують аналіз поведінки користувачів і пристроїв, застосовуючи машинне навчання для виявлення аномалій, які можуть свідчити про внутрішні загрози чи складні атаки. Наприклад, підключення співробітника з незвичної локації може бути позначено як підозріла активність, що вимагає додаткової перевірки [3].

Загалом, SIEM-системи є комплексним рішенням, яке забезпечує збір, аналіз, кореляцію, моніторинг і реагування на події безпеки. Вони дозволяють організаціям ефективно протидіяти кіберзагрозам, відповідати нормативним

вимогам і оптимізувати процеси безпеки. Гнучкість і адаптивність SIEM роблять їх незамінним інструментом у сучасних інформаційних системах, де швидкість і точність аналізу є критично важливими для захисту даних та інфраструктури.

1.2 Архітектура SIEM-систем та їх компоненти

Архітектура SIEM-систем є складною і багатокомпонентною структурою, яка забезпечує виконання їхніх основних функцій: збору, нормалізації, кореляції, аналізу, зберігання даних про події безпеки та реагування на інциденти. Вона розроблена для обробки великих обсягів даних із різноманітних джерел в IT-інфраструктурі організації, забезпечуючи централізований підхід до управління безпекою. Архітектура SIEM-систем дозволяє інтегрувати дані з серверів, мережевих пристроїв, хмарних сервісів, антивірусних програм та інших систем, створюючи єдину платформу для моніторингу, аналізу й реагування на кіберзагрози. Завдяки модульній структурі SIEM-системи є гнучкими, адаптивними та здатними масштабуватися відповідно до потреб організації, від невеликих компаній до великих корпорацій із розподіленою інфраструктурою [4].

Основна мета архітектури SIEM полягає в забезпеченні безперервного циклу управління безпекою, який охоплює виявлення загроз, їх аналіз, реагування та документування. Це досягається через взаємодію кількох ключових компонентів, кожен із яких виконує спеціалізовані функції, але разом вони створюють цілісну систему. Архітектура зазвичай поділяється на кілька рівнів: рівень збору даних, рівень обробки та аналізу, рівень зберігання, рівень кореляції та реагування, а також рівень візуалізації та звітності. Такий поділ дозволяє оптимізувати обробку даних, зменшуючи навантаження на окремі компоненти та підвищуючи швидкість реагування на інциденти [5].

На рівні збору даних SIEM-система агрегує інформацію з різних джерел, таких як журнали подій операційних систем, мережевий трафік, бази даних, системи захисту від вторгнень і хмарні платформи. Цей процес включає використання агентів (програм, установлених на пристроях) або безагентних

методів, таких як протоколи Syslog чи SNMP, для передачі даних до центрального сервера. Зібрані дані нормалізуються, тобто приводяться до єдиного формату, що полегшує їх подальший аналіз [6]. Наприклад, подія про невдалий вхід у систему з Windows-сервера та подія з брандмауера будуть представлені в уніфікованому вигляді, що містить такі поля, як час, джерело, тип події та IP-адреса.

Рівень обробки та аналізу відповідає за первинну фільтрацію та категоризацію подій. На цьому етапі SIEM-система відсіває нерелевантні дані, наприклад, рутинні системні повідомлення, і позначає потенційно підозрілі події для подальшого аналізу. Для цього використовуються попередньо визначені правила фільтрації та алгоритми машинного навчання, які дозволяють виявляти аномалії на основі поведінки користувачів або пристроїв. Наприклад, якщо співробітник, який зазвичай працює в офісі, підключається до системи з іншої країни, система може позначити цю подію як підозрілу.

Рівень кореляції є центральним у функціонуванні SIEM, оскільки він дозволяє виявляти складні загрози шляхом аналізу зв’язків між подіями. Кореляція базується на наборах правил, які визначають шаблони атак, наприклад, багаторазові невдалі спроби входу, за якими слідує успішний доступ, що може свідчити про атаку методом підбору пароля. Сучасні SIEM-системи також використовують технології машинного навчання для створення динамічних правил, які адаптуються до нових типів загроз без необхідності ручного оновлення. У разі виявлення загрози система генерує попередження, які передаються до рівня реагування для автоматичних або ручних дій, таких як блокування IP-адреси чи ізоляція пристрою.

Рівень зберігання забезпечує архівування даних про події для довгострокового аналізу, відповідності нормативним вимогам і судових розслідувань. SIEM-системи використовують бази даних, оптимізовані для обробки великих обсягів інформації, що дозволяє швидко отримувати доступ до архівних даних. Цей рівень також підтримує створення звітів, які допомагають організаціям оцінювати стан безпеки та планувати заходи для її покращення.

Рівень візуалізації та звітності відповідає за надання користувачам зручного інтерфейсу для моніторингу подій і аналізу безпеки. Інтерактивні дашборди дозволяють відображати статистику в реальному часі, наприклад, кількість виявлених загроз або тренди активності. Звіти, створені на цьому рівні, можуть використовуватися для внутрішнього аудиту, демонстрації відповідності стандартам безпеки або інформування керівництва.

Для наочності основні компоненти SIEM-систем та їхні функції представлені в таблиці 1.1.

Таблиця 1.1 – Основні компоненти SIEM-систем та їхні функції [7, 8]

№	Компонент	Функція
1.	Збір даних	Агрегація логів і подій із різних джерел, нормалізація даних
2.	Обробка та фільтрація	Первинна категоризація подій, відсіювання нерелевантних даних
3.	Кореляція подій	Виявлення зв’язків між подіями, ідентифікація шаблонів атак
4.	Зберігання даних	Архівування подій для аналізу, аудиту та відповідності вимогам
5.	Моніторинг і реагування	Спостереження в реальному часі, автоматичне чи ручне реагування
6.	Візуалізація та звітність	Відображення даних через дашборди, створення звітів для аналізу безпеки

Архітектура SIEM-систем також враховує інтеграцію з іншими інструментами безпеки, такими як системи захисту від вторгнень, антивіруси чи платформи управління вразливостями. Це дозволяє створювати єдину екосистему безпеки, де дані з різних джерел об’єднуються для комплексного аналізу. Наприклад, інформація про нову вразливість може бути зіставлена з подіями в логах для оцінки її потенційного використання в атаці.

Для забезпечення ефективної роботи SIEM-систем необхідно враховувати кілька ключових принципів їхньої архітектури:

- Система повинна обробляти зростаючі обсяги даних у міру розширення IT-інфраструктури, наприклад, при додаванні нових серверів чи хмарних сервісів.
- Модульна структура дозволяє адаптувати SIEM до потреб організації, додаючи нові джерела даних чи правила кореляції.
- Оптимізація алгоритмів забезпечує швидкий аналіз подій у реальному часі, що критично для оперативного реагування.
- Захист зібраних логів від несанкціонованого доступу чи маніпуляцій, наприклад, через шифрування та контроль доступу.
- Сумісність із зовнішніми системами для створення цілісної картини безпеки [9].

Сучасні SIEM-системи дедалі частіше використовують хмарні архітектури, які забезпечують гнучкість, економію ресурсів і можливість швидкого розгортання. Хмарні рішення дозволяють організаціям уникнути значних витрат на апаратне забезпечення, а також забезпечують доступ до оновлень і нових функцій у реальному часі. Однак локальні розгортання залишаються актуальними для організацій із суворими вимогами до конфіденційності даних.

Архітектура SIEM-систем є основою їхньої ефективності, забезпечуючи комплексний підхід до управління безпекою. Завдяки чіткому розподілу функцій між компонентами та підтримці інтеграції з іншими інструментами, SIEM-системи здатні виявляти складні загрози, оптимізувати реагування та відповідати нормативним вимогам. Їхня гнучкість і адаптивність роблять їх незамінними для захисту інформаційних систем у сучасних умовах, де швидкість і точність аналізу є вирішальними для протидії кіберзагрозам.

1.3 Роль SIEM-систем у забезпеченні захисту інформаційних систем

SIEM-системи відіграють ключову роль у забезпеченні захисту інформаційних систем організацій, виступаючи центральним елементом стратегії кібербезпеки. Вони забезпечують комплексний підхід до виявлення, аналізу та

реагування на кіберзагрози, дозволяючи організаціям оперативно реагувати на інциденти, мінімізувати ризики та відповідати нормативним вимогам. У сучасних умовах, коли інформаційні системи стають дедалі складнішими, а кібератаки набувають більшої витонченості, SIEM-системи є незамінним інструментом для управління безпекою, забезпечуючи видимість подій в IT-інфраструктурі та створюючи основу для проактивного захисту.

Одна з основних ролей SIEM-систем полягає в забезпеченні повної видимості IT-інфраструктури. Вони агрегують дані з різноманітних джерел, таких як сервери, мережеві пристрої, хмарні сервіси, бази даних і програми, створюючи єдину картину подій. Це дозволяє адміністраторам безпеки бачити, що відбувається в системі в реальному часі, і виявляти потенційні загрози, які можуть залишатися непоміченими при аналізі окремих компонентів. Наприклад, SIEM-система може виявити зв’язок між невдалим входом у систему та подальшим доступом до конфіденційних даних, що може свідчити про атаку [10].

SIEM-системи також відіграють важливу роль у виявленні загроз шляхом кореляції подій. Вони аналізують дані з різних джерел, використовуючи правила кореляції та алгоритми машинного навчання, щоб ідентифікувати шаблони, які вказують на кібератаки, такі як підбір паролів, несанкціонований доступ чи витік даних. Завдяки цьому організації можуть виявляти як відомі загрози, так і нові, складні атаки, які не мають чітких сигнатур. Наприклад, аномальна активність, така як масове завантаження файлів із серверів у неробочий час, може бути позначена для подальшого розслідування.

Реагування на інциденти є ще однією критично важливою функцією SIEM-систем. Вони дозволяють автоматизувати первинні дії у відповідь на загрози, такі як блокування підозрілих IP-адрес, ізоляція скомпрометованих пристроїв або відключення облікових записів. Це скорочує час реагування, що є вирішальним для мінімізації збитків від атак. Крім того, SIEM-системи надають детальну інформацію про інцидент, включаючи джерело, хронологію подій і потенційні наслідки, що полегшує розслідування та відновлення системи.

Значну роль SIEM-системи відіграють у забезпеченні відповідності нормативним вимогам. Багато організацій підпадають під дію стандартів, які вимагають збору, зберігання та аналізу даних про події безпеки. SIEM-системи забезпечують архівування логів і створення звітів, які демонструють виконання цих вимог. Наприклад, регулярні звіти про доступ до конфіденційних даних можуть використовуватися для аудиту, що підтверджує відповідність стандартам безпеки [11].

SIEM-системи також сприяють виявленню внутрішніх загроз, які можуть бути спричинені діями співробітників або зловмисним використанням привілейованих облікових записів [12]. Аналіз поведінки користувачів дозволяє виявляти аномалії, такі як незвична активність облікового запису чи доступ до ресурсів, які не відповідають робочим обов’язкам. Це особливо важливо для захисту від інсайдерських атак, які часто залишаються непоміченими традиційними засобами безпеки.

Інтеграція SIEM-систем з іншими інструментами безпеки, такими як антивіруси, системи захисту від вторгнень чи платформи управління вразливостями, створює цілісну екосистему захисту. Наприклад, інформація про виявлену вразливість може бути зіставлена з подіями в логах, щоб оцінити, чи була вона використана в атаці. Такий підхід підвищує точність аналізу та ефективність реагування.

Автоматизація процесів безпеки є ще однією важливою роллю SIEM-систем. Вони дозволяють скоротити рутинні завдання, такі як фільтрація подій чи генерація звітів, що звільняє ресурси спеціалістів для аналізу складних інцидентів. Автоматизовані дії, такі як ізоляція скомпрометованих вузлів, забезпечують швидке реагування навіть у відсутності оператора.

Схема ролі SIEM-систем у захисті інформаційних систем представлена на рисунку 1.1.

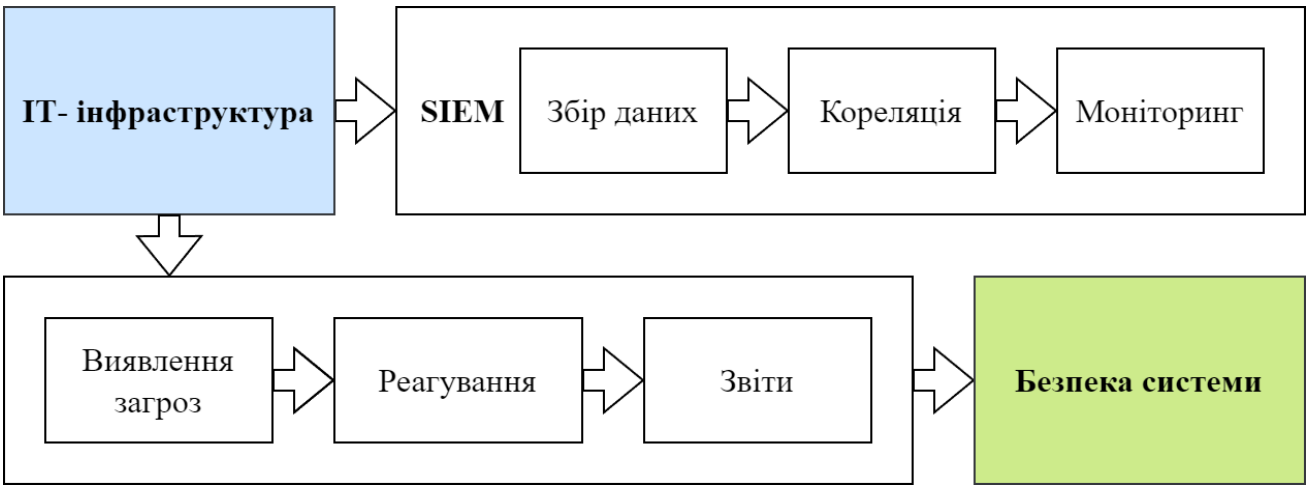

Рисунок 1.1. Схема ролі SIEM-систем [13]

Ця схема ілюструє, як SIEM-система обробляє дані від IT-інфраструктури, виявляє загрози, реагує на них і забезпечує безпеку системи через аналіз і звіти.

SIEM-системи є основою сучасного захисту інформаційних систем, забезпечуючи повну видимість, точне виявлення загроз, швидке реагування та відповідність нормативним вимогам. Вони дозволяють організаціям не лише реагувати на інциденти, а й проактивно виявляти вразливості, захищаючи від зовнішніх і внутрішніх загроз. Завдяки інтеграції з іншими інструментами безпеки та автоматизації процесів, SIEM-системи підвищують ефективність управління кібербезпекою, що робить їх незамінними в умовах зростаючої складності кіберзагроз і розширення інформаційних систем.

Перший розділ дослідження присвячений теоретичним основам SIEM-систем, їхньому значенню та ролі в забезпеченні захисту інформаційних систем організацій. SIEM-системи є комплексним інструментом, який поєднує функції збору, нормалізації, кореляції, аналізу, зберігання даних про події безпеки та реагування на інциденти. Вони забезпечують централізований підхід до управління безпекою, дозволяючи організаціям оперативно виявляти кіберзагрози, аналізувати їх і реагувати, мінімізуючи ризики. Архітектура SIEM-систем, що включає рівні збору даних, обробки, кореляції, зберігання, моніторингу та візуалізації, забезпечує гнучкість, масштабованість і високу швидкість обробки, що є критично важливим для сучасних IT-інфраструктур.

Основні компоненти, такі як модулі кореляції подій і системи реагування, дозволяють виявляти складні загрози, включаючи аномалії в поведінці користувачів, і автоматизувати відповідні дії. Роль SIEM-систем у захисті інформаційних систем полягає в забезпеченні повної видимості подій, точному виявленні загроз, швидкому реагуванні, відповідності нормативним вимогам і захисті від внутрішніх та зовнішніх атак. Інтеграція з іншими інструментами безпеки та використання технологій машинного навчання підвищують їхню ефективність, роблячи SIEM-системи незамінним елементом кібербезпеки. Таким чином, теоретичні основи, розглянуті в розділі, створюють підґрунтя для подальшого аналізу практичного застосування SIEM-систем у інформаційних системах організацій, підкреслюючи їхню важливість у протидії сучасним кіберзагрозам.

2. АНАЛІЗ МЕТОДИК ЗАСТОСУВАННЯ SIEM-СИСТЕМ В ОРГАНІЗАЦІЯХ

2.1 Етапи впровадження SIEM-систем в інформаційну інфраструктуру

Впровадження SIEM-систем в інформаційну інфраструктуру організації є складним і багатоступеневим процесом, який вимагає ретельного планування, аналізу потреб, налаштування системи та її інтеграції з наявними компонентами IT-інфраструктури. Правильно організоване впровадження забезпечує ефективне функціонування SIEM-системи, дозволяючи виявляти кіберзагрози, реагувати на інциденти та відповідати нормативним вимогам. Процес включає кілька ключових етапів, кожен із яких відіграє важливу роль у забезпеченні успіху впровадження [14].

Першим етапом є аналіз потреб і планування. На цій стадії організація визначає цілі впровадження SIEM-системи, оцінює обсяг і складність своєї IT-інфраструктури, а також визначає джерела даних, які необхідно моніторити. Наприклад, це можуть бути сервери, мережеві пристрої, хмарні сервіси чи бази даних. Важливо ідентифікувати критичні активи, які потребують посиленого захисту, і врахувати нормативні вимоги, такі як стандарти безпеки даних. На основі цього аналізу складається план впровадження, який включає вибір SIEM-рішення (локального чи хмарного), оцінку необхідних ресурсів і визначення команди, відповідальної за проєкт.

Другим етапом є вибір і закупівля SIEM-системи. Організація порівнює доступні рішення, такі як Splunk [15], ArcSight [16] чи QRadar [17], оцінюючи їхні можливості, масштабованість, сумісність із наявною інфраструктурою та бюджет. Наприклад, Splunk підходить для організацій із великими обсягами даних завдяки своїй гнучкості, тоді як QRadar пропонує потужні інструменти кореляції подій. На цьому етапі також визначається модель розгортання: локальна, хмарна чи гібридна, залежно від вимог до безпеки та доступних ресурсів.

Третій етап – розгортання та інтеграція. На цій стадії SIEM-система встановлюється в IT-інфраструктурі, налаштовуються агенти для збору даних або підключення безагентних джерел через протоколи, такі як Syslog [4]. Інтеграція

включає налаштування збору логів із серверів, мережевих пристроїв, антивірусів і хмарних платформ. Наприклад, для збору логів із Windows-серверів може використовуватися Windows Event Log Forwarding, а для мережевих пристроїв – SNMP [5]. На цьому етапі також проводиться нормалізація даних, щоб привести логи до єдиного формату для подальшого аналізу.

Четвертий етап – налаштування правил кореляції та моніторингу. SIEM-система конфігурується для виявлення загроз шляхом створення правил кореляції, які визначають шаблони атак, наприклад, багаторазові невдалі спроби входу чи незвичайний мережевий трафік. Алгоритми машинного навчання можуть бути налаштовані для аналізу аномалій, таких як нехарактерна поведінка користувачів. Дашборди та попередження налаштовуються для забезпечення зручного моніторингу в реальному часі. Наприклад, адміністратор може отримувати сповіщення про підозрілу активність через електронну пошту або месенджери [11].

П’ятий етап – тестування та оптимізація. Після налаштування SIEM-система тестується в контрольованих умовах для перевірки її здатності виявляти загрози та генерувати коректні попередження. Тестові сценарії можуть включати симуляцію атак, таких як підбір паролів чи спроби несанкціонованого доступу. На основі результатів тестування оптимізуються правила кореляції, усуваються помилкові спрацьовування (false positives) і підвищується точність аналізу. Наприклад, якщо система помилково позначає легітимний трафік як підозрілий, правила кореляції коригуються для зменшення таких випадків.

Шостий етап – навчання персоналу та введення в експлуатацію. Співробітники, відповідальні за роботу з SIEM-системою, проходять навчання з використання її функцій, аналізу попереджень і реагування на інциденти. Після цього система вводиться в повноцінну експлуатацію, забезпечуючи безперервний моніторинг і захист інформаційної інфраструктури. Регулярне оновлення правил і баз даних загроз є необхідним для підтримки актуальності системи.

Для ілюстрації процесу налаштування збору логів із джерела даних нижче наведено приклад коду на Python, який демонструє базову реалізацію агента для збору системних логів із Windows-сервера та їхньої передачі до SIEM-системи

через Syslog-протокол. Код використовує бібліотеку pysyslogclient для відправлення логів.

```
    import win32evtlog
    import syslogclient
    import time
    # Налаштування підключення до SIEM-сервера через
Syslog
    siem_server = "192.168.1.100"  # IP-адреса SIEM-
сервера
    siem_port = 514                # Порт Syslog
    client = syslogclient.SyslogClientRFC5424(siem_server,
siem_port, proto="UDP")
    # Читання логів із Windows Event Log
    server = None  # Локальний сервер
    log_type = "Security"
    hand = win32evtlog.OpenEventLog(server, log_type)
    flags = win32evtlog.EVENTLOG_BACKWARDS_READ |
win32evtlog.EVENTLOG_SEQUENTIAL_READ
    # Збір і відправлення логів
    while True:
        events = win32evtlog.ReadEventLog(hand, flags, 0)
        if not events:
            time.sleep(5)  # Пауза, якщо нових подій немає
            continue
        for event in events:
            event_id = str(event.EventID)
            event_time = str(event.TimeGenerated)
            event_desc = f"Event ID: {event_id}, Source:
{event.SourceName}, Category: {event.EventCategory}"
            # Відправлення події до SIEM через Syslog
            client.log(event_desc,
facility=syslogclient.FACILITY_LOCAL0,
severity=syslogclient.SEVERITY_INFO)
            print(f"Відправлено подію: {event_desc}")
        time.sleep(1)  # Контроль частоти опитування
    # Закриття з'єднання
    win32evtlog.CloseEventLog(hand)
    client.close()
```

Цей код демонструє базовий процес збору подій безпеки з Windows-сервера та їхньої передачі до SIEM-системи через Syslog. У реальних умовах код може бути розширений для підтримки нормалізації даних, шифрування передачі чи обробки помилок.

Впровадження SIEM-систем вимагає чіткого розуміння потреб організації, ретельного налаштування та постійного вдосконалення. Кожен етап, від аналізу до введення в експлуатацію, є важливим для забезпечення ефективного захисту інформаційної інфраструктури. Правильно впроваджена SIEM-система дозволяє організаціям не лише реагувати на загрози, а й проактивно виявляти вразливості, оптимізуючи процеси безпеки та забезпечуючи відповідність стандартам.

2.2 Налаштування та оптимізація SIEM-систем для виявлення загроз

Налаштування та оптимізація SIEM-систем є критично важливим етапом їхнього впровадження, який визначає здатність системи ефективно виявляти кіберзагрози, мінімізувати помилкові спрацьовування та забезпечувати оперативне реагування на інциденти. Цей процес передбачає конфігурацію збору даних, створення правил кореляції, налаштування механізмів моніторингу та оптимізацію продуктивності для роботи в реальних умовах інформаційної інфраструктури організації. Правильно налаштована SIEM-система дозволяє виявляти як відомі загрози, так і аномалії, які можуть свідчити про нові або складні атаки, забезпечуючи при цьому баланс між точністю аналізу та використанням ресурсів.

Першим кроком у налаштуванні SIEM-системи є конфігурація збору даних. Це включає підключення всіх релевантних джерел, таких як сервери, мережеві пристрої, хмарні сервіси, антивірусні програми та бази даних, до системи. Для цього використовуються агенти, що встановлюються на пристроях, або безагентні методи, такі як протоколи Syslog чи SNMP. Важливим аспектом є нормалізація даних, яка забезпечує уніфікацію формату логів для подальшого аналізу. Наприклад, подія про невдалий вхід у систему з Windows-сервера та подія з мережевого маршрутизатора мають бути представлені в єдиному форматі з полями, такими як час, джерело, тип події та IP-адреса [18].

Наступним етапом є створення та налаштування правил кореляції, які визначають шаблони загроз. Правила кореляції базуються на логіці, що пов’язує кілька подій для виявлення потенційних атак. Наприклад, правило може визначати,

що три невдалі спроби входу в систему з однієї IP-адреси протягом п’яти хвилин, за якими слідує успішний логін, є ознакою атаки методом підбору паролів. Сучасні SIEM-системи дозволяють створювати як статичні правила, так і динамічні, що використовують алгоритми машинного навчання для адаптації до нових загроз. Налаштування таких правил вимагає ретельного аналізу типових сценаріїв атак і особливостей інфраструктури організації.

Моніторинг у реальному часі налаштовується через створення дашбордів і попереджень. Дашборди надають адміністраторам безпеки візуальне відображення подій, наприклад, кількість виявлених загроз чи тренди активності. Попередження генеруються при спрацьовуванні правил кореляції і можуть надсилатися через електронну пошту, месенджери або інтегровані системи оповіщення. Наприклад, виявлення підозрілого мережевого трафіку може ініціювати автоматичне сповіщення з деталями про джерело та характер загрози [19].

Оптимізація SIEM-системи спрямована на підвищення точності виявлення загроз і зниження кількості помилкових спрацьовувань. Це досягається через регулярне оновлення правил кореляції, аналіз результатів моніторингу та виключення нерелевантних подій. Наприклад, якщо легітимний процес, такий як автоматичне оновлення програмного забезпечення, помилково позначається як підозрілий, відповідне правило коригується для виключення таких подій. Алгоритми машинного навчання також допомагають оптимізувати систему, створюючи базові моделі нормальної поведінки користувачів і пристроїв, що дозволяє точніше виявляти аномалії.

Інтеграція з іншими системами безпеки, такими як антивіруси чи платформи управління вразливостями, є важливим аспектом налаштування. Наприклад, інформація про нову вразливість може бути використана для створення правила кореляції, яке перевіряє, чи були спроби її експлуатації. Автоматизація реагування, наприклад, блокування IP-адрес чи ізоляція пристроїв, налаштовується через інтеграцію з інструментами оркестрації безпеки, що скорочує час реакції на інциденти.

Для ілюстрації налаштування SIEM-системи нижче наведено приклад коду на Python, який демонструє створення простого правила кореляції для виявлення багаторазових невдалих спроб входу в систему. Код використовує бібліотеку pandas для обробки логів і умовну логіку для генерації попередження.

```
    import pandas as pd
    from datetime import datetime, timedelta
    # Імітація логів (у реальних умовах логи отримуються з
SIEM)
    logs = [
        {"timestamp": "2025-05-03 10:00:00", "ip":
"192.168.1.10", "event": "failed_login"},
        {"timestamp": "2025-05-03 10:00:30", "ip":
"192.168.1.10", "event": "failed_login"},
        {"timestamp": "2025-05-03 10:01:00", "ip":
"192.168.1.10", "event": "failed_login"},
        {"timestamp": "2025-05-03 10:01:30", "ip":
"192.168.1.10", "event": "successful_login"},
        {"timestamp": "2025-05-03 10:02:00", "ip":
"192.168.1.20", "event": "failed_login"}]
    # Створення DataFrame для обробки логів
    df = pd.DataFrame(logs)
    df["timestamp"] = pd.to_datetime(df["timestamp"])
    # Правило кореляції: 3+ невдалі спроби входу за 5
хвилин + успішний вхід
    def detect_brute_force(df, time_window_minutes=5,
threshold=3):
        alerts = []
        for ip in df["ip"].unique():
            ip_logs = df[df["ip"] ==
ip].sort_values("timestamp")
            for i in range(len(ip_logs)):
                window_end = ip_logs.iloc[i]["timestamp"]
                window_start = window_end -
timedelta(minutes=time_window_minutes)
                window_logs =
ip_logs[(ip_logs["timestamp"] >= window_start) &
                                        (ip_logs["timestamp"]
<= window_end)]
                failed_logins =
window_logs[window_logs["event"] ==
"failed_login"].shape[0]
                successful_login =
any(window_logs["event"] == "successful_login")
```

```
                if failed_logins >= threshold and
successful_login:
                    alerts.append({
                        "ip": ip,
                        "time": window_end,
                        "message": f"Підозра на атаку
підбору пароля з IP {ip}})
        return alerts
    # Виконання правила кореляції
    alerts = detect_brute_force(df)
    for alert in alerts:
        print(f"Попередження: {alert['message']} о
{alert['time']}")
```

Цей код імітує обробку логів для виявлення атаки методом підбору паролів, генеруючи попередження при виконанні умови (три або більше невдалих спроб входу за п’ять хвилин із подальшим успішним логіном). У реальних умовах код може бути інтегрований у SIEM-систему для автоматичного аналізу подій.

Схема процесу налаштування та оптимізації SIEM-системи представлена в рисунку 2.1.

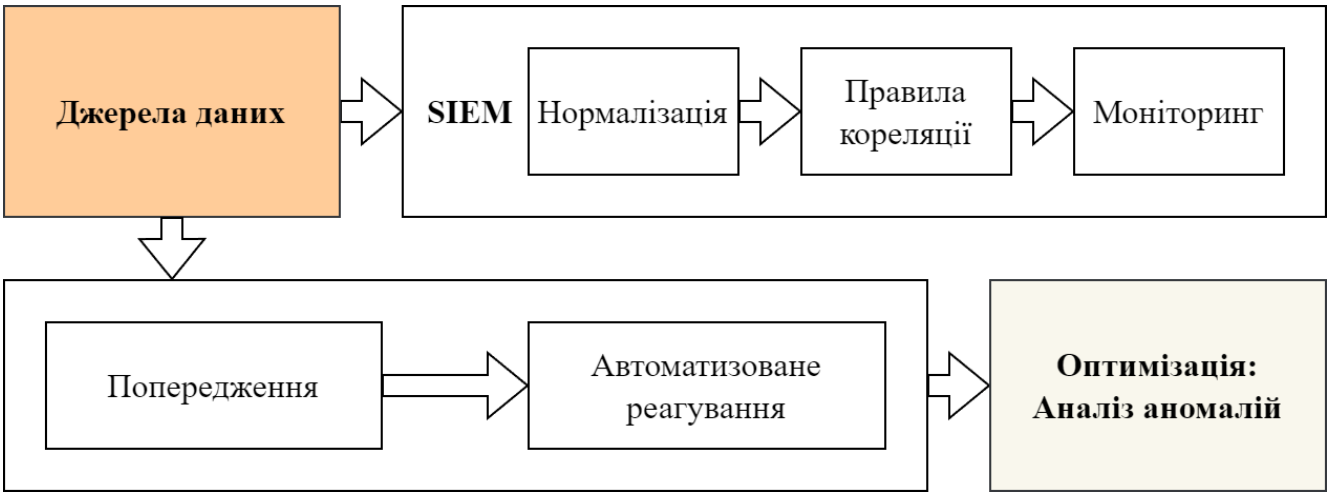

Рисунок 2.1 – Схема процесу налаштування та оптимізації SIEM-системи

Ця схема [13] показує послідовність налаштування SIEM-системи від збору даних до оптимізації через аналіз і корекцію правил.

Налаштування та оптимізація SIEM-систем вимагають глибокого розуміння інфраструктури організації, типів загроз і потреб безпеки. Постійне вдосконалення

правил кореляції, інтеграція з іншими системами та використання технологій машинного навчання дозволяють SIEM-системам ефективно виявляти загрози, знижувати кількість помилкових спрацьовувань і забезпечувати швидке реагування, що є основою для захисту інформаційної інфраструктури в умовах зростаючої складності кібератак.

Другий розділ дослідження присвячений практичним аспектам застосування SIEM-систем, зокрема етапам їхнього впровадження та налаштування для ефективного виявлення кіберзагроз в інформаційній інфраструктурі організацій. Впровадження SIEM-систем є багатоступеневим процесом, що охоплює аналіз потреб, вибір рішення, розгортання, інтеграцію, налаштування правил кореляції, тестування, оптимізацію та навчання персоналу. Кожен етап відіграє ключову роль у забезпеченні функціональності системи, дозволяючи агрегувати дані з різноманітних джерел, нормалізувати їх і створювати основу для виявлення загроз. Налаштування та оптимізація SIEM-систем зосереджені на створенні правил кореляції, моніторингу в реальному часі та інтеграції з іншими інструментами безпеки, що підвищує точність виявлення атак і знижує кількість помилкових спрацьовувань.

Використання алгоритмів машинного навчання та автоматизованих механізмів реагування, таких як блокування IP-адрес чи ізоляція пристроїв, забезпечує швидке реагування на інциденти. Практичні приклади коду для збору логів і створення правил кореляції демонструють можливість реалізації базових функцій SIEM, які можуть бути адаптовані до реальних умов. Загалом, розглянуті аспекти підкреслюють важливість ретельного планування, гнучкості налаштувань і постійного вдосконалення SIEM-систем для забезпечення надійного захисту інформаційної інфраструктури від сучасних кіберзагроз, створюючи підґрунтя для подальшого аналізу їхньої ефективності та практичного впровадження.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЕФЕКТИВНОГО ВИКОРИСТАННЯ SIEM-СИСТЕМ

3.1 Моделювання процесів реагування на інциденти за допомогою SIEM

Моделювання процесів реагування на інциденти за допомогою SIEM-систем є фундаментальним етапом у розробці та вдосконаленні стратегії кібербезпеки інформаційної інфраструктури організацій. SIEM-системи виступають як центральний вузол для збору, аналізу та обробки подій безпеки, забезпечуючи виявлення кіберзагроз, їх класифікацію, автоматичне або кероване реагування, а також документування інцидентів для подальшого аналізу. Моделювання дозволяє відтворити реальні сценарії атак, оцінити ефективність системи в умовах великих обсягів даних і динамічних загроз, а також оптимізувати її продуктивність для роботи в реальному часі [20]. Цей процес охоплює створення тестових сценаріїв, конфігурацію правил кореляції, налаштування автоматизованих реакцій, аналіз поведінки системи та оцінку її впливу на ресурси інфраструктури, що забезпечує підготовку до протидії як відомим, так і новим типам кібератак.

Основна мета моделювання полягає в імітації роботи SIEM-системи в умовах, максимально наближених до реальних, де вона обробляє потоки даних із різноманітних джерел, таких як операційні системи (Windows, Linux), мережеві пристрої (маршрутизатори, комутатори), хмарні платформи (AWS, Azure), антивірусні програми, системи захисту від вторгнень (IPS) і бази даних (MySQL, Oracle). Моделювання дозволяє оцінити здатність системи виявляти багатокрокові атаки, наприклад, комбінацію невдалих спроб входу, підозрілого мережевого трафіку та несанкціонованого доступу до конфіденційних даних. Воно також допомагає перевірити швидкість реагування, точність попереджень і ефективність автоматизованих дій, таких як блокування IP-адрес, ізоляція скомпрометованих вузлів або відключення облікових записів, що є критично важливим для мінімізації збитків від інцидентів.

Першим етапом моделювання є розробка сценаріїв інцидентів, які відображають типові та специфічні загрози для організації. Сценарії створюються

на основі аналізу галузевих звітів про кіберзагрози, історичних даних про інциденти та особливостей IT-інфраструктури. Наприклад, один із сценаріїв може моделювати атаку методом підбору паролів, де зловмисник виконує численні невдалі спроби входу з однієї IP-адреси, після чого отримує доступ до системи через скомпрометований обліковий запис. Інший сценарій може імітувати внутрішню загрозу, коли співробітник завантажує великий обсяг даних у неробочий час, що супроводжується передачею файлів на зовнішній сервер через незашифроване з’єднання. Третій сценарій може відтворювати атаку типу "відмова в обслуговуванні" (DoS), де мережа перевантажується підозрілим трафіком із кількох джерел. Кожен сценарій включає набір подій, їхню хронологію та очікувані результати, що дозволяє оцінити здатність SIEM-системи виявляти та класифікувати загрози.

На основі сценаріїв конфігуруються правила кореляції, які є основою аналітичного ядра SIEM-системи. Правила кореляції визначають логіку, що пов’язує кілька подій для ідентифікації потенційної загрози. Наприклад, правило для виявлення атаки методом підбору паролів може мати таку логіку: якщо протягом 10 хвилин із однієї IP-адреси зафіксовано п’ять або більше невдалих спроб входу (подія типу "failed_login") і подальший успішний вхід (подія типу "successful_login"), система генерує попередження з високим пріоритетом. Такі правила створюються з використанням мов запитів, наприклад, Splunk Processing Language (SPL) для Splunk або ArcSight Logger Query Language для ArcSight, які дозволяють задавати складні умови, включаючи часові рамки, порогові значення та фільтри за атрибутами подій (IP-адреса, ім’я користувача, тип події).

Сучасні SIEM-системи також використовують моделі машинного навчання для створення динамічних правил кореляції, які адаптуються до нових загроз без ручного втручання. Наприклад, алгоритми кластеризації можуть створювати базові профілі поведінки користувачів, порівнюючи поточну активність із цими профілями для виявлення аномалій, таких як незвичайний час доступу чи нетиповий обсяг переданих даних. Такі моделі особливо ефективні для виявлення складних атак, які не відповідають заздалегідь визначеним шаблонам, наприклад,

прихованих спроб експлуатації вразливостей або інсайдерських загроз.

Автоматизація реагування є важливим компонентом моделювання, оскільки вона скорочує час між виявленням загрози та її нейтралізацією. SIEM-системи інтегруються з інструментами оркестрації безпеки, такими як платформи SOAR, для виконання автоматизованих дій. Наприклад, при виявленні атаки методом підбору паролів SIEM може відправити команду брандмауеру для блокування IP-адреси через API (наприклад, REST API для Cisco Firepower). Інші дії можуть включати ізоляцію скомпрометованого пристрою шляхом зміни VLAN у мережевому комутаторі, відключення облікового запису через Active Directory або перенаправлення підозрілого трафіку на ізольовану мережу (honeypot) для аналізу. Автоматизація налаштовується з урахуванням пріоритетів попереджень: високопріоритетні загрози, такі як успішний несанкціонований доступ, обробляються негайно, тоді як низькопріоритетні, наприклад, поодинокі невдалі спроби входу, можуть позначатися для ручного аналізу.

Моделювання проводиться в тестовому середовищі, яке відтворює реальну IT-інфраструктуру організації. Це середовище включає віртуалізовані сервери, мережеві пристрої, хмарні компоненти та синтетичні логи, що імітують нормальну активність і події, пов’язані з інцидентами. Для генерації логів використовуються інструменти, такі як Splunk Attack Simulator, ELK Stack або власні скрипти, які створюють події з різними атрибутами (час, IP-адреса, тип події, користувач). Тестове середовище дозволяє оцінити продуктивність SIEM-системи, зокрема швидкість обробки даних, затримки в генерації попереджень і використання ресурсів (ЦП, оперативна пам’ять, дисковий простір). Наприклад, обробка 10 000 подій за секунду може бути тестовим показником для оцінки масштабованості системи в умовах великої організації.

Аналіз результатів моделювання зосереджений на оцінці ключових метрик ефективності SIEM-системи. До них належать:

- Відсоток виявлених загроз: частка змодельованих інцидентів, які система коректно ідентифікувала.

- Кількість помилкових спрацьовувань: відсоток попереджень, що не відповідають реальним загрозам, який необхідно мінімізувати.
- Час реагування: інтервал від моменту виникнення події до генерації попередження та виконання автоматизованої дії.
- Ефективність автоматизації: частка інцидентів, нейтралізованих без ручного втручання.
- Використання ресурсів: вплив системи на обчислювальні ресурси, що є важливим для хмарних або локальних розгортань.

Наприклад, якщо правило кореляції для атаки методом підбору паролів генерує 20% помилкових попереджень через легітимну активність, воно коригується шляхом додавання фільтрів, таких як виключення IP-адрес із білого списку. Аналіз також враховує продуктивність системи в умовах пікових навантажень, наприклад, при обробці 100 000 подій за секунду, що може бути типовим для великої організації.

Інтеграція SIEM-системи з іншими інструментами безпеки, такими як системи захисту від вторгнень, антивіруси чи сканери вразливостей, є необхідною для створення комплексного процесу реагування. Наприклад, інформація про нову вразливість із сканера Tenable Nessus може бути використана для створення правила кореляції, яке перевіряє логи на спроби її експлуатації. Інтеграція через API або протоколи, такі як REST або SOAP, забезпечує обмін даними в реальному часі, підвищуючи точність аналізу.

Документація відіграє ключову роль у моделюванні, фіксуючи сценарії інцидентів, правила кореляції, автоматизовані дії та процедури ручного реагування. Вона включає хронологію подій, джерела загроз, дії, виконані системою, і рекомендації для аналітиків. Наприклад, при виявленні складної атаки, такої як APT, документація може передбачати ескалацію до зовнішньої команди реагування на інциденти (CERT). Документація також використовується для навчання персоналу та створення звітів для відповідності нормативним вимогам.

Схема процесу реагування на інциденти за допомогою SIEM-системи представлена на рисунку 3.1.

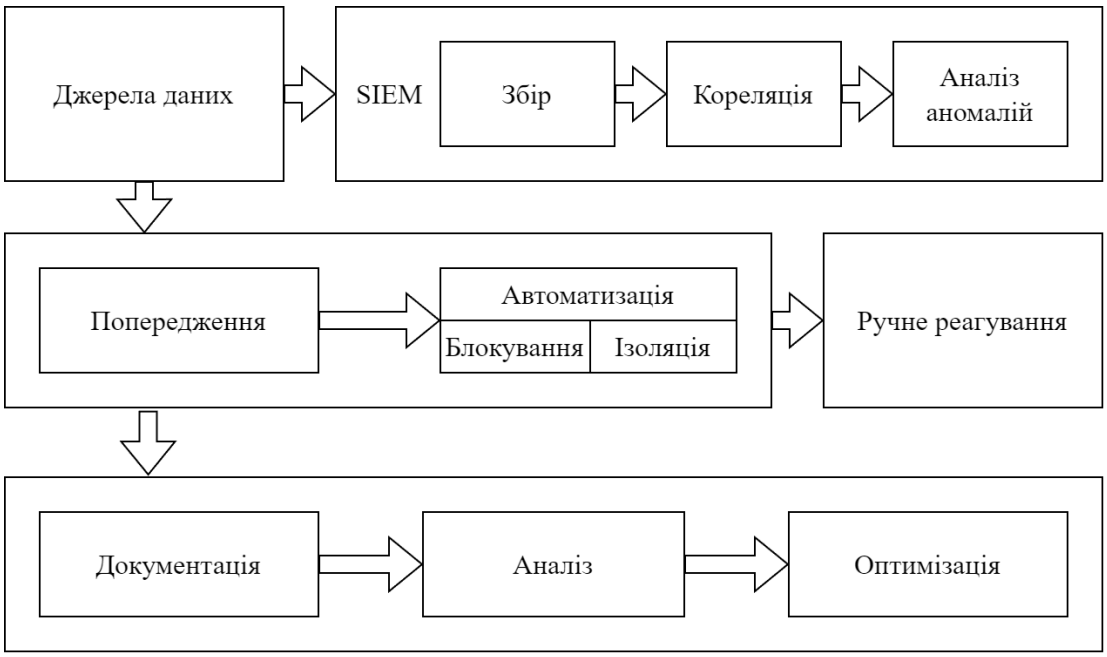

Рисунок 3.1 – Схема процесу реагування на інциденти за допомогою SIEM-системи

Ця схема ілюструє послідовність обробки подій від збору до реагування та подальшого аналізу для вдосконалення системи.

Для ілюстрації моделювання нижче наведено спрощений код на Python, який імітує обробку логів для виявлення атаки методом підбору паролів і генерацію попередження. Код використовує бібліотеку pandas для аналізу.

```
    import pandas as pd
    from datetime import datetime, timedelta
    # Імітація логів
    logs = [
        {"timestamp": "2025-05-03 10:00:00", "ip":
"192.168.1.10", "event": "failed_login"},
        {"timestamp": "2025-05-03 10:00:30", "ip":
"192.168.1.10", "event": "failed_login"},
        {"timestamp": "2025-05-03 10:01:00", "ip":
"192.168.1.10", "event": "failed_login"},
        {"timestamp": "2025-05-03 10:01:30", "ip":
"192.168.1.10", "event": "successful_login"}]
    # Створення DataFrame
    df = pd.DataFrame(logs)
    df["timestamp"] = pd.to_datetime(df["timestamp"])
    # Правило кореляції
    def detect_brute_force(df, threshold=3):
```

```
        alerts = []
        for ip in df["ip"].unique():
            ip_logs = df[df["ip"] == ip]
            failed_logins = ip_logs[ip_logs["event"] ==
"failed_login"].shape[0]
            if failed_logins >= threshold and
any(ip_logs["event"] == "successful_login"):
                alerts.append(f"Атака підбору пароля з IP
{ip}")
        return alerts
    # Виконання правила
    alerts = detect_brute_force(df)
    for alert in alerts:
        print(f"Попередження: {alert}")
```

Цей код демонструє базову логіку виявлення інциденту, яка може бути розширена для інтеграції з реальною SIEM-системою.

Моделювання процесів реагування на інциденти за допомогою SIEM-систем є комплексним підходом, який поєднує технічні, аналітичні та організаційні аспекти. Воно забезпечує підготовку до реальних загроз, оптимізує правила кореляції, автоматизує реакції та створює основу для ефективного управління кібербезпекою. Інтеграція з іншими системами, використання передових технологій, таких як машинне навчання, і чітка документація підвищують стійкість інформаційної інфраструктури до сучасних і майбутніх кіберзагроз, роблячи SIEM-системи незамінним інструментом у захисті організацій.

3.2 Оцінка ефективності SIEM-систем та методи їх удосконалення

Оцінка ефективності SIEM-систем є ключовим етапом їхньої експлуатації, який дозволяє визначити, наскільки система відповідає потребам організації в забезпеченні кібербезпеки, виявленні загроз і реагуванні на інциденти. Ефективність SIEM залежить від її здатності точно й оперативно виявляти загрози, мінімізувати помилкові спрацьовування, забезпечувати швидке реагування та оптимально використовувати ресурси інформаційної інфраструктури. У процесі оцінки аналізуються ключові метрики продуктивності, такі як відсоток виявлених інцидентів, час реакції, рівень автоматизації та вплив на обчислювальні ресурси.

На основі результатів оцінки розробляються методи удосконалення, які включають оптимізацію правил кореляції, інтеграцію з іншими системами безпеки, використання передових технологій і навчання персоналу. Ці заходи забезпечують адаптацію SIEM до нових загроз і підвищення її ефективності в умовах динамічного кіберсередовища.

Оцінка ефективності SIEM-систем проводиться шляхом аналізу їхньої роботи в контрольованих і реальних умовах. У контрольованих умовах використовуються тестові середовища, які імітують IT-інфраструктуру організації та генерують синтетичні логи для моделювання атак, таких як підбір паролів, несанкціонований доступ чи витік даних. У реальних умовах оцінка базується на аналізі фактичних подій безпеки, включаючи виявлені інциденти, попередження та дії, виконані системою. Для комплексної оцінки використовуються кількісні та якісні метрики, які дозволяють оцінити як технічні, так і організаційні аспекти роботи SIEM.

Кількісні метрики включають відсоток виявлених загроз, який показує, скільки змодельованих або реальних інцидентів система коректно ідентифікувала. Високий показник свідчить про точність правил кореляції та ефективність аналізу аномалій. Наприклад, якщо система виявляє 95% атак методом підбору паролів, але пропускає складні багатокрокові атаки, це вказує на потребу вдосконалення правил. Інша важлива метрика – кількість помилкових спрацьовувань, які створюють додаткове навантаження на аналітиків. Занадто високий рівень помилкових попереджень може бути спричинений надмірно чутливими правилами кореляції або недостатньою фільтрацією подій. Час реакції, що вимірює інтервал від моменту виникнення події до генерації попередження та виконання дії, є критично важливим для оцінки оперативності системи. Наприклад, реагування протягом 30 секунд на високопріоритетну загрозу вважається оптимальним для великих організацій. Використання ресурсів, включаючи навантаження на ЦП, оперативну пам’ять і дисковий простір, оцінюється для визначення масштабованості системи, особливо в умовах обробки великих обсягів даних.

Якісні метрики охоплюють зручність інтерфейсу, інтеграцію з іншими системами безпеки та рівень автоматизації. Наприклад, інтуїтивно зрозумілі дашборди дозволяють аналітикам швидко оцінювати ситуацію, тоді як інтеграція з брандмауерами чи антивірусами підвищує ефективність реагування. Автоматизація дій, таких як блокування IP-адрес чи ізоляція пристроїв, знижує залежність від ручного втручання, що є особливо важливим у разі масових атак.

Для наочності ключові метрики оцінки ефективності SIEM-систем представлені в таблиці 3.1.

Таблиця 3.1 – Основні метрики оцінки ефективності SIEM-систем

Метрика	Опис	Очікуваний результат
Відсоток виявлених загроз	Частка коректно ідентифікованих інцидентів	≥ 90%
Помилкові спрацьовування	Відсоток попереджень, що не відповідають реальним загрозам	≤ 10%
Час реакції	Час від виявлення події до виконання дії	≤ 30 секунд для високопріоритетних загроз
Використання ресурсів	Навантаження на ЦП, пам’ять, дисковий простір	≤ 70% від доступних ресурсів
Рівень автоматизації	Частка інцидентів, оброблених без ручного втручання	≥ 70% для типових загроз

Удосконалення SIEM-систем базується на результатах оцінки ефективності та спрямоване на підвищення точності виявлення, зниження помилкових спрацьовувань, оптимізацію продуктивності та адаптацію до нових загроз. Одним із основних методів є оптимізація правил кореляції. Це включає аналіз попереджень для виявлення причин помилкових спрацьовувань і коригування правил, наприклад, додавання фільтрів для виключення легітимної активності, такої як автоматичні оновлення програмного забезпечення. Для підвищення точності використовуються алгоритми машинного навчання, які створюють динамічні

моделі поведінки користувачів і пристроїв, дозволяючи виявляти аномалії, такі як незвичайний час доступу чи нетиповий обсяг переданих даних.

Інтеграція з іншими системами безпеки є ще одним важливим методом удосконалення. SIEM-системи можуть отримувати дані від сканерів вразливостей, антивірусів чи систем захисту від вторгнень, що дозволяє створювати більш точні правила кореляції. Наприклад, інформація про нову вразливість може бути зіставлена з логами для перевірки спроб її експлуатації. Інтеграція через API забезпечує обмін даними в реальному часі, підвищуючи ефективність реагування. Крім того, підключення до платформ оркестрації безпеки дозволяє автоматизувати складні сценарії реагування, такі як послідовне блокування IP-адреси, ізоляція пристрою та повідомлення адміністратора.

Використання передових технологій, зокрема машинного навчання та штучного інтелекту, значно розширює можливості SIEM-систем. Алгоритми кластеризації та класифікації дозволяють виявляти невідомі загрози, які не відповідають статичним правилам, наприклад, приховані атаки типу APT. Аналіз поведінки користувачів допомагає виявляти інсайдерські загрози, такі як несанкціоноване копіювання даних. Для оптимізації ресурсів складні обчислення, пов’язані з машинним навчанням, можуть виконуватися на хмарних серверах, залишаючи локальні компоненти для базового аналізу.

Навчання персоналу є критично важливим для вдосконалення SIEM-систем. Аналітики безпеки повинні бути підготовлені до роботи з дашбордами, аналізу попереджень і реагування на інциденти. Регулярні тренінги, які включають симуляцію атак, допомагають підвищити кваліфікацію персоналу та підготувати його до складних сценаріїв, таких як розслідування багатокрокових атак. Крім того, створення чітких процедур ескалації інцидентів, наприклад, залучення зовнішніх експертів для аналізу складних загроз, підвищує ефективність реагування.

Регулярне оновлення бази даних загроз і правил кореляції є необхідним для адаптації до нових кібератак. SIEM-системи можуть підключатися до глобальних джерел інформації про загрози, таких як бази даних MITRE ATT&CK або Threat

Intelligence Feeds, для отримання актуальних сигнатур і шаблонів атак. Це дозволяє своєчасно виявляти нові методи, такі як експлуатація нульових вразливостей.

Оптимізація продуктивності включає аналіз використання ресурсів і впровадження методів масштабування. Наприклад, розподіл обробки даних між кількома вузлами або використання хмарних ресурсів знижує навантаження на локальну інфраструктуру. Налаштування політики зберігання логів, наприклад, архівування старих даних на менш продуктивних сховищах, також сприяє економії ресурсів.

Для наочності методи удосконалення SIEM-систем представлені в таблиці 3.2.

Таблиця 3.2 – Методи удосконалення SIEM-систем

Метод удосконалення	Опис	Очікуваний ефект
Оптимізація правил кореляції	Коригування правил для зниження помилкових спрацьовувань	Зменшення помилкових попереджень до ≤ 5%
Інтеграція з іншими системами	Підключення до антивірусів, сканерів вразливостей, брандмауерів	Підвищення точності виявлення на 10–15%
Використання машинного навчання	Аналіз аномалій і створення динамічних правил	Виявлення ≥ 80% невідомих загроз
Навчання персоналу	Тренінги з аналізу попереджень і реагування на інциденти	Скорочення часу розслідування на 20%
Оновлення бази даних загроз	Інтеграція з джерелами інформації про нові загрози	Актуалізація правил протягом 24 годин
Оптимізація продуктивності	Розподіл обробки даних, використання хмарних ресурсів	Зниження навантаження на ресурси до 60%

На основі даних таблиці можна зробити висновок, що удосконалення SIEM-систем є багатогранним процесом, який охоплює технічні, аналітичні та організаційні методи, спрямовані на підвищення їхньої ефективності та

адаптивності до сучасних кіберзагроз. Оптимізація правил кореляції дозволяє знизити кількість помилкових спрацьовувань до рівня ≤ 5%, що значно підвищує точність виявлення інцидентів. Інтеграція SIEM-систем з іншими захисними інструментами, такими як антивіруси, сканери вразливостей і брандмауери, забезпечує зростання точності виявлення загроз на 10–15%, сприяючи комплексному захисту. Використання машинного навчання для аналізу аномалій і створення динамічних правил дає змогу виявляти ≥ 80% невідомих загроз, що є критично важливим в умовах зростання складності кібератак. Навчання персоналу скорочує час розслідування інцидентів на 20%, підвищуючи оперативність реагування. Оновлення бази даних загроз забезпечує актуалізацію правил протягом 24 годин, що дозволяє системі швидко адаптуватися до нових викликів. Нарешті, оптимізація продуктивності шляхом розподілу обробки даних і використання хмарних ресурсів знижує навантаження на ресурси до 60%, підвищуючи ефективність роботи системи. Загалом, застосування цих методів дозволяє значно підвищити ефективність SIEM-систем, забезпечуючи надійний захист підприємства від кіберзагроз і оптимізуючи процеси управління безпекою.

Оцінка ефективності SIEM-систем і методи їх удосконалення створюють основу для підвищення рівня кібербезпеки організації. Комплексний аналіз метрик дозволяє виявити слабкі місця системи, тоді як методи оптимізації, інтеграції та використання передових технологій забезпечують її адаптацію до нових загроз. Регулярне вдосконалення правил кореляції, навчання персоналу та оновлення бази даних загроз гарантують, що SIEM-система залишається ефективним інструментом для виявлення, реагування та запобігання інцидентам безпеки в динамічному кіберсередовищі.

Третій розділ дослідження зосереджений на моделюванні процесів реагування на інциденти та оцінці ефективності SIEM-систем, а також розробці методів їх удосконалення для забезпечення надійного захисту інформаційної інфраструктури організацій. Моделювання процесів реагування дозволило відтворити реальні сценарії кіберзагроз, таких як атаки методом підбору паролів, витік даних і внутрішні загрози, оцінивши здатність SIEM-систем виявляти

інциденти, генерувати попередження та виконувати автоматизовані дії, такі як блокування IP-адрес чи ізоляція пристроїв.

Використання правил кореляції, алгоритмів машинного навчання та інтеграція з інструментами оркестрації безпеки забезпечили точне виявлення як відомих, так і невідомих загроз, підкреслюючи важливість автоматизації для скорочення часу реагування. Оцінка ефективності SIEM-систем через аналіз метрик, таких як відсоток виявлених загроз, кількість помилкових спрацьовувань, час реакції та використання ресурсів, виявила сильні сторони системи та області для покращення, зокрема потребу в оптимізації правил кореляції та зниженні навантаження на інфраструктуру.

Методи удосконалення, включаючи коригування правил, інтеграцію з іншими системами безпеки, використання машинного навчання, навчання персоналу, оновлення бази даних загроз і оптимізацію продуктивності, створюють основу для адаптації SIEM до нових викликів кібербезпеки. Загалом, розділ демонструє, що ретельне моделювання, оцінка та постійне вдосконалення SIEM-систем є необхідними для забезпечення їхньої ефективності в захисті інформаційних систем.

ВИСНОВКИ

Дипломна робота, присвячена методиці застосування SIEM-систем в інформаційній системі організації, охопила теоретичні основи, практичні аспекти впровадження та моделювання процесів використання цих систем для забезпечення кібербезпеки. Проведене дослідження підкреслює важливість SIEM-систем як ключового інструменту для захисту інформаційної інфраструктури в умовах зростання складності кіберзагроз і розширення IT-екосистем організацій.

У першому розділі розглянуто теоретичні основи SIEM-систем, їхнє поняття, функції та архітектуру. Встановлено, що SIEM-системи забезпечують централізований збір, нормалізацію, кореляцію, аналіз і зберігання даних про події безпеки, дозволяючи виявляти загрози, реагувати на інциденти та відповідати нормативним вимогам. Архітектура, що включає модулі збору даних, кореляції, моніторингу та звітності, забезпечує гнучкість і масштабованість, а їхня роль у захисті інформаційних систем полягає у створенні повної видимості подій, точному виявленні загроз і швидкому реагуванні, що робить SIEM незамінним інструментом кібербезпеки.

Другий розділ зосереджений на практичних аспектах застосування SIEM-систем, зокрема етапах їхнього впровадження та налаштування для виявлення загроз. Впровадження охоплює аналіз потреб, вибір рішення, розгортання, інтеграцію, налаштування правил кореляції, тестування та навчання персоналу, що забезпечує ефективну інтеграцію системи в інформаційну інфраструктуру. Налаштування та оптимізація SIEM передбачають створення правил кореляції, моніторинг у реальному часі, автоматизацію реагування та зниження помилкових спрацьовувань, що підвищує точність виявлення атак і оптимізує ресурси. Практичні приклади реалізації збору логів і правил кореляції демонструють можливість адаптації SIEM до реальних умов.

Третій розділ присвячений моделюванню процесів реагування на інциденти та оцінці ефективності SIEM-систем. Моделювання дозволило відтворити сценарії кіберзагроз, оцінити здатність системи виявляти інциденти та виконувати

автоматизовані дії, такі як блокування IP-адрес чи ізоляція пристроїв. Оцінка ефективності через аналіз метрик, включаючи відсоток виявлених загроз, час реакції та використання ресурсів, виявила сильні сторони SIEM і необхідність оптимізації для зниження помилкових спрацьовувань. Методи удосконалення, такі як коригування правил кореляції, інтеграція з іншими системами безпеки, використання машинного навчання, навчання персоналу та оновлення бази даних загроз, забезпечують адаптацію SIEM до нових викликів кібербезпеки.

Загалом, дослідження продемонструвало, що SIEM-системи є комплексним рішенням для управління кібербезпекою, яке поєднує аналітичні, автоматизовані та організаційні аспекти. Їхнє успішне впровадження вимагає ретельного планування, налаштування та постійного вдосконалення для забезпечення точного виявлення загроз, швидкого реагування та відповід “‘’ності нормативним вимогам. Розроблена методика застосування SIEM-систем, підкріплена моделюванням і оцінкою ефективності, створює надійну основу для захисту інформаційних систем організацій від сучасних і майбутніх кіберзагроз. Подальші дослідження можуть бути спрямовані на вдосконалення алгоритмів машинного навчання для аналізу аномалій, розробку більш енергоефективних рішень для хмарних SIEM-систем і створення універсальних стандартів інтеграції для забезпечення глобальної сумісності.

ПЕРЕЛІК ПОСИЛАНЬ

1. Suarez-Tangil G., Palomar E., Ribagorda A., Sanz I. Providing SIEM systems with self-adaptation // *Information Fusion*. 2015. Vol. 21. P. 145–158.
2. Miloslavskaya N. Analysis of SIEM systems and their usage in security operations and security intelligence centers // Biologically Inspired Cognitive Architectures (BICA) for Young Scientists: Proceedings of the First International Early Research Career Enhancement School on BICA and Cybersecurity (FIERCES 2017) / *Springer International Publishing*, 2018. P. 282–288.
3. Menges F., Latzo T., Vielberth M., Sobola S., Pöhls H. C., Taubmann B., Pernul G. Towards GDPR-compliant data processing in modern SIEM systems // *Computers & Security*. 2021. Vol. 103. P. 102165. DOI: https://doi.org/10.1016/j.cose.2020.102165.
4. Sheeraz M., Paracha M. A., Haque M. U., Durad M. H., Mohsin S. M., Band S. S., Mosavi A. Effective security monitoring using efficient SIEM architecture // *Hum.-Centric Comput. Inf. Sci*. 2023. Vol. 13. P. 1–18.
5. Laue T., Klecker T., Kleiner C., Detken K. O. A SIEM architecture for advanced anomaly detection // *Open Journal of Big Data*. 2022. Vol. 6, No. 1. P. 26–42.
6. Gnatyuk S., Berdibayev R., Sydorenko V., Polozhentsev A., Ryabyy M. Enterprise Service Bus Construction in SOA Architecture for SIEM Implementation in Critical Information Infrastructure // *CPITS*. 2022. P. 11–20.
7. Montesino R., Fenz S., Baluja W. SIEM-based framework for security controls automation // *Information Management & Computer Security*. 2012. Vol. 20, No. 4. P. 248–263.
8. Tariq A., Manzoor J., Aziz M. A., Tariq Z. U. A., Masood A. Open source SIEM solutions for an enterprise // *Information & Computer Security*. 2022. Vol. 31, No. 1. P. 88–107.
9. Berdibayev R., Gnatyuk S., Yevchenko Y., Kishchenko V. A concept of the architecture and creation for SIEM system in critical infrastructure // Systems,

Decision and Control in Energy II / *Cham: Springer International Publishing*, 2021. P. 221–242.

10. Hase L., Wedel F. H. The Path to Choosing a SIEM System – A Systematic Literature Review // *Seminar IT-Management in the Digital Age* (Summer 2024). FH Wedel, Germany, 2024. P. 1–12.
11. Skendžić A., Kovačić B., Balon B. Management and monitoring security events in a business organization – SIEM system // 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO). *IEEE*, 2022. P. 1203–1208.
12. Areo G. Integrating Human Pose Estimation Concepts into SIEM for Advanced Cyber Threat Management. 2024. URL: https://www.researchgate.net/profile/Gideon-Areo/publication/386170916_Integrating_Human_Pose_Estimation_Concepts_into_SIEM_for_Advanced_Cyber_Threat_Management/links/6747224d790d154bf9aef261/Integrating-Human-Pose-Estimation-Concepts-into-SIEM-for-Advanced-Cyber-Threat-Management.pdf (дата звернення: 03.05.2025).
13. Ehis A. M. T. Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture // *Archives of Advanced Engineering Science*. 2023. P. 1–10.
14. Rosenberg M., Schneider B., Scherb C., Asprion P. EDO4SIEM – a procedure model for the implementation of security information and event management systems in organisations // *IADIS International Journal on Computer Science and Information Systems*. 2024. Vol. 19, No. 1. P. 31–47.
15. Splunk. *Офіційний сайт.* URL: https://www.splunk.com/ (дата звернення: 03.05.2025).
16. ArcSight Intelligence. *ERC Training center.* URL: https://edu.erc.ua/en/news/arcsight-intelligence/ (дата звернення: 03.05.2025).
17. IBM QRadar Suite. *IBM.* URL: https://www.ibm.com/qradar (дата звернення: 03.05.2025).
18. Zakharov A. A., Shabalin A. M., Kruchkovsky K. S. Features of Creating a Virtual Laboratory for Developing and Applying Correlation Rules in Modern SIEM-

Systems when Training Security Operation Center Analysts (by the Example of Microsoft Windows) // *SmartIndustryCon*. IEEE, 2024. P. 367–372.

19. Sebbar A., Cherqi O., Chougdali K., Boulmalf M. Real-Time Anomaly Detection in SDN Architecture Using Integrated SIEM and Machine Learning for Enhancing Network Security // *GLOBECOM 2023 – 2023 IEEE Global Communications Conference*. IEEE, 2023. P. 1795–1800.
20. Al-Dahasi E., Khan F. A. Automating Security Incident Response in SCADA Systems through SIEM-ML Integration // *2024 29th International Conference on Automation and Computing (ICAC)*. IEEE, 2024. P. 1–10.