МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: "**СИСТЕМИ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**"

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

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

_____ Юрій РУБАН

(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42
Юрій РУБАН
Ім'я, ПРІЗВИЩЕ

Керівник: Світлана ЛЕГОМІНОВА
Д.е.н., професор Ім'я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Д.т.н., професор Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рубан Юрій Романович

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Системи моніторингу та реагування на інциденти інформаційної безпеки”,
керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., професор,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *системи моніторингу, реагування, інцидент, інформаційна безпека, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити теоретичні аспекти інцидентів інформаційної безпеки та їх мониторингу;
4.2. Проаналізувати системи мониторингу інформаційної безпеки;
4.3. Сформувати рекомендації щодо практичного застосування систем мониторингу та реагування на інциденти.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “10“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	Виконано
2.	Збір та аналіз літератури.	29.03.2025	Виконано
3.	Дослідження теоретичних аспектів сутності інцидентів інформаційної безпеки та їх мониторингу	08.04.2025	Виконано
4.	Аналіз систем мониторингу інформаційної безпеки	15.04.2025	Виконано
5.	Формування рекомендацій щодо практичного застосування систем мониторингу та реагування на інциденти	22.04.2025	Виконано
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	Виконано
7.	Оформлення роботи.	06.05.2025	Виконано
8.	Оформлення презентації.	09.05.2025	Виконано
9.	Отримання рецензії на роботу.	__.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ Юрій РУБАН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Рубан Юрій Романович

до захисту кваліфікаційної роботи

за спеціальністю 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Системи моніторингу та реагування на інциденти інформаційної безпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач РУБАН Юрій у кваліфікаційній роботі дослідив теоретичні аспекти інцидентів інформаційної безпеки та їх мониторингу, визначив оптимальні систем мониторингу інформаційної безпеки, запропонував рекомендацій щодо практичного застосування систем мониторингу та реагування на інциденти. РУБАН Юрій показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявила себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача РУБАНА Юрія на оцінку "_____" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Рубан Ю. Р. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувач вищої освіти РУБАН Юрій
на тему “Системи моніторингу та реагування на інциденти інформаційної безпеки”

Актуальність. У сучасному цифровому середовищі зростає кількість і складність кіберінцидентів, які можуть загрожувати як безперервності бізнесу, так і безпеці критичної інфраструктури. Організації дедалі частіше стикаються з необхідністю вчасного виявлення загроз, реагування на них та зниження потенційних втрат. Застосування SIEM- і SOAR-технологій, побудова життєвого циклу інцидент-менеджменту відповідно до міжнародних стандартів (ISO/IEC 27001, NIST) стає не лише технічною, а й регуляторною необхідністю. У зв’язку з цим дослідження, присвячене аналізу та практичній реалізації систем моніторингу та реагування на інциденти інформаційної безпеки, є надзвичайно актуальним.

Позитивні сторони.

1. У роботі проаналізовано архітектуру сучасних SIEM/EDR/SOAR-рішень, нормативну базу, а також запропоновано практичні хмарні підходи для малого бізнесу.
2. Кваліфікаційна робота структурована згідно з академічними вимогами. Матеріал викладено логічно, з використанням схем і рисунків для ілюстрації ключових понять.
3. Автором опрацьовано значну кількість джерел, зокрема англомовні публікації, стандарти й технічну документацію.
4. Результати роботи мають прикладне значення, зокрема в частині вибору економічно доцільних хмарних рішень для побудови систем моніторингу безпеки.

Недоліки.

Доцільним було б розширити розділ з практичним тестуванням вибраних рішень у реальному або симульованому середовищі, зокрема з прикладами генерації інцидентів і сценаріями реагування.

Висновок: Кваліфікаційна робота виконана змітовно зі значними помилками та заслуговує оцінки “ _____ ”, а здобувач Рубан Юрій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР
д.т.н., професор *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню систем моніторингу та реагуванню на інциденти інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 4 рисунки, висновківі списку використаних джерел із 46 найменувань. Загальний обсяг роботи становить 56 аркушів, з яких 5 аркуші займає список використаних джерел.

Метою роботи полягає у дослідженні ефективної системи моніторингу та реагування на інциденти інформаційної безпеки організацій .

Об'єктом дослідження процес систематизації моніторингу та реагування на інциденти інформаційної безпеки

Предмет дослідження **–** особливості систем моніторингу та реагування на інциденти інформаційної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі застосовано методи системного аналізу, порівняння, моделювання, експертного оцінювання, логічного узагальнення.

Як результат, у роботі проаналізовано сучасні підходи до моніторингу подій інформаційної безпеки, досліджено архітектуру та функціональні можливості систем типу SIEM і SOAR, життєвий цикл реагування на інциденти згідно з міжнародними стандартами, проведено порівняльний аналіз провідних платформ моніторингу, а також розроблено практичні рекомендації щодо впровадження та тестування таких систем.

Галузь застосування. Використання запропонованої системи моніторингу та реагування дозволяє своєчасно виявляти інциденти, знижувати ймовірність порушення конфіденційності, цілісності та доступності інформації, а також оптимізувати процеси реагування в організаціях різного масштабу.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНЦИДЕНТ, SIEM, SOAR, МОНІТОРИНГ, РЕАГУВАННЯ, ISO/IEC 27001, NIST, КІБЕРЗАГРОЗА, АНАЛІТИКА ПОДІЙ, СИСТЕМИ МОНІТОРИНГУ БЕПЕКИ.

ABSTRACT

The qualification thesis is dedicated to the study of monitoring and incident response systems in the field of information security. The paper consists of an introduction, three chapters including 4 figures, conclusions, and a list of 46 references. The total volume of the work is 56 pages, 5 of which are occupied by the list of abbreviations and references.

The purpose of the study is to investigate and analyze the effectiveness of a system for monitoring and responding to information security incidents.

The object of the study is the process of ensuring information security in organizational information systems.

The subject of the study includes technologies, tools, and methods for monitoring and responding to information security incidents.

***Research methods*.** To address the above scientific objective, the work employs methods of systems analysis, comparison, modeling, expert evaluation, and logical generalization.

As a result, the paper analyzed modern approaches to monitoring information security events, investigated the architecture and functionality of SIEM and SOAR systems, the incident response lifecycle according to international standards, conducted a comparative analysis of leading monitoring platforms, and developed practical recommendations for implementing and testing such systems.

Field of application. The use of the proposed monitoring and response system enables timely detection of incidents, reduces the likelihood of breaches of confidentiality, integrity, and availability of information, and optimizes response processes across organizations of different scales.

Keywords: INFORMATION SECURITY, INCIDENT, SIEM, SOAR, MONITORING, RESPONSE, ISO/IEC 27001, NIST, CYBER THREAT, EVENT ANALYTICS, SECURITY MONITORING SYSTEMS.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах зростаючої цифровізації та розповсюдження хмарних технологій загрози інформаційній безпеці стають дедалі складнішими та поширеними. Інцидент безпеки – будь-яка подія, що ставить під загрозу цілісність, конфіденційність чи доступність інформації – може варіюватися від несанкціонованого доступу до витоку даних чи DoS-атаки. Ефективне виявлення та реагування на такі інциденти є критично важливим для забезпечення безпеки організацій. Сучасні рішення SIEM надають централізований збір і аналіз журналів подій, допомагаючи організаціям «виявляти, аналізувати й усувати загрози безпеці» до того, як вони завдадуть шкоди. Технології SOAR автоматизують реагування на інциденти й управління ними, що дозволяє командам безпеки швидше обробляти загрози та підвищувати ефективність операцій. Крім того, законодавчі та нормативні вимоги стимулюють розвиток систем моніторингу. Наприклад, міжнародні стандарти ISO/IEC 27001 та NIST CSF визначають рамки для побудови процедур обробки інцидентів, а GDPR вимагає повідомлення про витоки персональних даних протягом 72 годин після виявлення. В Україні Закон «Про основні засади забезпечення кібербезпеки»[2] встановлює обов'язкові заходи захисту критичної інформаційної інфраструктури. Таким чином, дсолідження на тему систем моніторингу та реагування на інциденти є актуальною задачею.

Метою роботи полягає у дослідженні ефективної системи моніторингу та реагування на інциденти інформаційної безпеки організацій .

Об'єктом дослідження процес систематизації моніторингу та реагування на інциденти інформаційної безпеки

Предмет дослідження – особливості систем моніторингу та реагування на інциденти інформаційної безпеки.

Методи дослідження. У роботі застосовано методи системного аналізу, порівняння, моделювання, експертного оцінювання, логічного узагальнення.

Практичне значення одержаних результатів. Використання запропонованої системи моніторингу та реагування дозволяє своєчасно виявляти інциденти, знижувати ймовірність порушення конфіденційності, цілісності та доступності інформації, а також оптимізувати процеси реагування в організаціях різного масштабу.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття та класифікація інцидентів інформаційної безпеки

Інцидент інформаційної безпеки — це подія або серія пов’язаних подій, що становлять реальну, або потенційну загрозу конфіденційності, цілісності, доступності інформації та/або IT-інфраструктури організації. Відповідно до стандарту ISO/IEC 27035, інцидент безпеки — це «одна, або кілька небажаних - неочікуваних подій, які можуть мати суттєвий вплив на діяльність організації та інформаційну безпеку»[26].

Класифікація інцидентів базується на кількох ключових критеріях: за походженням (внутрішні чи зовнішні), за характером (технічні, організаційні, природні), за рівнем шкоди (низький, середній, високий), а також за вектором атак чи причиною виникнення. Так, стандарт ISO/IEC 27035-2 наводить такі приклади категорій: природні катастрофи, відмови інфраструктури, технічні атаки, інциденти, пов’язані з людським фактором, і правові чи регуляторні порушення[27]. NIST SP 800-61 поділяє інциденти за поширеними векторами атак, зокрема зловмисне програмне забезпечення, несанкціонований доступ, атаки відмови в обслуговуванні, порушення політик та соціальна інженерія[33].

Вторинним критерієм класифікації є рівень наслідків: від випадків, які потребують лише моніторингу й реєстрації, до тих, що викликають суттєві фінансові збитки, репутаційні втрати або порушення безперервності бізнес-процесів. У цьому контексті ENISA у своїй таксономії пропонує розрізняти інциденти за ступенем впливу на конфіденційність, цілісність і доступність та за необхідністю залучення різних рівнів реагування CSIRT чи правоохоронних органів.

Класифікація за складністю та чисельністю подій передбачає поділ на одиночні (simple), складні (complex) та масштабні (mass incidents). Одиничні інциденти охоплюють одну точку уразливості або один тип атак, складні включають декілька векторів загроз або одночасні атаки, а масштабні — це системні або масовані дії, наприклад глобальні DDoS-атаки чи великі витоки даних.

Важливо також виокремлювати інциденти за джерелом виникнення: випадкові (наприклад, помилки користувачів або збої обладнання), навмисні (сплановані кібератаки, внутрішні зловмисники) та змішані, коли технічна помилка сприяє експлуатації вразливості третіми особами. У разі навмисних атак, як правило, застосовується додаткова класифікація за мотивацією зловмисників: фінансова вигода, корпоративний шпіонаж, хактивізм або державні кіберакції[11].

Підхід ISO/IEC 27035-1 акцентує увагу на процесному аспекті — інциденти слід розглядати у контексті життєвого циклу реагування, де класифікація є першим кроком для коректного призначення пріоритетів і ресурсів. Класифікація також полегшує автоматизацію процесів моніторингу та кореляції подій у SIEM- та UEBA-системах, спрямованих на швидке виявлення аномалій та вчасне реагування[27].

1.2. Шляхи реалізації загроз

Загрози інформаційній безпеці можуть реалізовуватися через канали зв’язку та програмні засоби. У табл. 1.1 [1] подано узагальнену класифікацію поширених загроз, що впливають на різні компоненти інформаційних систем. Вона ілюструє типові способи реалізації таких загроз, однак для повного аналізу слід враховувати конкретні умови й особливості середовища.

Таблиця 1.1

Основні вектори реалізації загроз інформаційній безпеці

Об'єкти впливу	**Порушення конфіденційності інформації**	**Порушення цілісності інформації**	**Порушення працездатності системи**
Апаратні засоби	Несанкціонований доступ – підключення; використання ресурсів; викрадення носіїв	Несанкціонований доступ – підключення; використання ресурсів; модифікація, зміна режимів	Несанкціонований доступ – зміна режимів; виведення з ладу; пошкодження
Програмне забезпечення	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – впровадження „троянів", „вірусів", „хробаків"	Несанкціонований доступ – спотворення; знищення; підміна
Дані	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – спотворення; модифікація	Несанкціонований доступ – спотворення; знищення; підміна
Персонал	Розголошення; передача відомостей про захист; халатність	Вербування; підкуп персоналу	Покидання робочого місця; фізичне усунення

Узагальнення аналізу шляхів реалізації загроз показує, що сучасні атаки поєднують технічні, фізичні й соціальні компоненти, використовуючи широкий спектр каналів та інструментів. По-перше, фізичні методи — від крадіжки носіїв та апаратних втручань у серверні приміщення до несанкціонованого доступу до робочих станцій — залишаються дієвими, особливо в поєднанні з внутрішньою загрозою через недбалість або зловмисні дії співробітників. По-друге, мережеві вектори, такі як DDoS-атаки, перехоплення трафіку та інжекційні атаки (SQL, LDAP, XSS), дозволяють порушувати конфіденційність, цілісність і доступність систем; при цьому ін'єкції залишаються однією з найпоширеніших уразливостей. Третій канал — софтверні методи — охоплює впровадження шкідливого ПЗ, від троянів до ransomware, а також використання вразливостей у сторонньому ПЗ і компонентах. Не забуваємо і про соціальні техніки соціальної інженерії, зокрема фішинг, вішинг та BEC—атаки, не

вимагають складних технічних знань і часто стають початковою точкою складних многоетапних атак.

1.3. Принципи та концепції моніторингу інформаційної безпеки

Принципи моніторингу інформаційної безпеки базуються на поєднанні стратегічних концепцій управління ризиками, безперервного циклу вдосконалення і чітких вимог стандартів та нормативних документів. Головним є виявлення, оцінка й обробка подій безпеки в режимі реального часу або майже реального часу з метою підтримки прийняття рішень щодо захисту активів організації. Усі підходи підкреслюють важливість інтеграції моніторингу в загальну систему управління інформаційною безпекою, використання автоматизованих інструментів для збору та аналізу телеметрії, а також регулярного перегляду політик і технічних засобів на основі отриманих даних.

Моніторинг розглядається як безперервний процес збору, кореляції та аналізу даних про події безпеки з різних джерел. Поняття «Information Security Continuous Monitoring» (ISCM) від NIST вбачає у цьому циклі п’ять ключових кроків – підготовка, збір даних, обробка, аналіз результатів та реагування – що відображаються у SP 800-137. У ISO/IEC 27001:2022 моніторинг входить до елементів циклу «Plan–Do–Check–Act» (PDCA), де контроль і аналіз виконання політик інформаційної безпеки дають зворотний зв’язок для удосконалення системи управління інформаційною безпекою [22].

Ключова концепція – ризик-орієнтований підхід: моніторингові заходи мають фокусуватися на тих активах та загрозах, які здатні завдати найбільшої шкоди організації. Це вимагає попередньої оцінки ризиків та встановлення чітких метрик (KRI, KPI) для вимірювання ефективності контролів.

1.4. Нормативні вимоги та звітність у системах моніторингу та реагування на інциденти

У сучасних інформаційних системах забезпечення безпеки вимагає не лише технічних заходів, але й чіткої відповідності широкому спектру нормативних актів і стандартів. До них належать українське законодавство (наприклад, Закон України «Про основні засади забезпечення кібербезпеки», підзаконні акти КМУ, нормативи Національного координаційного центру кібербезпеки, українські версії міжнародних стандартів)[2] та міжнародні вимоги – ISO/IEC 27001, ISO/IEC 27035, NIST SP 800-61, GDPR, PCI DSS, CIS Controls. Ці документи визначають обов'язкові практики з журналювання подій, контролю доступу, управління інцидентами та збереження даних. Сучасні SIEM/SOAR-системи (Security Information and Event Management / Security Orchestration, Automation and Response) безпосередньо підтримують реалізацію таких вимог: вони централізовано збирають і зберігають журнали подій, корелюють і аналізують сигнали, автоматизують реагування на події та формують звіти для аудиту. Зокрема, у міжнародному стандарті ISO/IEC 27001:2022 (Annex A.8.15) підкреслено, що «журнали подій… повинні створюватися, зберігатися і регулярно аналізуватися для виявлення інцидентів безпеки»[22]. Відповідно, впровадження SIEM/SOAR істотно полегшує виконання таких вимог.

1. Українські нормативні вимоги

В Україні ключовим актом є Закон №2163-VIII «Про основні засади забезпечення кібербезпеки», який створює загальну правову основу. Організаціям, що оперують державними інформаційними ресурсами, накладаються жорсткі обов'язки щодо моніторингу та реагування[2]. Наприклад, постановою КМУ №447 від 28.03.2025 у правила захисту інформації додано пункти, які вимагають від власників держсистем

невідкладно виявляти й усувати кіберінциденти та повідомляти про них Державний центр кіберзахисту (CERT-UA/НКЦК) [4]. Згідно з цими змінами, «власники (розпорядники) систем… здійснюють виявлення кіберінцидентів і реагування на них, усунення їх наслідків» та «невідкладно інформують CERT-UA… про інциденти кібербезпеки від середнього рівня критичності й вище». Окрім того, у тому ж документі регламентовано, що для моніторингу безпеки мають використовуватися «системи виявлення, запобігання та нейтралізації кіберзагроз, за допомогою яких здійснюються збір та аналіз мережевої телеметрії, а також реагування на кіберінциденти та кібератаки» [4]. Інакше кажучи, державні вимоги прямо передбачають використання інструментів типу SIEM/IDS для збору логів та автоматизованого аналізу мережевих подій.

2 Міжнародні стандарти та вимоги

ISO/IEC 27001 – міжнародний стандарт побудови системи управління інформаційною безпекою. Він встановлює загальні принципи управління ризиками і безпекою. У своєму додатку А містить контролі з журналювання та моніторингу (п. A.12.4 в ISO/IEC 27001:2013, еквівалент п.8.15 в ISO/IEC 27001:2022) і з управління інцидентами (A.16.1). Згідно зі стандартом, організація повинна «реєструвати журнали подій» та періодично їх переглядати; також необхідно мати формалізовану процедуру для повідомлення про інциденти та реагування на них.

ISO/IEC 27035 – стандартизація процесу управління інцидентами безпеки. ISO 27035 описує повний цикл: оцінка подій (Event Management), класифікація, реагування, відновлення, а також навчання на уроках інцидентів. Іншими словами, він деталізує фази підготовки, виявлення, реагування та розслідування, узгоджуючись із кращими практиками (частково суміщається з життєвим циклом, запропонованим NIST).

NIST SP 800-61 – гайд від Національного інституту стандартів США з організації роботи з інцидентами. Він поділяє процес реагування на чотири етапи: підготовка; виявлення та аналіз; локалізація і усунення; відновлення; та

подальші поліпшення (lessons learned). NIST наголошує на необхідності безперервного моніторингу і аналізу подій з використанням різноманітних інструментів. Зокрема, в ньому рекомендується застосовувати «різноманітні засоби, такі як SIEM-системи, IDS та антивірусне ПЗ, для постійного моніторингу та аналізу мережевої активності і сигналів»[11]. Це відповідає ідеї сучасних SIEM, які збирають логи та генерують алерти в режимі 24/7.

GDPR (General Data Protection Regulation) – регламент ЄС про захист персональних даних. Стаття 32 GDPR вимагає впровадити «адекватні технічні та організаційні заходи» для захисту даних, зокрема псевдонімізацію й шифрування ПД; забезпечення конфіденційності, цілісності та доступності систем обробки. GDPR також встановлює жорстку процедуру повідомлення про злом: порушення безпеки ПД має бути задокументовано й повідомлено наглядовому органу протягом 72 годин. Хоча сам стандарт прямо не диктує технологій журналювання, його вимоги до швидкого виявлення порушень стимулюють використання SIEM для аудиту доступів та інцидент-менеджменту[26].

PCI DSS (Payment Card Industry Data Security Standard) – стандарт безпеки для карткових платіжних систем. Його Requirement 10 прямо зобов’язує «записувати і переглядати всі доступи до ресурсів та даних карток»[35]. Логи мають зберігатися не менше року (а оптимально – 3 роки). PCI DSS також вимагає унікальних облікових записів і контролю доступу (Req.7–8), а у Requirement 12 – наявності плану реагування на інциденти та регулярного тестування. Таким чином, SIEM відповідає ключовим пунктам PCI DSS: централізація логів, їх перегляд, зберігання та швидке сповіщення про підозрілі події.

CIS Controls – набор пріоритетних практик інфобезпеки. Серед 18 контролів особливо важливі: *Control 8: Audit Log Management* – «збирати, сповіщати, аналізувати та зберігати журнали, що можуть допомогти виявити, зрозуміти чи відновитися після атаки» [14]; *Control 17: Incident Response*

Management – встановлює політику IP, включно з процесом звітування про інциденти (17.3) та процедуру реагування з прописаними ролями й каналами зв'язку (17.4) [13]. CIS Controls фактично консолідують вимоги ISO, NIST і інших стандартів у вигляді конкретних рекомендацій щодо логів та IP.

3. Роль SIEM/SOAR у забезпеченні відповідності

- Журналювання та моніторинг:

SIEM-системи централізують збір логів з усіх критичних компонентів (серверів, мережі, програм). Вони зберігають і корелюють ці події, що дозволяє виконати вимоги ISO 27001 (Annex A.12 – зберігання й аналіз журналів) і PCI DSS (Requirement 10 – логування користувацьких дій і зберігання логів не менше року) [35]. Крім того, автоматична кореляція подій у SIEM відповідає CIS Control 8, яка передбачає аналіз журналів для виявлення атак. Завдяки цьому організація отримує швидку інформацію про аномалії в режимі реального часу, «відтворюючи» події інциденту при необхідності.

- Контроль доступу:

SIEM відслідковує спроби входу, використання облікових записів та привілеїв. Всі події авторизації фіксуються в логах, що необхідно для звітування (як того вимагає ISO/IEC 27001). Отримані дані дозволяють виявляти несанкціоновані дії чи порушення привілеїв. Більше того, SIEM може інтегруватись з рішеннями управління доступом (MFA, RBAC), збираючи від них відомості. Це допомагає виконати заходи GDPR, зокрема п.32 щодо псевдонімізації та шифрування, – оскільки SIEM-фільтри можуть приховувати ПД у логах, залишаючи тільки технічну інформацію.

- Управління інцидентами:

SOAR-платформи доповнюють SIEM, автоматизуючи життєвий цикл реагування. Інформація із SIEM (кореляція сигналів, згенеровані алерти) служить тригером для SOAR, який виконує прописані кроки реагування: наприклад, ізоляцію уражених вузлів, сповіщення відповідальних осіб, оновлення статусу інциденту тощо. Такий підхід відповідає методологіям ISO

27001 (Annex A.16) та NIST 800-61 (контейнмент, усунення, відновлення), де важлива швидкість і скоординованість дій. NIST прямо рекомендує використовувати SIEM та інші системи моніторингу для виявлення інцидентів, а SOAR гарантує, що процедура реагування відпрацьовується послідовно і з докладним журналом дій [11].

- Зберігання даних:

SIEM-сховище сконфігуроване відповідно до політик довгострокового зберігання: логи резервуються, а при необхідності – шифруються. Це забезпечує відповідність ISO 27001 (захист та цілісність даних) і GDPR (конфіденційність/доступність за ст.32). SIEM також дозволяє анонімізувати або псевдонімізувати персональні дані у звітах, що є частиною «протоколів аудиту» для GDPR. В цілому, завдяки SIEM організація дотримує регламентованих строків збереження логів і може відновити всі події за потреби (вимога PCI DSS до ретенції логів виконана).

- Автоматизована звітність та аудит:

SIEM/SOAR спрощують підготовку аудиторських звітів. Системи містять шаблони для стандартних звітів (відповідності регламентам), які формуються на основі зібраних логів та виконаних дій. Наприклад, за рахунок модулів комплаєнсу, IBM QRadar «автоматично формує звіти відповідності» різним стандартам (GDPR, ISO 27001, PCI DSS тощо). Це суттєво знижує навантаження при перевірках і робить систему готовою до аудиту: можна швидко показати підтвердження наявності журналів, процедур IP та результатів моніторингу, що є вимогами як НКЦК і законодавства, так і міжнародних стандартів.

SIEM і SOAR-системи є ключовими інструментами для забезпечення комплаєнсу з українськими та міжнародними вимогами кібербезпеки. Вони автоматизують журналювання, контроль доступу, реагування на інциденти й звітність, що дозволяє організаціям легше виконувати норми Законів, постанов КМУ, стандартів ISO/IEC, NIST, GDPR, PCI DSS, CIS Controls тощо. Таким

чином, впровадження SIEM/SOAR суттєво підвищує готовність організації до перевірок та аудиту з кібербезпеки.

1.5 Життєвий цикл реагування на інциденти

Моніторинг та реагування на інциденти базується на чітко визначеному життєвому циклі, який дозволяє організаціям системно підходити до підготовки, виявлення, стримування, усунення та аналізу подій безпеки.

Цикл починається з етапу підготовки, коли формується команда реагування, розробляється політика інцидент-менеджменту, визначаються ролі, обов’язки та необхідні технічні й організаційні ресурси для забезпечення готовності до подій[16]. На цьому етапі також встановлюються засоби збору та зберігання логів, налаштовуються інструменти для превентивного моніторингу та створюються процедури регулярного навчання й тренувань персоналу, що дозволяє знизити ймовірність і масштаб потенційних інцидентів.

Другий етап — виявлення й аналіз — передбачає постійний збір телеметрії з мережевих пристроїв, серверів і робочих станцій, своєчасне корелювання подій і застосування аналітичних моделей для ідентифікації аномальної поведінки, після чого команда проводить детальний аналіз для підтвердження наявності інциденту та оцінки його потенційного впливу.

Далі етап стримування та ліквідації має на меті мінімізувати збитки й зупинити розповсюдження загрози: до стандартних заходів належать ізоляція вражених систем, блокування мережевого трафіку, припинення шкідливих процесів та застосування тимчасових контрзаходів для обмеження доступу зловмисника до ресурсів.

Одночасно з цим відбувається ліквідація первинних причин (наприклад, видалення шкідливого ПЗ, закриття вразливостей конфігурації) та відновлення

працездатності систем шляхом відкату до чистих бекапів або повторної інсталяції компонентів.

П’ятий етап — відновлення — включає відновлення бізнес-процесів і перевірку цілісності даних, а також повернення систем до нормального функціонування з урахуванням рекомендацій щодо посилення безпеки, отриманих під час реагування Центр ресурсів комп'ютерної безпеки.

Заключний етап післяінцидентної активності (lessons learned) передбачає детальний розбір інциденту, документування хронології подій, оцінку ефективності застосованих заходів і оновлення процедур, політик й інструментів моніторингу на основі отриманих уроків для підвищення стійкості до майбутніх загроз EC-Council. Важливо, що результати цього етапу повертаються на фазу підготовки, створюючи замкнений цикл безперервного вдосконалення, який визнається як в NIST SP 800-61, так і в ISO/IEC 27035-1[26].

Важливу роль у підвищенні ефективності циклу реагування відіграє автоматизація рутинних завдань, що дозволяє не лише скоротити середній час виявлення (MTTD) та середній час реагування (MTTR), а й зменшити навантаження на команду безпеки за рахунок автоматичного блокування підозрілих IP-адрес, ізоляції інфікованих вузлів та запуску попередньо налаштованих сценаріїв розслідування. Автоматизовані платформи SOAR інтегрують різноманітні джерела телеметрії та інструменти безпеки, що надає єдиний інтерфейс для кореляції подій, виконання playbook-ів та моніторингу виконання контрзаходів в режимі реального часу [12]. Застосування штучного інтелекту і машинного навчання для виявлення аномалій покращує точність детекції нетипової поведінки користувачів і пристроїв, що дозволяє знизити кількість хибнопозитивних сповіщень і зосередити увагу аналітиків на реально критичних загрозах.

Інтеграція моніторингу у загальну стратегію управління ризиками (IRM) забезпечує цілісне бачення ризикового профілю організації та дає змогу

оперативно коригувати рівень контролів згідно з динамікою загроз. Безперервний збір даних про події та їх аналіз у контексті бізнес-процесів формує основу проактивного підходу, коли ризики не лише виявляються, а й послідовно оцінюються та обробляються відповідно до стратегії організації. Одночасно широке коло зацікавлених сторін, зокрема IT-відділи, керівники напрямків та аудитори, отримують доступ до єдиних показників безпеки, що сприяє прозорості прийняття рішень та виявленню «слабких ланок» у процесах[41].

Впровадження автоматизованих інформаційних потоків прискорює розповсюдження даних про інциденти між командами та зовнішніми партнерами, забезпечуючи стандартизовані формати обміну та мінімізуючи людський фактор у критичних точках процесу. Проте створення ефективної автоматизації стикається з низкою викликів: від браку кваліфікованих фахівців, здатних налаштувати складні робочі процеси, до високих початкових витрат на інтеграцію та необхідності підтримувати актуальність правил і моделей у швидкозмінному ландшафті загроз. Окрім цього, забезпечення безперервного зберігання, шифрування та захисту журналів подій є критично важливим для проведення атестацій, аудиту та ретроспективного аналізу інцидентів у відповідності до вимог ISO/IEC 27001 і NIST [6].

Завершальною складовою життєвого циклу реагування, як зазначалося вище, є етап післяінцидентного аналізу, під час якого відбувається детальне документування хронології подій, оцінка ефективності застосованих заходів і формування рекомендацій щодо оновлення процесів, політик та технічних рішень. Саме результати цього етапу лягають в основу планування наступних тренувань, оновлення playbook-ів і доопрацювання архітектури моніторингу, що створює безперервний цикл вдосконалення та забезпечує стійкість організації до еволюції кіберзагроз.

Висновки до розділу 1

Узагальнюючи викладене в першому розділі, можна констатувати, що розуміння інцидентів інформаційної безпеки, їх джерел та механізмів реалізації створює міцну основу для побудови систем захисту. Класифікація інцидентів дає змогу орієнтуватися в різноманітті загроз, а детальний аналіз шляхів їхньої реалізації сприяє точному визначенню вразливих місць інфраструктури. Зі свого боку, міжнародні стандарти формують єдині вимоги до оцінки ризиків, контролів і процесів реагування, а опис життєвого циклу інциденту демонструє необхідність постійного циклу вдосконалення та тісної взаємодії людей і технологій. Загалом, узгоджені теоретичні підходи дозволяють організаціям ефективно моніторити, аналізувати та реагувати на інциденти, зменшуючи імовірність порушень безпеки та мінімізуючи потенційні втрати.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНИХ СИСТЕМ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ

2.1. Класифікація та архітектура SIEM-систем

Системи Security Information and Event Management (SIEM) поєднують підходи Security Information Management (SIM) та Security Event Management (SEM), створюючи єдине рішення для збору, кореляції та аналізу подій безпеки з множини джерел у реальному часі. SIEMсистеми розрізняються за класифікацією на основі способу розгортання, типу збору даних та архітектурної моделі, що дозволяє організаціям обирати оптимальний баланс продуктивності, маштабованості та вартості впровадження.

За моделлю розгортання SIEM-системи поділяються на локальні (on-premises), хмарні (cloud-based) та гібридні рішення. On-premises SIEM забезпечують повний контроль над інфраструктурою та даними, але вимагають значних капітальних витрат на обладнання та підтримку. Cloud-based SIEM-платформи знижують капітальні витрати завдяки модель “Pay-as-you-go” та забезпечують автоматичне масштабування, проте можуть викликати побоювання щодо конфіденційності даних і відповідності регуляторним вимогам [46]. Гібридні варіанти дозволяють комбінувати переваги обох підходів, розміщуючи критичні компоненти on-premises, а аналітичні та зберігаючі сервіси — у хмарі.

SIEM-системи також класифікують за способом збору логів та подій: агентні, безагентні та комбіновані. Агентні вирішення встановлюють програмні агенти на кінцевих пристроях, які виконують попередню фільтрацію й нормалізацію подій перед відправленням на центральний колектор. Безагентні системи, навпаки, переважно використовують протоколи Syslog або NetFlow для пасивного збирання логів без встановлення додаткового ПЗ на вузлах.

Комбіновані моделі забезпечують гнучкість: вразливі до навантаження сервери обробляють дані агентно, а менш критичні ендпоінти віддають перевагу безагентному збору [31].

Архітектура SIEM спроектована як комплексна система, що складається з кількох взаємопов'язаних модулів, кожен із яких виконує свою роль у забезпеченні безперервного моніторингу й обробки кіберінцидентів. Для того, щоби створити або вдосконалити рішення SIEM, необхідно чітко розуміти функції кожного з цих елементів. Нижче наведено основні компоненти, які мають входити до сучасної системи SIEM.

1. Збір та консолідація журналів
Першочерговим завданням будь-якої SIEM-платформи є прийом і зберігання логів з усіх джерел: мережевих елементів (фаєрволи, маршрутизатори), серверів, кінцевих пристроїв та прикладних сервісів, зокрема хмарних. Потужні системи здатні приймати і агрегувати тисячі подій у реальному часі. Це забезпечує повне охоплення IT-ландшафту організації й дозволяє фіксувати навіть найменші сліди потенційних атак.

2. Нормалізація та розбір записів
Після отримання логів із різноманітних систем приходить черга уніфікації даних. Нормалізація перетворює всю інформацію до єдиного формату, а парсинг розбиває її на структуровані поля.
Такий підхід значно спрощує подальшу обробку й аналіз, адже система отримує вже стандартизовані записи, готові для порівняння та кореляції.

3. Кореляційний механизм
У серці SIEM розташований двигун кореляції — аналітична система, яка шукає міжподієві зв'язки й виявляє підозрілі патерни. Наприклад, серія невдалих спроб входу з різних робочих точок за короткий відрізок часу може свідчити про брутфорс-атаку.
Сучасні платформи комбінують класичні правила з методами машинного

навчання та зовнішніми даними про загрози, щоб точніше й швидше виявляти аномалії.

4. Система сповіщень і формування звітів
Коли кореляційний движок фіксує потенційно небезпечну подію, SIEM негайно генерує алерт, який надсилається команді безпеки для подальшого розслідування. Деколи такі повідомлення інтегрують із системами SOAR для автоматизованого реагування.
Окрім цього, інструмент надає детальні звіти та інформаційні панелі, що дозволяють відслідковувати тренди, оцінювати рівень відповідності нормативам та аналізувати ефективність заходів захисту.

5. Управління логами та архівування
Оскільки багато галузей (наприклад, охорона здоров’я чи фінанси) зобов’язані зберігати журнали тривалий час, SIEM-система мусить гарантувати цілісність та доступність логів протягом встановленого періоду.
Адміністратори налаштовують політики резервного копіювання й архівування відповідно до вимог стандартів (наприклад, HIPAA для медицини), щоби при аудиті чи розслідуванні можна було швидко отримати потрібні дані.

Вища гнучкість досягається завдяки модульній архітектурі, коли організаційні політики, аналітичні правила і моделі машинного навчання можуть підвантажуватися динамічно, без зупинки основного сервісу SIEM. Крім того, розподілена архітектура з кількома зонами обробки (edge collectors, центральний аналізатор, довгострокове сховище) дозволяє масштабувати систему по горизонталі, уникати єдиного точки відмови та оптимізувати мережевий трафік між філіями та дата-центрами.

У цілісній схемі дані надходять із джерел у вигляді сирих логів, потім агрегуються та нормалізуються, після чого проходять кореляцію й аналітику. Результатом є пріоритизовані інциденти, які передаються системі алертингу та дашбордів, а також механізмам автоматизованого реагування для подальшої обробки та усунення загроз [7]. Цей підхід гарантує, що навіть складні

багатокрокові атаки будуть своєчасно виявлені й відреаговані, забезпечуючи високий рівень стійкості IT-інфраструктури.

2.2. Методи виявлення аномалій і кореляції подій (UEBA, ML-підходи)

У сучасних SIEM-системах кореляція подій та виявлення аномалій базуються на поєднанні традиційних правилових методів із алгоритмами машинного навчання та поведінкової аналітики (UEBA), що дозволяє не лише миттєво виявляти відомі патерни атак, але й автоматично знаходити невідомі загрози на основі відхилень від норми. Правилова кореляція працює за чітко визначеними шаблонами: наприклад, якщо система фіксує п’ять невдалих спроб входу з однієї IP-адреси та одночасно успішний логін із тієї ж адреси, то такий ланцюжок подій інтерпретується як потенційний інцидент злому й зумовлює генерацію сповіщення [31].

Водночас для обробки значного обсягу телеметрії та зниження рівня фальш-тривог застосовуються алгоритми статистичного аналізу та кластеризації. Один із прикладів — використання Gaussian Mixture Models (GMM) або Isolation Forest для автоматичного визначення нетипових шаблонів трафіку або поведінки користувачів, коли дані розподіляються щодо встановленої норми, а відхилення вище певного порогу спрацьовують як аномалії [40].

У межах UEBA (User and Entity Behavior Analytics) платформи, такі як Splunk UBA, спочатку створюють «бейслайни» для кожного користувача та пристрою: на основі історичних даних машинне навчання визначає типову частоту логінів, географічне розташування, часові режими доступу та інші параметри, а потім кожне нове відхилення від цих моделей, наприклад нетипово велика передача даних або вхід з нової країни, оцінюється за ризик-

балом і може автоматично ініціювати кореляцію з іншими подіями безпеки. Аналогічний підхід реалізований у Exabeam, де для кожного ентіті формуються поведінкові профілі, і виявлення складних атак, наприклад багатоетапного скумбінованого зловживання правами, відбувається шляхом поєднання аномальних подій у «відбиток» атаки.

Крім того, сучасні SIEM-платформи активно використовують методи глибокого навчання, зокрема автоенкодери та LSTM-мережі, для виявлення складних послідовностей подій у часових рядах. Так, SIEM+ застосовує рекурентні нейронні мережі для прогнозування типових часових вікон активності сервера, а нетипові «вибухи» подій, що не відповідають моделі, вважаються потенційним індикатором скомпрометованої системи [10].

Ефективна кореляція подій передбачає мультисистемний підхід: дані з IDS/IPS, EDR, мережевих фаєрволів і GRC-платформ збираються централізовано, нормалізуються і за допомогою спільних кореляційних правил та ML-моделей поєднуються в єдині інциденти. Наприклад, коли Suricata виявляє підозрілий пакет, EDR фіксує запуск невідомого процесу, а SIEM-система спільно з Threat Intelligence розгортає контекст загрози, це дозволяє миттєво призначити інциденту критичний пріоритет і запустити автоматизований воркфлоу реагування через SOAR [44].

Таким чином, поєднання правилових механізмів, ML-аналізу та поведінкової аналітики забезпечує високий рівень точності виявлення, знижує кількість хибнопозитивів і дозволяє реагувати на складні кіберзагрози в режимі реального часу.

2.3. Інтеграція інструментів моніторингу та реагування в системі кіберзахисту для забезпечення мережевої й операційної безпеки

На початковому етапі побудови системи кіберзахисту ключову функцію виконують системи виявлення та запобігання вторгненням. Інструменти на кшталт Snort і Suricata представляють собою типові рішення IDS/IPS, які завдяки технології глибокого аналізу мережевого трафіку (Deep Packet Inspection) дозволяють виявляти навіть незначні аномалії в роботі мережі. Це забезпечує фахівцям з безпеки змогу швидко ідентифікувати потенційні загрози та оперативно реагувати на них.

Такі платформи, як Splunk, IBM QRadar або AlienVault USM, забезпечують централізоване збирання та аналіз журналів подій із серверів, мережевого обладнання й кінцевих пристроїв. Це дає можливість не лише ідентифікувати окремі загрози, а й виявляти багатокомпонентні атаки, які на перший погляд здаються несуттєвими, але в сукупності становлять серйозну небезпеку. Вимоги українського законодавства щодо захисту критичної інформаційної інфраструктури передбачають обов’язкове впровадження подібних систем як складової частини комплексного захисту.

З позиції операційної безпеки важливим є постійне спостереження за станом серверних і клієнтських систем. Рішення на зразок CrowdStrike Falcon чи Carbon Black дозволяють відстежувати поведінку кінцевих точок, аналізувати підозрілу активність і своєчасно виявляти шкідливу діяльність, включно з атаками внутрішнього походження. Також широко застосовуються сканери вразливостей (наприклад, Nessus, OpenVAS), які регулярно здійснюють оцінку стану мережевої інфраструктури на предмет наявних уразливостей.

Сучасні SIEM-рішення активно інтегрують технології машинного навчання. Завдяки цьому події аналізуються з використанням нейронних мереж, Random Forest та інших моделей, що дозволяє зменшити кількість

хибнопозитивних тривог і зосередити увагу аналітиків на справді важливих інцидентах.

Процес реагування починається з оперативного виявлення підозрілої активності завдяки налаштованим механізмам сповіщення. Далі відповідні фахівці проводять аналіз ситуації — із використанням як автоматизованих алгоритмів, так і ручної експертної оцінки. Один із перших кроків у такому випадку — локалізація загрози шляхом відключення небезпечного вузла, блокування IP-адреси чи обмеження доступу до скомпрометованих ресурсів, що знижує ризик подальшого поширення інциденту.

Після усунення основних наслідків важливо оновити конфігурації безпеки, застосувати актуальні патчі та адаптувати політики доступу, щоб уникнути повторення інциденту в майбутньому. Етапи цього процесу наочно демонструються у схемі (рис. 2.1), а більш детально описані у NIST SP 800-61 Rev.2 – «Computer Security Incident Handling Guide»[3].

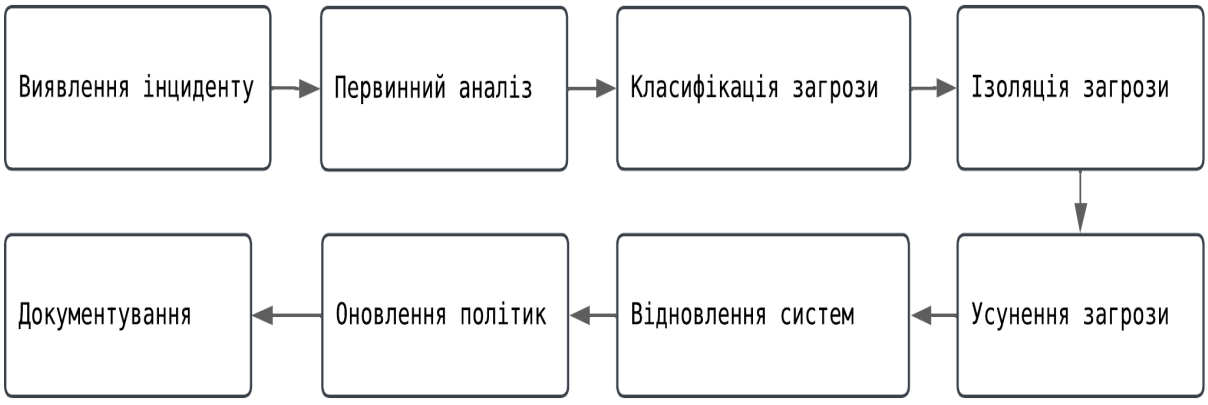

Рис.2.1 Процес реагування на інциденти

Інтеграція усіх згаданих інструментів формує єдину екосистему кіберзахисту, де моніторинг трафіку, обробка логів та контроль кінцевих точок здійснюються в тісній взаємодії, підвищуючи ефективність реагування на загрози.

Застосування таких засобів, як Snort і Suricata для аналізу трафіку, Splunk і IBM QRadar для кореляції подій, а також CrowdStrike Falcon для захисту кінцевих пристроїв, забезпечує надійний багаторівневий захист організації. Це створює умови для безперебійного функціонування підприємства, де інформаційна безпека є невід'ємною частиною його операційної стійкості.

Водночас, окрім технічного арсеналу, вагомим компонентом захисту є підготовка персоналу. Регулярне навчання співробітників з питань кібербезпеки, включно з тренінгами, імітацією атак та внутрішніми аудитами, сприяє підвищенню обізнаності й формуванню корпоративної культури безпеки. Як демонструють практичні кейси, інвестиції в підготовку персоналу суттєво зменшують кількість інцидентів, спричинених людським фактором. На схемі (Рис.2.2) можна побачити основні етапи та послідовність навчання пресоналу. Закон України «Про основні засади забезпечення кібербезпеки» прямо вказує на необхідність професійної підготовки кадрів у сфері кіберзахисту та впровадження відповідних навчальних програм [3].

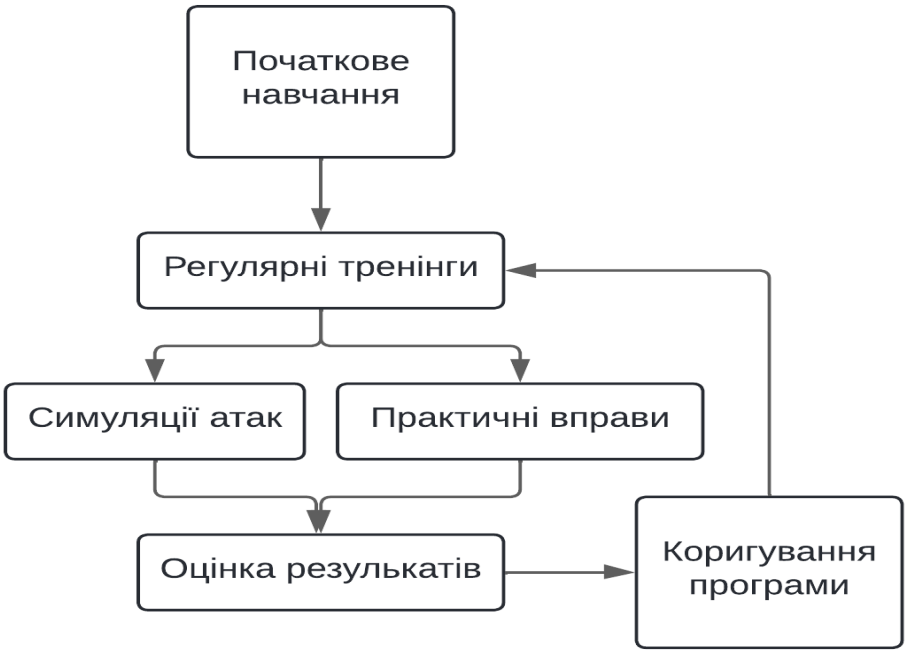

Рис.2.2 схема навчання персоналу

2.4. Порівняльний аналіз Splunk, IBM QRadar та Wazuh

Splunk Enterprise Security, IBM QRadar та Wazuh – популярні SIEM-рішення з різними підходами. Splunk ES – комерційна платформа з гнучкою архітектурою і розвиненим екосистемою додатків, розрахована на корпоративні інфраструктури з великими обсягами даних. Ліцензування Splunk зазвичай прив'язане до обсягу індексованих логів, а інструменти аналітики дозволяють реалізовувати складні сценарії виявлення. IBM QRadar також орієнтований на великі підприємства і використовує модель ліцензій за EPS (подій за секунду). Він відомий потужними можливостями кореляції подій і широким набором конекторів, але потребує уважного планування ємності (EPS, FPM) під пікові навантаження.

Wazuh – відкрите рішення (форк OSSEC/Elastic Stack), яке не вимагає ліцензійних витрат. Воно охоплює основні функції SIEM (збір і аналіз логів, перевірка цілісності файлів, детектор вразливостей тощо) і добре підходить для організацій із обмеженим бюджетом. З іншого боку, Wazuh потребує власних зусиль з розгортання і підтримки. На практиці Wazuh демонструє високу швидкість обробки: у незалежному тесті для записів з мережевих джерел він обробляв близько 14 000 подій/сек, що було на 38–64% вище за інші відкриті SIEM [41]. Splunk і QRadar можуть масштабуватися ще більше (десятки тисяч EPS і більше) при використанні кластера, але їхнім пропускним здатністю керує ліцензія.

За рівнем хибних спрацьовувань та охопленням джерел: усі три рішення потребують налаштування. Splunk і QRadar зазвичай підтримують сотні вбудованих конекторів і стандартних шаблонів обробки, тоді як Wazuh базується на відкритих правилах і agent'ах для основних ОС та пристроїв. Наприклад, Microsoft відзначає, що неповне логування навіть критичних підсистем може створювати «сліпі зони» [39]. Загалом, Splunk вважається

найбільш «масштабованим» і функціонально багатим за рахунок спільноти, QRadar – досвідченим у корпоративній безпеці, а Wazuh – бюджетним і гнучким, але вимагає більше ручної роботи.

Підбиваючи висновки щодо вибору SIEM, можна зазначити, що вибір залежить від розміру організації, бюджету та критичності систем. Для великих підприємств з високими вимогами до безпеки й ресурсів зазвичай віддають перевагу Splunk ES або IBM QRadar – їхні можливості та підтримка обґрунтовують вищі витрати [38]. Ці рішення забезпечують глибоку аналітику і широко підтримують інтеграцію з різними джерелами даних. Для організацій з обмеженим бюджетом або з обмеженим штатом безпеки кращим вибором може бути Wazuh – він безкоштовний і дає належний функціонал, але вимагає інвестицій часу на налаштування та підтримку. Як показують дослідження, відкриті SIEM-рішення привертають увагу малих і середніх підприємств через доступність, однак слід усвідомлювати додаткові експлуатаційні витрати [41[].

Узагальнюючи, при невеликому масштабі і тісному бюджеті варто розглядати Wazuh чи хмарні легкі сервіси, а при великих обсягах даних і високих вимогах до безпеки – Splunk або QRadar.

2.5. Постінцидентний аналіз та усунення вразливостей

Постінцидентний аналіз є ключовим етапом життєвого циклу реагування на інциденти, що дозволяє не лише закріпити результати ліквідації загрози, а й системно виявити слабкі місця в захисних механізмах і процесах, щоб запобігти повторенню подібних подій у майбутньому. Усунення вразливостей, в свою чергу, є невід’ємною складовою постінцидентного аналізу і передбачає комплекс заходів від ідентифікації вразливостей до їх остаточного нейтралізування та перевірки результатів.

1. Проведення розслідування й аналізу причин

Першим кроком є ретельне збирання та кореляція всіх доступних даних інциденту — логів мережі, системних подій та даних EDR/HIDS — для з'ясування ланцюжка подій, що призвів до компрометації. У рамках Root Cause Analysis аналізуються не лише технічні вектори атаки (наприклад, експлуатація відомої вразливості чи фішинговий лист), а й організаційні аспекти: невідповідні конфігурації, відсутність оновлень або прогалини в політиках доступу.

2. Документування інциденту та уроків

Після технічного розслідування команда фіксує повну хронологію подій, причини кожного кроку та дії, що вже були виконані під час реагування. У звіті Lessons Learned описуються не лише технічні деталі, але й організаційні прогалини — наприклад, пізнє виявлення атаки або недостатня комунікація між підрозділами. Результати Lessons Learned формують базу для перегляду політик та процедур згідно з рекомендаціями ISO/IEC 27035 і NIST SP 800-61[18].

3. Ідентифікація та пріоритезація вразливостей

У ході розслідування виявляються конкретні вразливості — у ПЗ, конфігураціях чи бізнес-процесах. Кожну вразливість оцінюють за критеріями CVSS (Common Vulnerability Scoring System) або внутрішніми метриками ризику, що поєднують ймовірність експлуатації та потенційний вплив на бізнес. Пріоритізація дозволяє спрямувати обмежені ресурси на усунення найбільш критичних проблем у першу чергу.

4. Усунення вразливостей

Усунення вразливостей включає низку дій:

- Випуск патчів або оновлень програмного забезпечення відповідно до політики керування змінами.
- Зміна конфігурацій (блокування небезпечних портів, посилення налаштувань шифрування, обмеження прав доступу).
- Впровадження компенсаційних заходів, якщо патчі недоступні (наприклад, мережеві ACL або WAF-правила).

- Оновлення політик та процедур, щоб автоматизувати подібне усунення у майбутньому (наприклад, регулярне сканування вразливостей).

5. Перевірка ефективності заходів

Після застосування контрзаходів необхідно підтвердити їхню дієвість шляхом повторного сканування та тестування (penetration test або автоматизований Vulnerability Scan). Якщо вразливість не усунена повністю, цикл повторюється: аналізуються нові дані, корегуються заходи й перевіряється результат.

6. Оновлення систем моніторингу та кореляційних правил

На основі уроків інциденту та усунених вразливостей оновлюють правила SIEM (логічні кореляції) і IDS/IPS (сигнатури для Suricata, правила детекції у Wazuh). Це дозволяє у майбутньому виявляти ознаки схожих атак швидше та з меншою кількістю хибнопозитивів.

7. Формалізація процесу постінцидентного аналізу

Здобутий досвід формалізують у вигляді чек-лістів і шаблонів звітів (Post-Incident Review Playbooks від CISA) для стандартизації процесу та забезпечення швидкого залучення відповідних фахівців у разі нових інцидентів.

2.6 Методи аудиту та тестування систем моніторингу та реагування на інциденти

Аудит інформаційної безпеки – це системний, незалежний і документований процес отримання об’єктивних якісних та кількісних оцінок поточного стану захисту інформаційних ресурсів. Його завданнями є збір об’єктивних доказів безпеки, аналіз ризиків і вразливостей, оцінка рівня захищеності системи, виявлення «вузьких місць» захисту та перевірка відповідності стандартам і вимогам. Аудит дозволяє скласти картину ІБ–ризиків компанії, перевірити виконання політик та заходів безпеки, та отримати

рекомендації щодо покращення захисту. В Україні та світі підготовка аудиторів регламентується стандартами, зокрема ISO/IEC 27007 (вказівки щодо аудиту СУІБ, що доповнює ISO 19011), сам стандарт ISO/IEC 19011 (методологія аудитів систем менеджменту) та стандарти ISO/IEC 27001/27035, а також рекомендації NIST SP 800-53 (контроли безпеки) та SP 800-61 (реагування на інциденти).

Важлива роль аудиту – перевірка ефективності систем моніторингу та реагування (SIEM/SOAR). Під час аудиту SIEM оцінюють коректність налаштування збору подій і кореляційних правил, відповідність логування політикам та реакцію на знайдені індикатори. NIST підкреслює необхідність встановлення чітких стандартів і процедур логування, а також регулярного аналізу зібраних даних. Автоматизовані інструменти (SIEM/SOAR) повинні своєчасно відсилати сповіщення про підозрілу активність, а результат їхньої роботи фіксується та аналізується в процесі аудиту. Такі перевірки дозволяють виявити пропуски у конфігурації моніторингу, недостатній обсяг збираних даних або недоліки у реакціях на інциденти та рекомендувати відповідні поліпшення.

Види аудиту. За ініціативою організації розрізняють різні види аудитів ІБ. Зовнішній аудит – зазвичай разова оцінка, що виконується сторонніми спеціалістами або організаціями. Прикладом може бути пентест або «етичний хакинг», коли зовнішній фахівець оцінює стійкість системи до атак з боку інтернету. Зовнішній аудит включає сканування портів, пошук вразливостей у мережевому та прикладному ПЗ, спроби взаємодії з Web-, поштовими і файловими серверами тощо. Внутрішній аудит – безперервна діяльність штатної команди аудиторів за внутрішнім регламентом організації. Він проводиться всередині мережевого простору організації (за зовнішнім фаєрволом) та зазвичай включає автоматизовані перевірки внутрішніх хостів і мережевих пристроїв, аналіз дотримання політик доступу, контролю прав

користувачів, паролів тощо. Внутрішній аудит також оцінює ризики існуючих технологій та перевіряє, чи виконуються встановлені організаційні процедури.

- Аудит відповідності (compliance audit) – перевіряє, наскільки політики та реальні заходи безпеки відповідають прийнятим стандартам і вимогам (наприклад, ISO 27001, нормативам галузі). Аудитори зіставляють конфігурації й звіти систем з критеріями стандартів і виявляють невідповідності.
- Технічний аудит – фокусується на технічних засобах захисту: перевірці конфігурацій мережевих пристроїв, антивірусів, систем виявлення вторгнень тощо. Цей аудит зазвичай включає детальну перевірку налаштувань, опитування системними сканерами та аналіз мережевих вразливостей (порти, сервіси).

Кожен з видів аудиту генерує звіт із виявленими ризиками, уразливостями і рекомендаціями. Наприклад, в результаті аудиту ІБ складаються: характеристика інформаційної системи як об’єкта захисту; формулярні опис кожного робочого місця і завдань; переліки ресурсів, користувачів та використовуваної інформації. Часто аудиторські звіти включають висновки про «слабкі точки» системи, невідповідні або неповні записи журналів (журналів подій) та план покращень. Звіти аудиту є важливим інструментом планування подальших заходів безпеки та оцінки інвестицій у захист ІБ.

Один з найважливіших методів перевірки безпеки – *penetration testing* (пентест): фахівці-«етичні хакери» імітують реальні атаки, щоб знайти способи обходу наявних механізмів захисту. У NIST SP 800-115 пентест визначено як тестування, при якому оцінювачі моделюють реальні напади на систему або мережу, використовуючи відомі вразливості і звичайні тактики зловмисників. Пентест включає фази планування, розвідки (сканування мережі, переліку послуг), атаки з використанням знайдених вразливостей і звітності. Під час

таких тестів оцінюють не тільки успіх атаки, а й здатність системи виявити і зафіксувати вторгнення (таким чином перевіряючи налаштування SIEM/SOAR).

Крім пентестів, до основних методів тестування належать:

- Оцінка вразливостей (Vulnerability Assessment): за допомогою сканерів виявляють відомі вразливості у програмному забезпеченні, мережевих пристроях та сервісах. Це менш інвазивний метод порівняно з пентестом, він дає перелік можливих слабких місць – непатчений софт, відкриті порти, небезпечні конфігурації – для подальшого дослідження.
- Перегляд і аналіз журналів подій (Log Review): систематичний аналіз системних та мережевих логів для виявлення аномалій і ознак інцидентів. Регулярний огляд журналів допомагає своєчасно виявити інциденти та порушення політик безпеки. NIST наголошує, що рутинний аналіз логів корисний для ідентифікації інцидентів, порушень політик та довгострокових проблем. Результати такого аналізу дозволяють підтвердити або спростувати сповіщення SIEM і за необхідності скоригувати правила кореляції подій.
- Імітація інцидентів (Simulation): проведення навчальних або реальних тренувань (tabletop / full-scale exercises). За цим методом передбачають сценарії нападів (напр., фішинг, DoS тощо) для перевірки готовності команди реагування і коректності процесів. Такі заходи дають змогу оцінити, наскільки швидко і ефективно відпрацьовуються процедури реагування (план реагування, ескалація, повідомлення відповідальних). [NIST SP 800-61 рекомендує періодично влаштовувати «mesaeta learning» та аналіз проведених інцидентів для покращення процедур реагування].
- Red Team / Blue Team: комплексні змагання між «червоними» і «синіми» командами. Червона команда імітує реальних зловмисників, застосовуючи різні методи атаки (фішинг, соціальна інженерія, lateral movement, злам зламаних облікових, використання власних інструментів тощо), тоді як Синя команда відстежує, виявляє та блокує атаки. Результатом такої вправи є звіти Red Team про виконані атаки і рекомендації, а також звіти Blue

Team про виконані захисні дії. Наприклад, в описах Red Team наведено, що вона надає детальні звіти про всі виконані операції, а Blue Team фіксує та документує виправлення виявлених уразливостей. Поєднання Червоних та Синіх команд (іноді з участю «Purple Team») дозволяє провести глибокий аудит системи захисту й відпрацювати інтегровані заходи захисту.

Прикладом застосування є регулярний аудит SOC (Security Operations Center): незалежні аудитори перевіряють, чи налаштовані всі критичні системи логування, чи збираються логи із серверів, брандмауерів, хмарних сервісів, IDS/IPS, та коректно відпрацьовуються інциденти. Під час такого аудиту можуть виявитися: налаштування, що пропускають частину подій; зайві або неактуальні сигнатури; нестача тестів у SOAR; відсутність реагування на певні класи подій тощо. Такі знахідки фіксуються в звіті.

Типові результати аудиту включають формулювання: характеристику ІС як об’єкта захисту; опис структурних компонентів і конфігурацій; формуляри робочих місць та завдань користувачів; переліки завдань і видів інформації, що обробляються. Також аудитори надають звіт про виявлені інциденти (журнали нападів, помилки конфігурацій тощо) і «слабкі місця» системи. На основі цих даних розробляються рекомендації – наприклад, зміни в політиках доступу, додаткові правила кореляції в SIEM, впровадження нових засобів моніторингу або навчання персоналу. Грамотно проведений аудит (внутрішній чи зовнішній) дозволяє впевнитися у тому, що системи SIEM/SOAR і процеси реагування дійсно ефективні, і що ресурси безпеки використовуються раціонально.

Висновки до розділу 2

У результаті проведеного аналізу сучасних систем моніторингу та реагування на інциденти інформаційної безпеки стало очевидним, що їх

ефективність значною мірою визначається правильним вибором архітектурної моделі та гнучкістю в інтеграції з іншими засобами захисту. Розгляд локальних, хмарних і гібридних рішень продемонстрував, як компроміс між контролем над інфраструктурою, швидкістю впровадження та витратами на підтримку визначає кінцевий вигляд системи. Системи SIEM, об’єднуючи збір, нормалізацію та кореляцію подій, забезпечують єдину точку зору на безпекову ситуацію, тоді як IDS/IPS доповнюють цей підхід негайним виявленням мережевих атак на основі аналізу трафіку. На етапі післяінцидентного аналізу забезпечується критична можливість виявити корінні причини порушень та закріпити результати усунення вразливостей, що сприяє безперервному підвищенню стійкості IT-інфраструктури. Висвітлено методи аудиту й тестування, що дають змогу оцінити реальну ефективність впроваджених рішень. Накопичений досвід свідчить про те, що лише комплексний підхід — від продуманої архітектури до організації взаємодії між технологіями та фахівцями — здатен гарантувати своєчасне виявлення загроз, мінімізацію їх наслідків і підтримку належного рівня відповідності нормативним вимогам.

РОЗДІЛ 3. ХМАРНІ ПРАКТИЧНІ РІШЕННЯ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ДЛЯ МАЛОГО БІЗНЕСУ

У цьому розділі наведено практичні рекомендації щодо побудови систем моніторингу і реагування на інциденти інформаційної безпеки із застосуванням готових або хмарних рішень, орієнтованих на малий бізнес. Передбачається мінімальне власне розгортання серверних компонентів, що знижує складність обслуговування та початкові витрати.

3.1. Хмарні та готові до використання SIEM/EDR-рішення

Для малого бізнесу оптимальним є використання SaaS-рішень та безкоштовних редакцій відомих продуктів. Наприклад, Wazuh Cloud пропонує керовану хмарну платформу для моніторингу безпеки (SIEM/XDR), що відповідає стандартам PCI DSS та SOC2. Splunk Free дозволяє безкоштовно індексувати до 500 МБ логів на добу у межах одного інстансу, однак не підтримує оповіщення [37].

CrowdStrike Falcon – приклад хмарного EDR (Endpoint Detection and Response), яке легко масштабується для невеликої кількості пристроїв. EDR-системи безперервно реєструють поведінку кінцевих точок і з використанням аналітики виявляють підозрілу активність [8]. CrowdStrike надає безкоштовні демо-версії (Falcon Demo), що дозволяє малим компаніям оцінити можливості захисту без початкових інвестицій. Також існують вбудовані альтернативи – наприклад, Microsoft Defender for Business з базовим EDR для Windows-пристроїв.

Щодо мережевого моніторингу, відкритий Suricata може бути використаний як IDS/IPS-сенсор на окремому пристрої або віртуальній машині. Suricata – це багатопотоковий IDS/IPS з відкритим кодом, який застосовується і

в малих, і в великих організаціях. Вона аналізує мережевий трафік за допомогою правил безпеки і може працювати на Windows або Mac (а не тільки на Linux). Suricata є маловитратною та забезпечує глибоку інспекцію мережевих загроз [32].

Для аналітики поведінки користувачів (UEBA) використовують відповідні можливості SIEM. Наприклад, Splunk UBA застосовує моделі поведінки та машинне навчання для виявлення прихованих загроз [37]. Реалізація UEBA не потребує локальних серверів — достатньо налаштувати збір логів, а сам аналіз аномалій виконує хмарна платформа.

Варто також відзначити роль SOAR (Security Orchestration, Automation and Response). SOAR-платформи координують різні системи безпеки та автоматизують реагування на інциденти. Для малого бізнесу доступні легкі або open-source SOAR-рішення (наприклад, Shuffle), що дозволяють виконувати наперед визначені плейбуки без великої команди. Автоматизація SOAR дає змогу ефективніше обробляти численні алерти без пропорційного збільшення штату [28].

Приклад архітектури хмарного SIEM-рішення можна побачити на схемі (Рис.3.1) агенти та сенсори на кінцевих пристроях збирають події й відправляють їх у централізовану систему індексації. Система індексації аналізує дані та надає веб-інтерфейс для пошуку і візуалізації подій. Ця схема ілюструє, як події з різних джерел (ендпоінтів, мережі тощо) консолідуються у єдиному репозиторії SIEM для моніторингу й реагування.

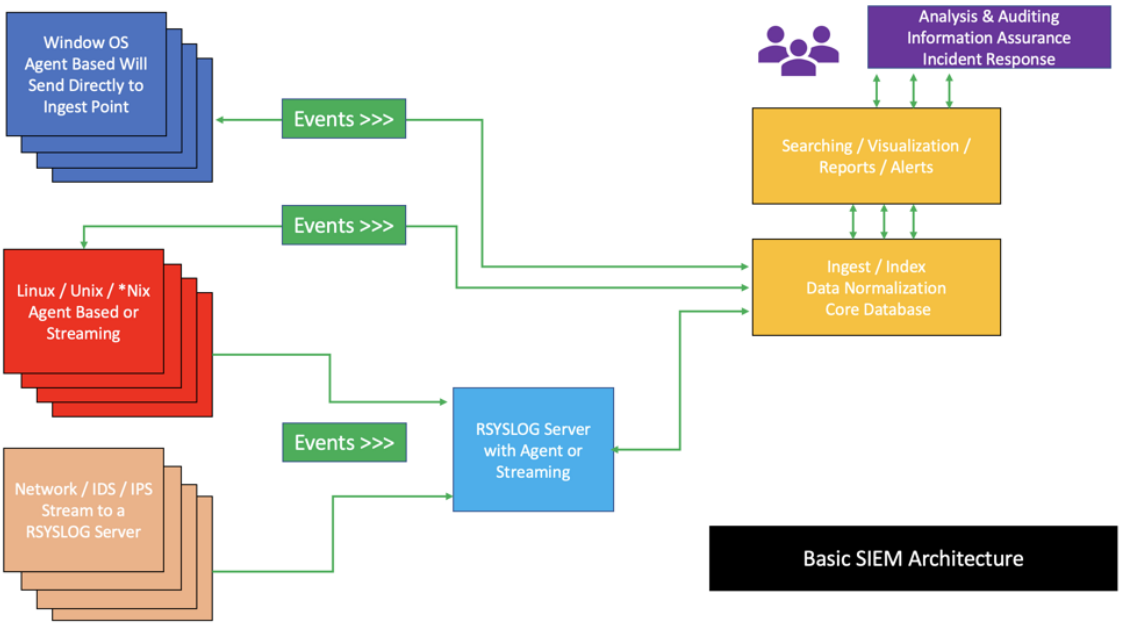

Рис.3.1 Приклад архітектури хмарного SIEM-рішення

3.2. Архітектурні схеми без локального розгортання

Оскільки SaaS-підхід мінімізує власну інфраструктуру, можливі прості архітектурні схеми. Зазвичай у них використовується агентське ПЗ на кінцевих точках (Wazuh/OSQuery на Windows, Splunk Universal Forwarder, Falcon Sensor) та мережеві IDS-датчики (Suricata, Zeek), що пересилають події у хмарну SIEM (рис. 3.1). У такій архітектурі не потрібно розгортати власні Linux-сервери. Основний сервер індексації (наприклад, хмарний кластер Wazuh або Splunk Cloud) збирає події з усіх джерел, а результати аналізу доступні через веб-інтерфейс.

Наприклад, агенти Wazuh на Windows-машинах відправляють системні логи (Sysmon, журнали подій) у Wazuh Cloud. Мережевий трафік контролює Suricata, яка відправляє IDS-події до SIEM через syslog або API. Splunk Free, запущений на окремій віртуальній машині (Windows або Docker-контейнері), індексує дані з різних джерел для подальшого аналізу. Одночасно CrowdStrike Falcon Sensor на кінцевих точках надсилає телеметрію у хмару Falcon для

розширеного аналізу. Така архітектура забезпечує всебічний моніторинг без необхідності складного розгортання локальних серверів.

Продовжуючи розвиток цієї моделі, варто зазначити, що сучасні хмарні рішення, такі як Microsoft Sentinel чи Splunk Cloud Platform, дозволяють організовувати моніторинг і реагування без встановлення будь-яких внутрішніх серверних компонентів. У таких схемах всі ключові функції – зберігання логів, їх індексація, кореляція подій, UEBA-аналітика, побудова дашбордів та оповіщення – виконуються безпосередньо у хмарному середовищі. З боку користувача достатньо встановити агенти на робочих станціях або використати вбудовані конектори до хмарних сервісів, таких як Office 365, AWS чи Google Workspace, після чого дані одразу надходять у хмарний SIEM.

Прикладом такої архітектури є Splunk Cloud, у якому всі елементи – індексери, балансувальники навантаження та пошукові вузли – розміщуються в дата-центрах Amazon Web Services або Google Cloud. Доступ до них здійснюється через захищені канали, а передача подій реалізується за допомогою Splunk Universal Forwarder або HTTP Event Collector. Аналогічно, у Microsoft Sentinel роль колектора виконує служба Azure Monitor, яка приймає події з локальних мережевих пристроїв, Windows-журналів, хмарних платформ і автоматично зберігає їх у Log Analytics.

На схемі (рис. 3.2) наведено спрощену архітектуру Splunk Cloud Platform (Victoria Experience). Індексери даних розгорнуті у кількох зонах доступності (AZ) для відмовостійкості, а пошукові сервери (Search Head Cluster) підключені до них через балансувальник навантаження. Події надходять від універсальних форвардерів (порт TCP 9997) або через HTTP Event Collector (порт 443) від агентів у середовищі замовника. Splunk Cloud за замовчуванням шифрує дані в транзиті і дозволяє налаштовувати правила доступу на мережевому рівні для підвищення безпеки [37].

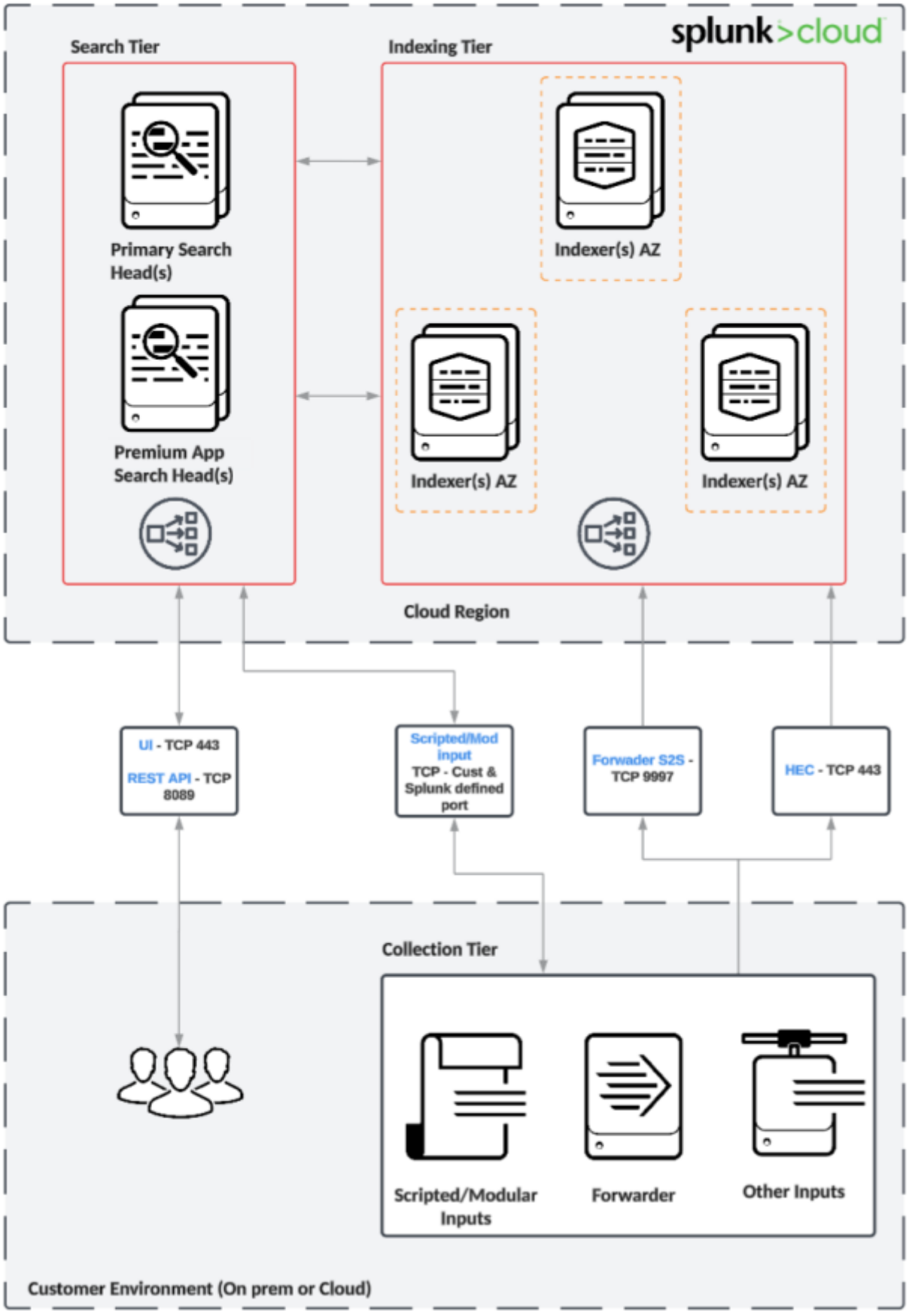

Рис. 3.2 Хмарна платформа Splunk з Victoria Experlence

Ще одна важлива складова – це автоматизація реагування через SOAR-функціональність. Наприклад, у Microsoft Sentinel такі сценарії створюються у вигляді playbook'ів у Logic Apps, де кожен інцидент може автоматично запускати ланцюжок дій: надсилання повідомлення в Teams, ізоляцію пристрою у Defender for Endpoint чи відкриття заявки в ITSM-системі. В open-source рішенні Wazuh хмарна консоль дозволяє інтегрувати прості автоматизовані дії на основі правил, наприклад, блокування IP-адрес через сторонній фаєрвол або надсилання повідомлень у Telegram через webhook.

Завдяки повній хмарній реалізації компанії можуть швидко розпочати моніторинг подій без витрат на розгортання інфраструктури, а масштабування відбувається автоматично. У такій архітектурі спрощується резервне копіювання, оновлення системи та забезпечується доступ до звітності з будь-якого пристрою. При цьому критично важливим стає забезпечення надійного інтернет-з’єднання та дотримання політик шифрування й обмеження доступу, оскільки конфіденційні журнали подій зберігаються у хмарі. Водночас завдяки гнучкій оплаті за спожиті ресурси та наявності безкоштовних або пробних версій, такі рішення залишаються доступними навіть для малого бізнесу, забезпечуючи професійний рівень захисту.

3.3. Оцінка ефективності

Хмарні SIEM/EDR-комплекти демонструють суттєве покращення видимості загроз для малого бізнесу. Централізована UEBA-аналітика в Splunk Free дозволяє автоматично виявляти відхилення від нормальної поведінки користувачів і систем без потреби в локальних серверах — достатньо налаштувати збір логів у хмару та активувати відповідні модулі ML-аналітики. Поєднання даних із Windows-логів (Wazuh Cloud) та мережевих IDS-сповіщень

(Suricata) підвищує шанси на своєчасне виявлення складних атак, таких як Pass-the-Hash чи латеральне переміщення всередині мережі [27].

Використання SOAR-плейбуків у Shuffle або інших легких платформах дозволяє автоматизувати рутинні дії: ізоляцію зловмисного вузла, блокування підозрілих IP-адрес і надсилання сповіщень до відповідальних осіб без збільшення штату аналітиків GXAIT. Це скорочує середній час реагування (MTTR) й одночасно знижує навантаження на команду безпеки.

Водночас для стабільного функціонування таких рішень потрібне надійне інтернет-з’єднання: збій каналу може призвести до втрати телеметрії, що знижує загальну ефективність моніторингу. Конфіденційність даних також залежить від рівня безпеки провайдера хмарних сервісів, а розміщення логів у чужих центрах опрацювання даних може підпадати під регуляторні ризики GDPR чи локальних законів про захист інформації. Безкоштовні редакції (Splunk Free, Falcon Demo) мають функціональні обмеження — ліміт на обсяг індексованих логів, відсутність оповіщень або глибокого контекстного аналізу — через що для зростання бізнесу може знадобитися перехід на платні тарифи або комбінування декількох інструментів [37].

Висновки розділу 3

Підсумовуючи, перехід на хмарні SIEM/EDR-платформи дозволяє малому бізнесу отримати сучасний рівень видимості й автоматизованої аналітики без потреби у власному дата-центрі чи значних IT-ресурсах. Комбінація Wazuh Cloud, Splunk Free і Falcon Demo показує, як за допомогою SaaS-рішень можна охопити моніторинг кінцевих пристроїв, мережевий трафік та поведінкову аналітику, при цьому легко масштабуватися та вбудувати прості SOAR-сценарії для негайного блокування підозрілих подій. Головним обмеженням залишається залежність від стабільного інтернет-з’єднання та політик

збереження даних провайдерів, а також функціональні рамки безкоштовних редакцій, що спонукає до поступового переходу на платні тарифні плани в міру зростання обсягів логів.

Таким чином, хмарні рішення виявилися ефективними інструментами для організації базового та проміжного рівня кіберзахисту, а їх введення гарантує гнучкість, швидкість розгортання і мінімальні капітальні витрати, залишаючи простір для поступового нарощування потужностей у міру зростання бізнесу.

ВИСНОВКИ

У кваліфікаційній роботі проведено аналіз та практичне дослідження систем моніторингу та реагування на інциденти інформаційної безпеки, що дало змогу узагальнити основну проблематику та сформувати наступні висновки.

1. Проаналізовано стан розвитку сучасних SIEM-систем, що доводить їхню ключову роль у забезпеченні інформаційної безпеки в організаціях із різним рівнем складності IT-інфраструктури. Встановлено, що сучасні платформи моніторингу та реагування на інциденти ефективно поєднують можливості збору, аналізу, кореляції та візуалізації подій, формуючи основу для прийняття рішень у сфері кіберзахисту.

2. Досліджено функціональну архітектуру SIEM-систем, зокрема механізми збору, агрегації та нормалізації логів з різноманітних джерел, включно з серверними платформами, мережевим обладнанням, кінцевими пристроями та хмарними службами. Виокремлено базові компоненти SIEM-рішень: модулі збору, парсингу, кореляції подій, генерації сповіщень, звітності та довготривалого зберігання логів.

3. Проаналізовано методи обробки та уніфікації даних у SIEM-системах, що дозволяє підвищити ефективність виявлення загроз та автоматизувати процеси реагування. Визначено, що нормалізація є критичною умовою для побудови логічних зв’язків між подіями та створення ефективних аналітичних сценаріїв.

4. Встановлено основні принципи кореляції подій у системах моніторингу, зокрема застосування правил на основі поведінкових шаблонів, індикаторів компрометації та алгоритмів машинного навчання. Зазначено, що впровадження таких методів значно скорочує час виявлення інцидентів і підвищує точність реагування.

5. Визначено інструменти оповіщення, звітності та візуалізації, реалізовані в сучасних SIEM-рішеннях. Встановлено, що аналітичні панелі й механізми звітності дають змогу службі безпеки оперативно оцінювати стан інфраструктури, виявляти слабкі місця та приймати обґрунтовані рішення.

6. Проведено порівняльний аналіз поширених SIEM-рішень, зокрема Splunk Enterprise, IBM QRadar та Wazuh. Виокремлено особливості кожного продукту з точки зору функціональності, архітектури, масштабованості та гнучкості розгортання. Обґрунтовано, що вибір конкретного рішення залежить від масштабів організації, обсягів оброблюваних даних та ресурсних обмежень.

7. Виявлено тенденції розвитку SIEM-технологій, зокрема зростання використання хмарних платформ, інтеграції з XDR- і SOAR-рішеннями, а також розширення застосування штучного інтелекту для прогнозування загроз. Установлено, що ці тенденції сприяють автоматизації операцій безпеки та зниженню навантаження на аналітиків.

8. Обґрунтовано доцільність використання SIEM-систем як ядра сучасного Центру моніторингу безпеки (SOC). Результати дослідження підтверджують, що впровадження SIEM дозволяє істотно підвищити рівень кіберстійкості організації, знизити ризики порушення конфіденційності та цілісності даних, а також забезпечити відповідність нормативним вимогам.

9. Запропоновано рекомендації для подальшого застосування результатів дослідження в практичній діяльності, зокрема: при впровадженні SIEM-систем доцільно орієнтуватися на рівень автоматизації, масштабованість платформи, можливість інтеграції з існуючими захисними механізмами та наявність адаптованих шаблонів кореляції для галузевих потреб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бортник К.Я., Делявський М.В., Кузьмич О.І. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2020. Випуск № 41 с. 140 URL: https://cit.lntu.edu.ua/index.php/cit/article/view/199

2. Закон України № 2163-VIII від 05.10.2017 «Про основні засади забезпечення кібербезпеки України» URL: https://zakon.rada.gov.ua/go/2163-19

3. Рубан Ю.Р. Навчально-науковий інститут кібербезпеки та захисту інформації ДУІКТ. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали Всеукраїнської науково-практичної Інтернет-конференції Київ: ДУІКТ, 2025. – 152-156 с. URL: https://duikt.edu.ua/uploads/p_2779_46212583.pdf

4. Постанова Кабінету Міністрів України від 28.03.2025 № 447 «Про внесення змін щодо кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури до деяких постанов Кабінету Міністрів України». URL: https://zakon.rada.gov.ua/go/447-2025-п

5. AI for Incident Response: Benefits, Challenges & Best Practices. URL: https://www.blinkops.com/blog/ai-incident-response

6. Alex Nelson Sanjay Rekhi Murugiah Souppaya Karen Scarfone. Incident Response Recommendations and Considerations for Cybersecurity Risk Management, 2025. – 40 с. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

7. Anjali Udasi. SIEM Architecture: Key Components, Integrations, and More URL: https://last9.io/blog/siem-architecture/

8. Anne Aarness. What is Endpoint Detection and Response (EDR)? 01.07.2025 URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

9. Anomaly Detection in Cybersecurity URL: https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/anomaly-

detection/

10. Austin Page, Farzaneh Abazari, Frank Eargle, Akramul Azim, and Jeff Gardiner. SIEM+: Harnessing Machine Learning for Advanced AnomalyDetection in Cybersecurity Software URL: https://caiac.pubpub.org/pub/03pp58fm

11. Ashlyn Burgett Practical Incident Response Guidance from NIST SP 800-61 URL: https://armorpoint.com/2024/05/08/a-step-by-step-guide-to-incident-response-practical-guidance-from-nist-sp-800-61

12. Automated Incident Response: What It Is, Tools and Use Cases URL: https://www.threatintelligence.com/blog/automated-incident-response

13. CIS Control 17: Incident Response Management URL: https://cas.docs.cisecurity.org/en/latest/source/Controls17/

14. CIS Control 8: Audit Log Management URL: https://cas.docs.cisecurity.org/en/latest/source/Controls8/

15. David Tidmarsh. The Top 3 Challenges with Incident Response URL: https://www.eccouncil.org/cybersecurity-exchange/incident-handling/incident-response-challenges/

16. Divyesh Vaishnav. NIST SP 800–61 Incident Response Life Cycle Explained URL: https://medium.com/%40divyesh.vaishanv/nist-sp-800-61-incident-response-life-cycle-explained-b7b63372cd3c

17. Eran Salfati, Michael Pease. Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT), 2022. – 58 c. URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8428.pdf

18. Fortinet Inc. FortiSOAR: Orchestration, Automation and Response Platform URL: https://www.fortinet.com/products/management/fortisoar

19. Harshala J. ISO 27001 Annex : A.12.4 Logging and Monitoring Its objective is recording events and generating evidence. URL: https://infocerts.com/iso-27001-annex-a-12-4-logging-and-monitoring/

20. ISO 27001 vs. ISO 27002: Understanding the difference; URL: https://www.nemko.com/iso-27001-vs-iso-27002

21. Incident management for high-velocity teams URL: https://www.atlassian.com/incident-management/incident-response/lifecycle

22. International Organization for Standardization. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements 2022. – URL: https://www.iso.org/standard/82875.html

23. IT Governance (USA). The ISO 27002 Standard: Code of Practice for Information Security Controls URL: https://www.itgovernanceusa.com/iso27002

24. Incident Response Automation: How It Works & Best Practices URL: https://www.cortex.io/post/incident-response-automation

25. Information sharing recommendations of NIST SP 800-61 URL: https://old.rapid7.com/blog/post/2017/02/21/nist-sp-800-61-information-sharing/

26. Introduction to Incident Response Life Cycle of NIST SP 800-61 URL: https://www.rapid7.com/blog/post/2017/01/11/introduction-to-incident-response-life-cycle-of-nist-sp-800-61/

27. Introduction to ISO/IEC 27035 - Planning for and Detection of Incidents URL: https://www.rapid7.com/blog/post/2017/04/20/introduction-to-isoiec-27035-planning-for-and-detection-of-incidents/

28. jobmarangu1. Leveraging Security Orchestration, Automation, and Response (SOAR) Tools for Small to Medium Businesses 04.22.2024 URL: https://gxait.com/business-technology/leveraging-security-orchestration-automation-and-response-soar-tools-for-small-to-medium-businesses/

29. Laiba Siddiqui. IT Events & Event Correlation: A Complete Guide URL: https://www.splunk.com/en_us/blog/learn/it-event-correlation.html

30. Leveraging Continuous Monitoring for Proactive Risk Management URL: https://www.certa.ai/blogs/leveraging-continuous-monitoring-for-proactive-risk-management

31. ManageEngine Log360 URL: https://www.manageengine.com/log-management/siem

32. Mark Viglione. Suricata: What is it and how can we use it. 03.04.2022 URL: https://www.infosecinstitute.com/resources/network-security-101/suricata-what-is-it-and-how-can-we-use-it/

33. Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone. National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide – Gaithersburg, MD, 2012. – 80 c. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

34. NIST Incident Response: 4-Step Life Cycle, Templates and Tips URL: https://www.cynet.com/incident-response/nist-incident-response/

35. NIST, GDPR, PCI-DSS, ISO 27001, CSF & FCA on Cyber Incident Response URL: https://www.cm-alliance.com/cybersecurity-blog/nist-gdpr-pci-dss-iso-27001-csf-fca-on-cyber-incident-response

36. Orion Cassetto. Automated Incident Response: What it is, and What its Key Benefits Are URL: https://radiantsecurity.ai/learn/automated-incident-response/

37. Splunk UBA models overview - Splunk Documentation URL: https://docs.splunk.com/Documentation

38. The Total Economic Impact™ Of IBM Security QRadar SIEM 2023. – 30 c. URL: https://4719eaee91034be722d8-c86a406a93c55de2464febd03debd4f0.ssl.cf1.rackcdn.com/ar_Forrester_The_Total_Economic_Impact_Of_IBM_Security_QRadar_SIEM_1.PDF

39. TJBanasik Modernize Log Management with the Maturity Model for Event Log Management (M-21-31) Solution URL: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/modernize-log-management-with-the-maturity-model-for-event-log/ba-p/3072842

40. UEBA Tools: Key Capabilities and 7 Tools You Should Know URL: https://www.exabeam.com/explainers/ueba/ueba-tools-key-capabilities-and-7-tools-you-should-know/

41. Viacheslav Kovtun. Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs URL:

https://pmc.ncbi.nlm.nih.gov/articles/PMC10977669/

42. Vice Vicente NIST Incident Response: Your Go-To Guide to Handling Cybersecurity Incidents URL: https://auditboard.com/blog/nist-incident-response

43. Vice Vicente. The Essentials of Integrated Risk Management (IRM) URL: https://auditboard.com/blog/integrated-risk-management-irm

44. What is Event Correlation? Examples, Benefits, and More URL: https://www.digitalguardian.com/blog/what-event-correlation-examples-benefits-and-more

45. What Is ISO/IEC 27005 and the Security Risk Management Standard URL: https://www.isms.online/iso-27005

46. What is SIEM Architecture? Components & Best Practices URL: https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-architecture/