Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах”

Виконав здобувач вищої освіти
II курсу, групи КІ-25М
ОПП «Комп’ютерна інженерія»
спеціальності F7 «Комп’ютерна інженерія»
_____ Килимник Д.В.
«____» _____ 2026 р.

Керівник проекту
доктор технічних наук, професор
_____ Коваленко О.В.
«____» _____ 2026 р.

Нормоконтроль проекту
_____ Коваленко А.С.
«____» _____ 2026 р.

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
Килимник Дмитро Віталійович
Сертифікат: 18DF2C9B93CEA204040000000961DA100B1C27A06
Дійсний з 24.11.2026 16:20:27 по 24.11.2027 16:20:26

Центральноукраїнський національний технічний університет
Факультет *Механіко-технологічний*
Кафедра *Кібербезпеки та програмного забезпечення*
Рівень вищої освіти *магістр*
Галузь знань _F_____*"Інформаційні технології"*_____
Спеціальність F7 *"Комп'ютерна інженерія"*
Освітньо-професійна (освітньо-наукова) програма _*"Комп'ютерна інженерія"*_

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
« 1 » вересня 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Килимнику Дмитру Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах*

2. Керівник роботи *Коваленко Олександр Володимирович, доктор технічних наук, професор*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 41-13 від 17.08.2026 року

3. Строк подання студентом роботи до захисту *2.12.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи*: Метою розробки є дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.	*5. Впровадження системи в промислову експлуатацію*
2. Перегляд аналогічних існуючих систем.	*6. Наукова новизна.*
3. Опис і обґрунтування проектних рішень.	*7. Заходи з охорони праці та техніки безпеки.*
4. Етапи програмування системи.	*8. Висновки.*

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Наукова новизна	*1 аркуш*
Структурна схема системи	*1 аркуш*
Функціональна схема системи	*1 аркуш*
Діаграма процесів	*1 аркуш*
Блок-схема алгоритму роботи додатку	*2 аркуша*

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Марченко К.М., к.т.н., доцент	06.10.2026	16.11.2026

8. Дата видачі завдання « 1 » вересня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.10.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.10.2026 р.	
3.	Розробка моделі компонента	20.10.2026 р.	
4.	Розробка структур даних	25.10.2026 р.	
5.	Розробка алгоритмів системи	30.10.2026 р.	
6.	Програмування алгоритмів	10.11.2026 р.	
7.	Розрахунки з охорони праці та техніки безпеки	15.11.2026 р.	
8.	Оформлення ПЗ	17.11.2026 р.	
9.	Попередній захист роботи	2.12.2026 р.	

Дата видачі завдання
« 1 » вересня 2026 р.

Підпис керівника

_____ _____
(прізвище та ініціали)

Завдання прийнято до виконання
« 1 » вересня 2026 р.

Підпис здобувача

_____ _____
(прізвище та ініціали)

АНОТАЦІЯ

Килимник Д.В. Дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах. F7 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Метою розробки є дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Об'єктом дослідження є процес мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Предметом дослідження є методи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Методи дослідження базуються на методах побудови комп'ютерних мереж, методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Visual C++.

Ключові слова: комп'ютерна інженерія, SIEM, моніторинг та оцінка загроз, гібридні хмарно-корпоративні інфраструктури

ABSTRACT

Kylymnyk D.V. Research and Software Implementation of a Network SIEM System for Threat Monitoring and Assessment in Hybrid Cloud-Enterprise Infrastructures. F7 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification thesis for the second (master's) level of higher education, software has been developed for a network SIEM (Security Information and Event Management) system designed to monitor and assess threats within hybrid cloud-enterprise infrastructures.

The objective of this development is the research and software implementation of a network SIEM system for threat monitoring and assessment in hybrid cloud-enterprise infrastructures.

The object of the research is the process of network SIEM-based threat monitoring and assessment in hybrid cloud-enterprise infrastructures.

The subject of the research consists of methods for network SIEM-based threat monitoring and assessment in hybrid cloud-enterprise infrastructures.

The research methodology draws upon techniques for computer network construction, information security theory, mathematical statistics, and software development.

The outcome of the work is the software implementation of a network SIEM system for threat monitoring and assessment in hybrid cloud-enterprise infrastructures.

During the development of the software model, an analysis of existing hardware and software tools was conducted. All components of the developed software are described in detail. A user-friendly interface has been developed. Instructions for using the software tools are provided.

The program can be used on PCs running the Windows 10/11 operating system.

The program was developed in the Visual C++ environment.

Keywords: computer engineering, SIEM, threat monitoring and assessment, hybrid cloud-enterprise infrastructures

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	94	–	
2	А4	Робоча програма	42	–	Додаток А
		Графічні документи			
3	А4	Наукова новизна	1	–	
4	А4	Структурна схема	1	–	
5	А4	Функціональна схема роботи системи	1	–	
6	А4	Діаграма взаємодії процесів	1	–	
7	А4	Блок-схема основної програми	1	–	
8	А4	Блок-схема роботи підпрограми	1	–	

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 9
ВСТУП..... 10
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 13
1.1 Призначення системи..... 13
1.2 Область застосування 14
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 16
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 16
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 34
2.3 Розгорнута постановка завдання 35
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 37
3.1 Опис функціонування системи 37
3.2 Розробка структурної схеми..... 40
3.3 Розробка функціональної схеми 45
3.4 Розробка діаграми процесів 46
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 48
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 48
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 70
6 НАУКОВА НОВИЗНА 75

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 76
7.1 Вступ 76
7.2 Аналіз умов праці ІТ-працівників 77
7.3 Техніка безпеки та протипожежна профілактика 81
7.4 Розробка заходів з охорони праці 83
7.5 Висновки до розділу 84
8 ОСНОВНІ ВИСНОВКИ 85
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 87

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЛОМ	–	локальна обчислювальна мережа
MME	–	міжмережні екрани
ATM	–	асинхронний режим передачі
BSD	–	адаптована для Internet реалізація операційної системи UNIX
ICMP	–	міжмережний протокол управляючих повідомлень
IP	–	Internet Protocol – міжмережний протокол
NFS	–	мережна файлова система
PPP	–	протокол передачі від точки до точки
RFC	–	опис набору протоколів Internet
RPC	–	віддалений виклик процедури
SLIP	–	міжмережний протокол для послідовного каналу
SMTP	–	Simple Mail Transfer Protocol – простий протокол передачі пошти
TCP	–	Transmission Control Protocol – протокол управління передачею
UDP	–	User Datagram Protocol – протокол користувальницьких датаграм
UNIX	–	багатозадачна операційна система
UTP	–	незахищена вита пара
URL	–	уніфікований покажчик інформаційного ресурсу

ВСТУП

Актуальність теми. SIEM (керування інформацією та подіями безпеки) – це централізована платформа, яка збирає, нормалізує, співвідносить та аналізує події безпеки в усьому підприємстві. Термін зараз охоплює все: від традиційних механізмів агрегації журналів до платформ виявлення на основі штучного інтелекту з вбудованими функціями SOAR, UEBA та аналітикою загроз у режимі реального часу.

Застаріле розгортання SIEM розглядає кожен інструмент безпеки як окреме джерело даних, генеруючи паралельні потоки сповіщень, які потребують ручної кореляції між консолями. Традиційні рівні моніторингу MSSP доповнюють це без додавання глибини розслідування. Платформи XDR від CrowdStrike та Palo Alto консолідують виявлення та реагування в межах стеку одного постачальника, що є реальним операційним вигодою для організацій, які вже стандартизовані на цьому постачальнику, та справжнім обмеженням для організацій, які його не мають.

Розрив між спрацьовуванням сповіщення та виявленням загрози – це місце, де концентрується операційний ризик, незалежно від того, яка категорія знаходиться на платформі, що генерує сповіщення. Усунення цього розриву є питанням як персоналу та процесу, так і платформи, тому керовані послуги SIEM існують як окремий рівень від самої ліцензії платформи.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

– Дослідження системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

– Програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Об’єктом дослідження є процес мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Предметом дослідження є методи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Методи дослідження базуються на методах побудови комп’ютерних мереж, методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

– Розроблено вітчизняний продукт мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVIII науково-технічній конференції здобувачів вищої освіти «Наука-виробництву», основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №17.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Технічні відмінності між SIEM, XDR, SOAR та управлінням журналами мають значення для того, що кожен інструмент може обробляти та співвідносити. Практичне питання для більшості покупців вужче: з якою з цих п'яти категорій, або з якої категорії, або з якої комбінації категорій, команда, яка буде нею керувати, може працювати цілодобово.

Платформа з найглибшою логікою виявлення у цьому списку все ще залежить від того, чи хтось її налаштовує, спостерігає за нею та реагує на те, що вона виявляє.

SIEM для команд середнього бізнесу

Більшість платформ, порівняних вище, створені та оцінені для корпоративних покупців із виділеними бюджетами на безпеку та відповідним персоналом.

Команда середнього бізнесу (від трьох до дванадцяти осіб, що охоплюють всю поверхню атаки) оцінює ті самі платформи з урахуванням набагато жорсткіших обмежень: відсутність виділеного SOC, відсутність вільного персоналу для тривалого розгортання та бюджет, який має витримати перевірку з боку когось, хто не працює в сфері безпеки.

Навіть дві платформи, ціна яких найближча до цієї реальності, – безкоштовне самокероване ядро Wazuh та позиціонування Graylog з економною командою, – вирішують лише питання вартості ліцензії. Жодна з них не вирішує питання про те, хто налаштовує платформу, стежить за нею після робочого часу або хто володіє рівнем хибнопозитивних результатів, коли початковий ентузіазм від розгортання зникає. Платформа, яку команда з трьох осіб не може налаштувати, використовує невикористаний набір функцій, незалежно від того, що вона може зробити в таблиці порівняння.

Саме цей операційний пробіл є тим місцем, де керований рівень змінює розрахунок. Чотириосібна IT-команда в кредитній спілці підходить цьому покупцю, і тематичне дослідження SIEM кредитної спілки UnderDefense показує, як це виглядає на практиці: приблизно 200 контрольованих кінцевих точок, SIEM, додана поверх існуючого розгортання CrowdStrike Falcon Complete.

Завдяки співпраці покриття було розширено з 8×5 до 24×7, включаючи вихідні та святкові дні, що надавалося як керований рівень, доданий до існуючої команди з чотирьох осіб.

Співпраця також виявила неправильну конфігурацію брандмауера, яку пропустили існуючі інструменти, і яку виправили до того, як її можна було використати. Менеджер з IT-операцій кредитної спілки безпосередньо описав процес: «Процес адаптації пройшов гладко та швидко».

Яку б платформу команда середнього бізнесу не обере з цього списку, операційне питання «хто дивиться це о 2-й годині ночі, а хто зменшить рівень хибнопозитивних результатів протягом наступних тижнів» вирішує результат більше, ніж сама ліцензія.

1.2 Область застосування

Ринок SIEM у 2026 році консолідується навколо меншої кількості постачальників та іншої архітектури. Gartner оцінив 17 платформ у «Магічному квадранті 2025» порівняно з 22 у 2024 році, і більшість із них зараз лідирують у використанні можливостей штучного інтелекту у своєму маркетингу.

Змінюється архітектура. SIEM-платформи поглинають інфраструктуру озер даних, щоб вирішити проблему обмежень вартості прийому та зберігання даних, які робили старі розгортання дорогими у великих масштабах.

Агенти штучного інтелекту для сортування та виявлення небезпек переходять від доповнення до ядра. Межа між SIEM, XDR та SOAR розмивається до такої міри, що категорії мають менше значення, ніж те, що

робить дане розгортання на 90-й день. Microsoft Sentinel, Cortex XSIAM та CrowdStrike Falcon Next-Gen SIEM – це три постачальники, які сходяться на одному шляху з трьох різних початкових точок. Нова хвиля інструментів SIEM на основі штучного інтелекту просуває ту саму конвергенцію ззовні.

Продукт, який робить SOC тихішим, не покращуючи покриття, може залишити основну проблему невирішеною. Марті застерігає, що такий продукт міг «перетворити видимі хибнопозитивні результати на невидимі хибнонегативні», відмінність, яку не буде показано в жодному демонстраційному матеріалі на панелі інструментів.

Команди, які отримують цінність від покращень на рівні штучного інтелекту, – це ті, які мають стабільне операційне покриття. SIEM, яка видає менше сповіщень, означає менше, якщо команда, яка працює над цими сповіщеннями, вже перевантажена. Саме цю прогалину заповнює керований сервіс SIEM: операційний рівень, який визначає, чи працює платформа на повну потужність, чи на тій частині, яку може покрити команда з обмеженими можливостями.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

Сторінки постачальників продуктів SIEM представляють можливості у вигляді списку функцій. Записи нижче представляють їх як операційне питання: яка команда може це запустити, на якій інфраструктурі та коли платформа почне окуповувати свою вартість.

1. Керована SIEM-система UnderDefense + агентний ШІ SOC: найкращий варіант для впровадження вже існуючої SIEM-системи

UnderDefense працює як незалежний від постачальника рівень над будь-якою комбінацією SIEM або XDR, отримуючи сигнали від Splunk, Sentinel, Elastic, CrowdStrike, Okta та інших інструментів, що вже використовуються, через вбудовані інтеграції. Платформа зіставляє дані виявлення з цих джерел в єдиний контекст розслідування, що усуває необхідність переходу між окремими консолями для кожного джерела.

Відмінність від окремої платформи полягає в тому, що відбувається після спрацьовування сповіщення. SIEM виявляє підозрілий вхід і позначає його для перевірки. UnderDefense Agentic AI SOC досліджує сповіщення, аналітик підтверджує активність безпосередньо з користувачем через Slack або Teams, а стримування відбувається в рамках того ж робочого процесу, тому внутрішня команда отримує інформацію про вирішений інцидент.

Що робить ШІ:

– Центр інформаційних технологій Agentic досліджує кожне сповіщення в середньому за 2 хвилини, при цьому штучний інтелект займається сортуванням, збагаченням та початковим аналізом, тоді як аналітики-люди приймають остаточне рішення щодо ескалації та реагування.

– Рівень штучного інтелекту не залежить від постачальника: він працює на будь-якій платформі, яку вже використовує клієнт, без необхідності міграції платформи для використання цієї можливості.

– Локальне розгортання Agentic AI SOC доступне для регульованих середовищ, де хмарна обробка на основі штучного інтелекту є обмеженням відповідності, зберігаючи обробку на основі штучного інтелекту всередині клієнтського середовища без жодної телеметрії, яка б його залишала.

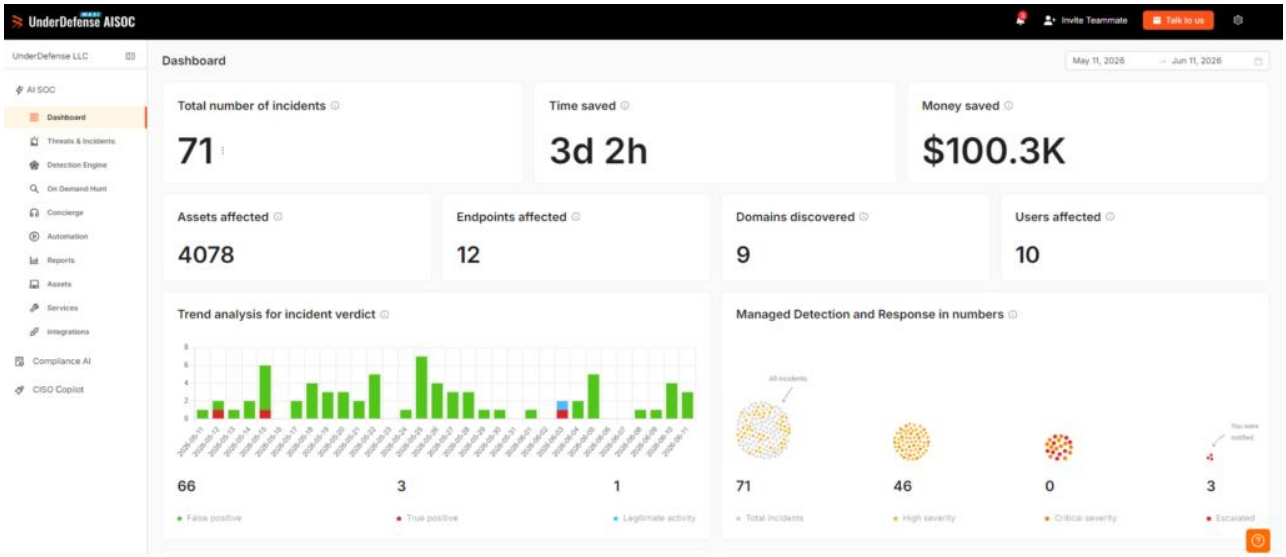


Рисунок 2.1 – Інтерфейс користувача UnderDefense

Сигнали відповідності стеку:

– Чудово підходить для організацій з існуючими інвестиціями в SIEM, яким потрібне стабільне операційне покриття без відповідного розширення внутрішнього персоналу.

– Чудово підходить для регульованих галузей (фінансові послуги, охорона здоров'я, урядові установи), де локальне розгортання SOC на базі штучного інтелекту відповідає вимогам щодо жорсткого зберігання даних.

– Слабше підходить для організацій з повністю укомплектованим внутрішнім центром захисту даних (SOC), який цілодобово охоплює всю поверхню виявлення та не має операційних прогалин, які потрібно заповнювати.

Коли складати короткий список / Коли пропускати:

Додайте короткий список, якщо в організації є SIEM, але команда, яка її охоплює, перевантажена, непослідовна або обробляє менше, ніж повна поверхня виявлення. Додайте короткий список, якщо вимоги до відповідності роблять обробку SOC лише в хмарі за допомогою штучного інтелекту непрацездатною. Пропустіть, якщо організація створює повністю власну функцію безпеки з нуля та має достатньо персоналу для її цілодобового обслуговування без зовнішнього операційного рівня.

2. Splunk Enterprise Security: найкращий варіант для великих підприємств, яким потрібна величезна гнучкість екосистеми

Splunk Enterprise Security – це SIEM-платформа, створена для великих, складних середовищ, яким потрібно консолідувати виявлення, розслідування та реагування на великі обсяги неоднорідних даних. Вона працює як Splunk Cloud або як самостійно керована локальна платформа Splunk Enterprise, включаючи розгортання з ізоляцією.

Що робить ШІ:

– AI Assistant від Splunk постачається як у версіях Essentials, так і Premier і дозволяє аналітикам робити запити природною мовою без написання SPL.

– Тільки в Premier та лише на Splunk Cloud працюють два агенти: сортування сповіщень зі зрозумілим поясненням кожного рейтингу та скасування шкідливого програмного забезпечення, яке розбиває скрипти рядок за рядком та виявляє індикатори компрометації.

У пакеті Essentials не враховуються обидва агенти. UEBA, SOAR та Automated Threat Analysis доступні лише для учасників Premier. Перш ніж порівнювати можливості, перевірте, який рівень ви обираєте для ціноутворення. Розрив між тим, що зазначено на сторінці продукту, та тим, що пропонує Essentials, достатньо великий, щоб змінити оцінку.

Сигнали відповідності стеку:

Рідний для хмарних середовищ та самостійно керований, включаючи ізоляцію.

– Сильно підходить, якщо організація вже використовує інструменти спостереження Splunk або IT-операцій. Перевага екосистеми реальна.

– Слабша відповідність, якщо стек в основному складається з Microsoft або CrowdStrike, де Sentinel або Falcon Next-Gen SIEM інтегруватимуться з меншими труднощами.

Коли складати короткий список / Коли пропускати:

Створіть короткий список, якщо вимога щодо розгортання з обмеженим доступом є жорсткою, або якщо метою є консолідація SIEM, SOAR та UEBA в рамках одного контракту. Пропустіть, якщо команда складається з менше ніж п'яти осіб, якщо обсяг споживання непередбачуваний або якщо обговорення бюджету не може досягти рівня Premier.

3. Microsoft Sentinel: найкращий варіант для організацій, орієнтованих на Microsoft та хмарні технології

Microsoft Sentinel – це хмарна SaaS-система SIEM, вбудована в портал Azure та Microsoft Defender, яка отримує дані з багатохмарних та локальних джерел через понад 400 конекторів. Sentinel працює виключно в інфраструктурі Azure. Організаціям з вимогами до місця проживання даних, що перешкоджають обробці даних, розміщеній в Azure, потрібно буде шукати інші варіанти в цьому списку.

Що робить ШІ:

– Security Copilot здійснює розслідування та допомогу у реагуванні природною мовою.

– Вбудовані UEBA та SOAR постачаються з базовим продуктом, без необхідності оновлення рівня.

– Інструмент міграції за допомогою штучного інтелекту конвертує правила виявлення зі Splunk або QRadar з перевіркою перед розгортанням. Це практична можливість для організацій, які активно відходять від конкурента.

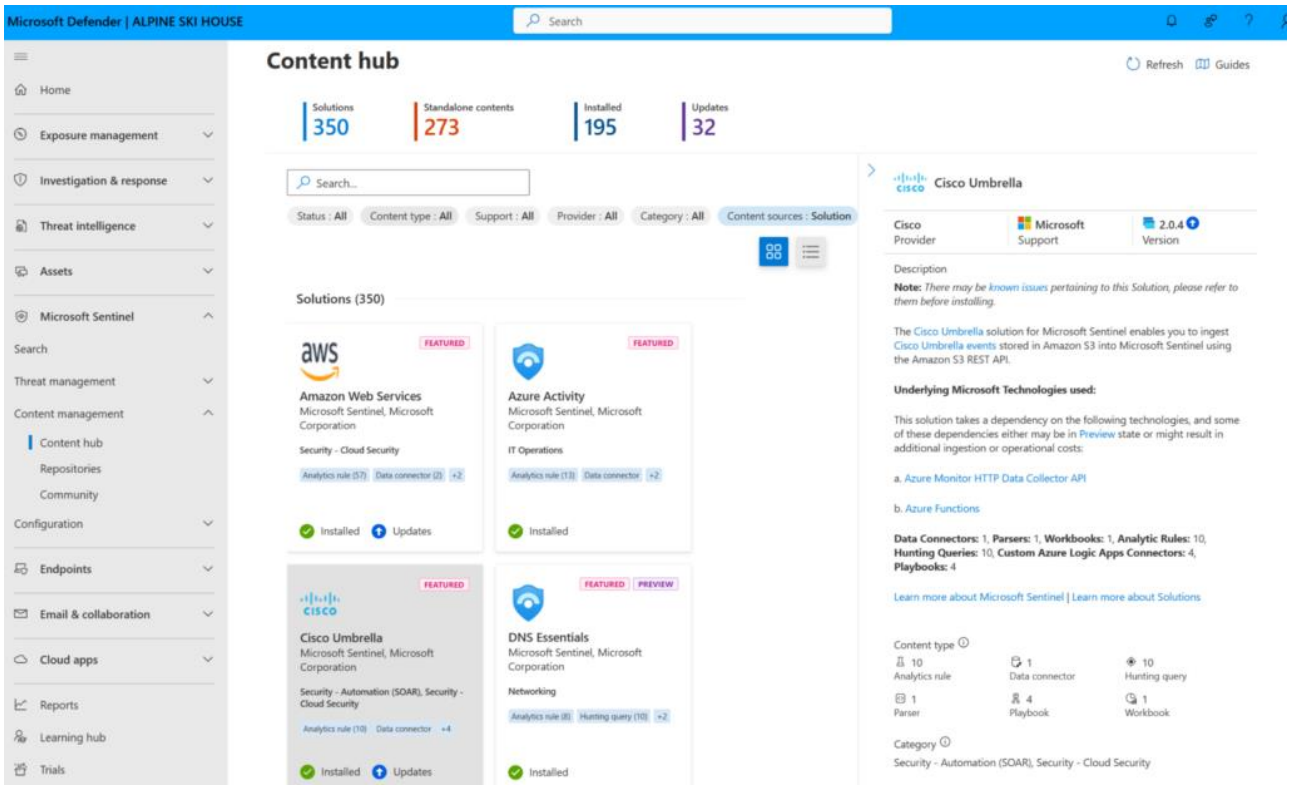


Рисунок 2.2 – інтерфейс користувача Microsoft Sentinel

Сигнали відповідності стеку:

– Чудово підходить для організацій, які вже використовують Microsoft 365, Azure або Defender, де власна інтеграція усуває накладні витрати на конектори та складність ліцензування.

– Слабше підходить для організацій, які переважно використовують інфраструктуру AWS або GCP, де міжхмарне отримання даних збільшує затримку та витрати.

Коли складати короткий список / Коли пропускати:

Виберіть варіант, якщо організація орієнтована на Microsoft та використовує хмарні технології, або перебуває в процесі міграції зі Splunk чи QRadar. Пропустіть, якщо вимоги до місця проживання даних перешкоджають обробці даних, розміщених в Azure, або якщо самостійне розгортання є обов'язковою вимогою.

4. Elastic Security: найкращий варіант для команд, орієнтованих на відкрите програмне забезпечення, які прагнуть прозорої з точки зору витрат SIEM

Elastic Security – це SIEM-платформа, побудована на Elastic Stack, яка поєднує в собі прийом журналів, поведінкове виявлення та автоматизоване реагування в одному механізмі. Вона працює за трьома шляхами розгортання: безсерверне, розміщене на Elastic Cloud або повністю самокероване, включаючи суверенну хмару, локальні та ізольовані середовища. Ціноутворення залежить від обсягу обчислень та сховища, що є структурною відмінністю від ліцензування на кінцеву точку, що робить вартість більш передбачуваною зі зростанням обсягу даних.

Що робить ШІ:

– Еластичні ринки використовують «операції безпеки агентів», де автономні агенти обробляють повний життєвий цикл від отримання даних до відповіді, а аналітики займаються оцінкою та схваленням.

– Архітектура не залежить від моделі: організації можуть підключати керовані моделі Elastic, OpenAI, Anthropic, Gemini або локальну модель з відкритим кодом.

– Ціноутворення залежить від використаних обчислювальних ресурсів та обсягу сховища, що є структурним відхиленням від моделей ліцензування для кожної кінцевої точки.

Сигнали відповідності стеку:

– Чудово підходить для команд, які хочуть запровадити власну LLM-методику замість моделі, обраної постачальником.

– Сильна відповідність, коли ціноутворення на основі обчислень краще відповідає структурі бюджету на безпеку, ніж ліцензування на кінцеву точку.

– Слабше підходить для команд без інженерних можливостей для налаштування та налаштування самостійно керованого розгортання.

Коли складати короткий список / Коли пропускати:

Додайте короткий список, якщо потрібне розгортання з обмеженим доступом і має значення гнучкість LLM. Додайте короткий список, якщо команда має інженерну підготовку для самостійного керування та хоче прозоре ціноутворення. Пропустіть, якщо команді потрібне кероване розгортання з низькою конфігурацією з першого дня.

5. CrowdStrike Next-Gen SIEM: найкращий варіант для клієнтів екосистеми CrowdStrike, яким потрібен петабайтний обсяг обробки даних

CrowdStrike Next-Gen SIEM – це хмарний модуль всередині платформи Falcon, що постачається на тій самій легкій архітектурі датчиків, яку клієнти CrowdStrike вже використовують для захисту кінцевих точок. Він доступний лише за принципом SaaS. Самостійне розгортання – це окремий продукт, Falcon LogScale, тому організації з локальними вимогами оцінюють LogScale окремо.

Що робить ШІ:

– «Charlotte Agentic SOAR» займається керованою автоматизацією робочих процесів реагування.

– Агент-оркестратор координує роботу агентів-спеціалістів домену, які працюють паралельно. Це власне пояснення CrowdStrike, чому це працює швидше, ніж послідовне виконання плейбуку.

– Твердження про «пошук у 150 разів швидший» завдяки архітектурі без індексів згадане на власній сторінці CrowdStrike як результат дослідження окремого клієнта; перевірте його за допомогою розкритої повторюваної методології, перш ніж використовувати його у внутрішньому бізнес-кейсі.

Сигнали відповідності стеку:

– Чудово підходить для організацій, які вже використовують Falcon для захисту кінцевих точок: архітектура з одним датчиком та однією консоллю усуває накладні витрати на інтеграцію, пов'язані з додаванням окремого постачальника SIEM.

– Слабше підходить для організацій, що використовують інший EDR, де основна перевага інтеграції зникає, а розгортання лише в хмарі може стати обмеженням.

Коли складати короткий список / Коли пропускати:

Виберіть варіант, якщо організація є існуючим клієнтом CrowdStrike Falcon і хоче мати можливості SIEM в одній консолі. Пропустіть цей варіант, якщо потрібне локальне або ізольоване розгортання; у цьому випадку оцініть Falcon LogScale. Організації, які не використовують CrowdStrike EDR, все ще можуть придбати NG-SIEM окремо, хоча перевага використання одного датчика зникає.

6. Palo Alto Cortex XSIAM: найкращий варіант для підприємств, які прагнуть консолідації SIEM, XDR та SOAR

Cortex XSIAM – це хмарна SOC-платформа від Palo Alto Networks, створена для заміни традиційних стеків SIEM, XDR та SOAR єдиним консолідованим продуктом. XSIAM розроблено з нуля для підприємств, які хочуть відмовитися від багатоточкових рішень та виконувати виявлення, розслідування та реагування з однієї консолі.

Що робить ШІ:

– Palo Alto стверджує, що понад 2900 моделей машинного навчання безперервно працюють на кінцевих точках, в мережі, ідентифікаторі та хмарній телеметрії в одному конвеєрі.

– «AgentiX» надає бібліотеку спеціалізованих агентів на базі штучного інтелекту, які маршрутизують сортування першого рівня зі швидкістю машини та позначають рішення, що потребують оцінки аналітика.

– XSIAM об'єднує телеметрію SIEM, XDR та SOAR в один шар даних, тому моделі корелюють між усіма типами сигналів одночасно без ручної перехресної кореляції.

Сигнали відповідності стеку:

– Чудово підходить для підприємств, які вже використовують Palo Alto NGFW або Prisma, де основною метою є консолідація платформи між SIEM, XDR та SOAR.

– Слабше підходить для організацій, що використовують гетерогенний стек без значного охоплення території Пало-Альто.

Коли складати короткий список / Коли пропускати:

Виберіть варіант, якщо метою є консолідація SIEM, XDR та SOAR в єдину платформу, і організація має бюджет для взаємодії на рівні підприємства. Пропустіть варіант, якщо організація не має існуючої присутності в Пало-Альто, і метою є консолідація між постачальниками. Глибина інтеграції платформи найсильніша в межах її власної екосистеми та менша, коли існуючий стек побудований навколо різних інструментів.

7. IBM QRadar SIEM: найкращий для регульованих галузей з глибокими вимогами до локальної інфраструктури та відповідності

IBM QRadar – єдина платформа у цьому списку без хмарного SaaS-проекту. Вона розгортається як апаратне забезпечення або віртуальні пристрої локально, з опцією керованого IBM сервісу через X-Force Threat Management Services для організацій, яким потрібен операційний рівень, не запускаючи його самостійно.

IBM продала QRadar SaaS компанії Palo Alto Networks у 2024 році, що залишає QRadar SIEM від IBM як локальний продукт з опцією управління IBM.

Що робить ШІ:

– UEBA виявляє аномальну поведінку користувачів та сутностей у всьому масиві даних.

– Вбудована підтримка правил Sigma означає, що бібліотека виявлення підтримується спільнотою та є портативною, без прив'язки до власного формату IBM.

– Фреймінг ШІ є більш стриманим, ніж у більшості інших галузей: немає заяв про агентну автоматизацію, немає мови автономного реагування. Для

регульованих середовищ, обережних щодо автономних дій на локальному рівні, це обмеження читається як функція.

Сигнали відповідності стеку:

– Чудово підходить для великих регульованих підприємств (фінансові послуги, уряд, охорона здоров'я), де обов'язкова локальна обробка даних, а штрафи за кожен гігабайт даних є реальною проблемою для бюджету.

– Слабше підходить для хмарних організацій або команд, яким потрібен швидкий шлях розгортання. Локальна модель QRadar має вищі накладні витрати на налаштування та обслуговування, ніж будь-яка хмарна платформа з цього списку.

Коли складати короткий список / Коли пропускати:

Додайте короткий список, якщо локальне розгортання є вимогою відповідності, а витрати на використання кожного гігабайта даних є відомим бюджетним обмеженням. Пропустіть, якщо організація використовує хмарні технології, якщо команді бракує інфраструктурних потужностей для локальних пристроїв або якщо швидкість розгортання є основним фактором.

8. Exabeam New-Scale Fusion: найкращий варіант для організацій, що в першу чергу орієнтовані на UEBA та зосереджені на поведінковій аналітиці

Exabeam New-Scale Fusion – це хмарне рішення, що поєднує SIEM та поведінкову аналітику в одній платформі. Для організацій, яким потрібне саме локальне розгортання, Exabeam пропонує LogRhythm як окрему лінійку продуктів.

Що робить ШІ:

– «Агенти Exabeam Nova» автоматизують рутинне сортування, генерують зведення випадків та обробляють перетворення правил виявлення.

– Динамічна оцінка ризиків на основі UEBA коригує пріоритет загроз відповідно до поведінкових базових значень, минаючи пороги статичних правил.

– «Аналіз поведінки агентів» розширює видимість агентів ШІ в середовищі. Це важливо для організацій, які використовують автономні

інструменти ШІ внутрішньо, що створює поверхню внутрішніх загроз, окрему від поведінки користувачів-людей.

Сигнали відповідності стеку:

– Чудово підходить для організацій, де внутрішні загрози та ризики, пов'язані з ідентифікацією, є основним пріоритетом виявлення.

– Чудово підходить, якщо команда використовує або планує використовувати внутрішніх агентів штучного інтелекту та хоче розширити моніторинг поведінки, щоб охопити їх.

– Слабше підходить для організацій, яким потрібне локальне розгортання, оскільки Fusion SIEM доступний лише в хмарі та не має гнучкості розгортання в цій лінійці продуктів.

Коли складати короткий список / Коли пропускати:

Виберіть варіант, якщо глибина UEBA та виявлення внутрішніх загроз є основними критеріями оцінки, або якщо моніторинг агентів штучного інтелекту є короткостроковою вимогою. Пропустіть, якщо потрібне локальне розгортання; оцініть LogRhythm, якщо набір функцій Exabeam підходить, але хмарне розгортання – ні.

9. Securonix Unified Defense SIEM: найкращий варіант для великих підприємств зі складними сценаріями внутрішніх загроз

Securonix працює в хмарному середовищі на однорівневій архітектурі, що об'єднує SIEM, UEBA, SOAR та аналітику загроз. Опція «принеси свою власну хмару» на Snowflake або AWS дозволяє організаціям зберігати дані безпеки всередині інфраструктури, яку вони вже контролюють.

Що робить ШІ:

– «Agentic Mesh» забезпечує автоматизацію за допомогою зрозумілих інструкцій штучного інтелекту на кожному кроці; аналітику надається пояснення кожної автоматизованої дії.

– «Сем, аналітик ШІ SOC» автоматично виконує збагачення, сортування та реагування.

– 365 днів завжди актуальних, доступних для пошуку даних на одному рівні – це конкретна операційна відмінність від платформ, які розміщують старі журнали у повільнішому сховищі.

Сигнали відповідності стеку:

– Чудово підходить для великих підприємств, де сценарії внутрішніх загроз є складними, а глибина UEBA має значення.

– Сильна відповідність там, де суверенітет даних вимагає зберігання даних безпеки всередині хмарної інфраструктури, контрольованої організацією.

– Слабше підходить для команд середнього бізнесу без спеціальної функції SOC. Глибина охоплення Securonix SIEM, UEBA, SOAR та TIP вимагає аналітиків, які можуть впровадити всю платформу. Команда, що працює на частковій потужності, отримує лише частку цінності, яку пропонує архітектура.

Коли складати короткий список / Коли пропускати:

Створіть короткий список, якщо метою є консолідація SIEM, UEBA, SOAR та TIP, або якщо зберігання даних, що постійно оновлюються, понад 90 днів є вимогою до дотримання нормативних вимог або операційною вимогою. Пропустіть, якщо команді безпеки не вистачає персоналу для роботи з єдиним стеком SIEM, UEBA, SOAR та TIP у всьому наборі можливостей. Цінність платформи масштабується залежно від аналітиків, які її використовують, і команда з обмеженим ресурсом не використовуватиме те, для чого створено Securonix.

10. SentinelOne Singularity AI SIEM: найкращий варіант для організацій, які бажають об'єднати EDR та SIEM в одному агенті

Singularity AI SIEM – це хмарна платформа, створена для «обробки та аналізу великих обсягів даних безпеки» в межах тієї ж платформи, на якій працює захист кінцевих точок SentinelOne. Суть полягає в архітектурному підході: один агент, одна консоль, що запускає SIEM та EDR разом, тому покупець не просить двох постачальників змусити двох окремих агентів співпрацювати.

Що робить ШІ:

– «Фіолетовий ШІ» займається розслідуваннями, перетворюючи необроблені дані журналів та сповіщень на структуровані описи справ, на основі яких аналітики можуть діяти, не створюючи запитів з нуля.

– «Конвеєри даних сингулярності» нормалізують та збагачують дані в момент їх отримання: власна відмінність SentinelOne від традиційних SIEM, які зосереджують штучний інтелект на рівні сповіщення.

– Рівень Enterprise включає «Agentic AI SOC Analyst», який виконує автоматизоване сортування від отримання даних через розслідування та рекомендації щодо утилізації; на двох нижчих рівнях це платне доповнення.

Сигнали відповідності стеку:

– Чудово підходить для організацій, які вже використовують SentinelOne для захисту кінцевих точок, де консолідація SIEM в одну платформу усуває постачальника та канал передачі даних.

– Слабше підходить для організацій з гетерогенним середовищем кінцевих точок або навмисною архітектурною перевагою для зберігання SIEM та EDR у окремих постачальників.

Коли складати короткий список / Коли пропускати:

Виберіть варіант, якщо організація вже є клієнтом SentinelOne і метою є консолідація. Пропустіть, якщо розділення постачальників EDR та SIEM є навмисним архітектурним вибором або якщо потрібне локальне розгортання.

11. Командування інцидентами Rapid7: найкраще для команд середнього бізнесу, які шукають вбудовану UEBA з SOAR

Rapid7 Incident Command (раніше InsightIDR) – це хмарна платформа для виявлення та реагування на події з вбудованими UEBA та SOAR. Її рівень штучного інтелекту має три названі компоненти: робочі процеси розслідування за допомогою агентного штучного інтелекту, сортування та утилізація сповіщень за допомогою штучного інтелекту, а також пошук у журналах природною мовою.

Що робить ШІ:

– «Робочі процеси розслідування агентів зі штучним інтелектом» запускають автоматизовані послідовності розслідувань, коли спрацьовує сповіщення, зменшуючи кількість ручних кроків між виявленням та контекстом аналітика.

– «Сортування та утилізація тривог за допомогою штучного інтелекту» обробляє початкову класифікацію ступеня тяжкості, перш ніж тривога надійде до аналітика.

– Пошук у журналах природною мовою усуває бар'єр мови запитів для команд без спеціалізованих мисливців за загрозами.

Сигнали відповідності стеку:

– Чудово підходить для команд SOC середнього рівня, яким потрібні вбудовані UEBA та SOAR, з ціноутворенням на основі активів, що дозволяє уникнути несподіваних витрат протягом місяців з великим обсягом обробки даних.

– Слабше підходить для великих підприємств зі складними середовищами з великим обсягом обробки, де платформи корпоративного відстеження з цього списку мають більшу глибину виявлення.

Коли складати короткий список / Коли пропускати:

Виберіть варіант, якщо команда знаходиться на середньому рівні зрілості, працює в хмарі та потребує UEBA та SOAR без високої складності розгортання. Пропустіть, якщо потрібне локальне розгортання або якщо масштаб середовища перевищує те, що зазвичай покривають середні цінові рівні.

12. Stellar Cyber: найкращий варіант для постачальників послуг з управління ресурсами (MSSP) та команд Lean SOC, яким потрібна автоматизація для кількох орендарів

Stellar Cyber розгортається як у локальних, так і в хмарних середовищах під назвою «Багатошаровий штучний інтелект» – брендований стек, що включає «Слідчого за допомогою штучного інтелекту», «Автоматичне сортування агентів», безперервне пошук загроз за допомогою штучного інтелекту та

реагування на інциденти за допомогою штучного інтелекту, що накладається на вбудований UEBA та поєднання статичних правил з контрольованим та неконтрольованим машинним навчанням.

Що робить ШІ:

– «Багатошаровий штучний інтелект» охоплює автоматизоване сортування, безперервне виявлення загроз та реагування на інциденти за допомогою штучного інтелекту в рамках однієї пакетної ліцензії.

– UEBA працює разом зі статичними правилами та як контрольованим, так і неконтрольованим машинним навчанням, гібридним стеком виявлення на трьох рівнях.

– Набір можливостей постачається за однією ліцензією.

Сигнали відповідності стеку:

– Чудово підходить для постачальників послуг з управління ресурсами (MSSP) та постачальників послуг з керуванням ресурсами (MDR), яким потрібна багатокористувацька архітектура для обслуговування кількох клієнтських середовищ з одного розгортання.

– Чудово підходить для підприємств, яким потрібна єдина пакетна ліцензія, що охоплює всі можливості, обходячи модульне ціноутворення, де можливості залежать від рівнів підвищення.

– Слабше підходить для організацій, які надають пріоритет довговічності постачальників та широкій екосистемі попередньо створеної інтеграції.

Коли складати короткий список / Коли пропускати:

Створіть короткий список, якщо потрібна багатокористувацька архітектура або якщо єдина повна ліцензія є кращою комерційною моделлю. Пропустіть, якщо зрілість постачальника та широта екосистеми є основними критеріями оцінки поряд з можливостями.

13. Sumo Logic Cloud SIEM: найкращий варіант для малих та середніх команд DevOps та SecOps

Sumo Logic Cloud SIEM – це виключно хмарна платформа, яку на власному сайті описують як «масштабовану багатокористувацьку платформу»,

побудовану на основі «розподіленої архітектури», яка, за словами постачальника, ніколи не втрачає дані. Sumo Logic не пропонує самостійно керованих або локальних варіантів, що виключає її для будь-якого покупця із суворими вимогами щодо місця розташування даних.

Що робить ШІ:

– «Аналітичний агент SOC» аналізує вхідне сповіщення, оцінює пов’язану активність у всьому масиві даних та виносить вердикт, підтверджений доказами, з обґрунтуванням; на сайті Sumo Logic зазначається скорочення MTTR до 75%, без зазначення масштабу чи базового рівня.

– UEBA визначає базові моделі поведінки за лічені хвилини, згідно з інформацією на сторінці продукту самого постачальника.

– Понад 900 готових правил виявлення постачаються з активацією SIEM, а також дослідник покриття для аналізу прогалин.

Сигнали відповідності стеку:

– Чудово підходить для малих та середніх команд DevOps та SecOps, яким потрібне керування журналами та аналітика безпеки в одному інтерфейсі. Essentials не включає SIEM, тому можливості SIEM знаходяться на вищому рівні.

– Слабше підходить для великих підприємств або організацій з вимогами до зберігання даних, де розгортання лише в хмарі та модель ціноутворення на основі кредитів створюють обмеження.

Коли складати короткий список / Коли пропускати:

Виберіть варіант, якщо команда невелика або середня, використовує хмарні технології та потребує SIEM разом із інструментами спостереження DevOps на одній платформі. Пропустіть цей варіант, якщо потрібне локальне розгортання або якщо дані безпеки мають залишатися поза хмарним середовищем, керованим постачальником.

14. Wazuh: найкращий варіант для бюджетних команд середнього бізнесу, які готові до самостійного управління

Wazuh – це платформа безпеки з відкритим кодом, що поєднує SIEM, XDR та виявлення кінцевих точок в архітектурі єдиного агента. Вона охоплює аналіз журналів, моніторинг цілісності файлів, виявлення вразливостей та реагування на інциденти в хмарних, локальних та гібридних середовищах. Самостійне розгортання (агент, сервер, індексатор та панель інструментів) працює на інфраструктурі, яку контролює організація, без залежності від постачальника щодо основного рівня виявлення та кореляції.

Що робить ШІ:

– Аналітик безпеки ШІ – це запланований звіт, що надсилається електронною поштою, доступний лише у Wazuh Cloud; безкоштовне самокероване ядро його не надає.

– Виявлення працює на основі кореляції на основі правил з відображенням MITRE ATT&CK та кореляцією CVE, що вужче, ніж мова агентної автоматизації в комерційних платформах, описаних вище.

– Компроміс прямий: для роботи зі штучним інтелектом потрібне хмарне рішення Wazuh Cloud за опублікованою ціною від 571 долара на місяць для обслуговування до 100 агентів; використання безкоштовного ядра означає керування виявленням без доповнення аналітика на основі штучного інтелекту.

Сигнали відповідності стеку:

– Чудово підходить для бюджетних команд середнього бізнесу з інженерними можливостями для розгортання, налаштування та підтримки самостійно керованої SIEM.

– Чудово підходить для організацій, яким потрібна безкоштовна база з можливістю переходу на керований хмарний рівень у міру розвитку функції безпеки.

– Слабше підходить для команд без виділених інженерних ресурсів для управління самостійно розміщеним розгортанням або для організацій, яким

потрібна підтримка корпоративного рівня та угоди про рівень обслуговування з першого дня.

Коли складати короткий список / Коли пропускати:

Створіть короткий список, якщо бюджет є основним обмеженням і команда має можливості самостійно керувати, або якщо початок на безкоштовній основі та масштабування до платного рівня з часом відповідає тому, як зростатиме бюджет на безпеку. Пропустіть, якщо команді бракує можливостей для підтримки самостійного розгортання або якщо можливості штучного інтелекту є обов'язковою вимогою з першого дня.

15. Graylog Security: найкращий варіант для команд безпеки, які переросли управління журналами

Graylog працює в хмарі, локально або гібридному розгортанні, за словами самого постачальника, з «повним паритетом функцій у кожному розгортанні» та «без примусових обмежень SaaS». Graylog Open, безкоштовний рівень з доступним вихідним кодом, знаходиться під платними версіями без обмеження обсягу, що є постійним безкоштовним рівнем.

Що робить ШІ:

– Виявлення аномалій за допомогою машинного навчання виявляє поведінкові відхилення без ручного написання правила для кожного шаблону.

– Звіти про інциденти, згенеровані штучним інтелектом, містять рекомендації щодо усунення наслідків, а також деталі виявлення.

– Підсумок панелі керування штучним інтелектом, а також конкретні іменовані виявлення, такі як виявлення неможливих подорожей та аномалій обсягу журналу.

Сигнали відповідності стеку:

– Чудово підходить для команд безпеки з обмеженим доступом, які переросли базове управління журналами та потребують можливостей SIEM без ціноутворення на рівні підприємства чи складного розгортання.

– Чудово підходить для організацій, яким потрібна повна гнучкість розгортання (хмарне, локальне або гібридне) без переплати та втрати функцій у процесі.

– Слабше підходить для великих підприємств, яким потрібна глибина UEBA, аналітика внутрішніх загроз або розширена автоматизація штучного інтелекту, що пропонуються комерційними платформами вищого рівня.

Коли складати короткий список / Коли пропускати:

Виберіть варіант, якщо команда економна, бюджетна та потребує можливостей SIEM з реальною гнучкістю розгортання, або якщо планується почати з безкоштовного рівня з відкритим кодом і перейти на платний. Пропустіть, якщо основною вимогою є глибина UEBA корпоративного рівня, виявлення внутрішніх загроз або розширена автоматизація ШІ.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Для розробки компонентів програмного забезпечення мережевої SIEM-системи було використано середовище та мову програмування Visual C++. Сучасні рішення для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах характеризуються високим рівнем складності, що робить створення прикладного софту виключно за допомогою базових засобів мови трудомістким процесом. Для нівелювання цих труднощів та прискорення розробки інтерфейсів оператора, модулів збору й візуалізації подій безпеки застосовуються спеціалізовані бібліотеки класів, зокрема MFC (Microsoft Foundation Classes).

Бібліотека MFC є потужним об’єктно-орієнтованим каркасом (*framework*), що інкапсулює складний програмний інтерфейс операційної системи та базові механізми взаємодії з апаратною платформою. Використання об'єктно-орієнтованого підходу дозволяє значно скоротити обсяг написання рутинного коду (у порівнянні з прямим використанням Windows API), спростити

керування потоками даних, реалізувати ефективне з'єднання з базами даних (де зберігаються інциденти безпеки, логи та правила кореляції) і забезпечити масштабованість архітектури SIEM.

Головними перевагами застосування Visual C++ та бібліотеки MFC у розробці системи мережевої SIEM є:

– Багаторазове використання коду та спадкування: стандартні елементи управління інтерфейсом, обробники подій і структури даних не потребують повторного написання, що мінімізує ймовірність помилок.

– Інкапсуляція API: складні низькорівневі функції безпеки й мережевої взаємодії об'єднані в логічну ієрархію класів, що полегшує їхній аналіз, підтримку та адаптацію до нових стандартів ОС.

– Продуктивність: компільований код на C++ забезпечує високу швидкість обробки великих масивів телеметричних даних і потоків подій, що критично важливо для виявлення загроз у реальному часі в гібридних хмарних інфраструктурах.

– Автоматизація прототипування: засоби генерації додатків дозволяють швидко формувати базову архітектуру багатомодульних застосунків із підтримкою асинхронної обробки й багатовіконного інтерфейсу моніторингу.

Таким чином, застосування Visual C++ спільно з ієрархією класів MFC забезпечує створення надійного, продуктивного та легко розширюваного програмного ядра для аналітичних модулів мережевої SIEM-системи.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти необхідно виконати наступний обсяг

роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформувати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Мультихмарні середовища поєднують публічні хмарні платформи, такі як AWS, Azure та Google Cloud Platform, з приватними хмарами або локальними центрами обробки даних. Кожна платформа генерує різноманітні журнали в різних форматах і протоколах, і команди безпеки стикаються з проблемою агрегації та нормалізації цих даних для отримання корисної аналітики.

Поширені проблеми включають:

– Різноманітність та обсяг журналів: Різні хмарні платформи створюють різні журнали з метаданими, специфічними для хмарного постачальника, що вимагає складної нормалізації.

– Ізольовані системи зберігання даних та фрагментована видимість: без централізованої агрегації команди безпеки ризикують мати сліпі зони в хмарних ресурсах.

– Затримка та обробка в режимі реального часу: Виявлення загроз у режимі реального часу вимагає масштабованого отримання даних та швидкої кореляції.

– Складність відповідності: Кілька хмар можуть піддавати дані різним системам відповідності та нормативним актам, що вимагає автоматизованих, аудитованих засобів контролю.

– Динамічні хмарні робочі навантаження: Постійно змінювані ресурси, тимчасові контейнери та безсерверні функції ускладнюють відстеження ресурсів та базове планування поведінки.

– Обмеження інтеграції та API: Деякі хмарні API мають обмеження швидкості або обмежений доступ до журналів, що впливає на повноту SIEM.

Вирішення цих проблем вимагає SIEM-рішення, створеного для обробки багатохмарної гетерогенності завдяки масштабованій архітектурі, вбудованим хмарним конекторам та комплексній аналітиці.

Ключові кроки для налаштування SIEM для багатохмарних середовищ

Визначення джерел даних та активів інвентаризації

Почніть з каталогізації всіх хмарних постачальників, облікових записів, робочих навантажень, мережевих компонентів і критично важливих програм у вашій багатохмарній інфраструктурі. Визначте джерела журналів, такі як хмарні журнали (CloudTrail, Azure Monitor, GCP Cloud Audit Logs), журнали оркестрації контейнерів (Kubernetes, OpenShift), журнали потоків VPC і SaaS-програми.

Налагодження централізованої агрегації журналів

Використовуйте власні механізми збору даних у хмарі, агенти або API для безпечної потокової передачі журналів у вашу SIEM. Налаштуйте конектори, які обробляють різні формати журналів та передають дані в єдину платформу. ThreatHawk SIEM надає попередньо вбудовані конектори та парсери для популярних хмарних сервісів, що забезпечує послідовну нормалізацію журналів.

Впровадження правил контекстного збагачення та кореляції

Збагачуйте журнали метаданими активів, ідентифікаторами користувачів, геолокацією та аналітикою вразливостей для підвищення точності виявлення. Створюйте правила кореляції та використовуйте поведінкову аналітику для виявлення підозрілих закономірностей, що охоплюють кілька хмар. Ця кореляція між середовищами є критично важливою для виявлення горизонтального переміщення або скоординованих атак.

Розгортання UEBA та моделей виявлення аномалій

Інтегруйте аналітику поведінки користувачів та сутностей (UEBA) з базовими стандартами поведінки та позначайте відхилення, які можуть свідчити про внутрішні загрози, скомпрометовані облікові дані або складні постійні загрози в багатохмарному середовищі.

Забезпечення моніторингу та звітності щодо відповідності

Зіставте джерела хмарних журналів із системами відповідності, що застосовуються до вашої організації, такими як відповідність HIPAA або GDPR,

та налаштуйте звітність платформи автоматизації відповідності в SIEM. Функції ThreatHawk SIEM, готові до відповідності, спрощують підготовку аудиту та забезпечення дотримання політик у всіх хмарних робочих навантаженнях.

Налаштування сповіщень та автоматизації реагування на інциденти

Ретельно встановлюйте пороги сповіщень, щоб мінімізувати шум, забезпечуючи при цьому своєчасне виявлення критичних інцидентів. Інтегруйте робочі процеси ThreatHawk SIEM та SOAR (оркестрація безпеки, автоматизація та реагування), де це можливо, для пришвидшення розслідування та усунення інцидентів.

Оптимізація для масштабування та хмарних функцій

Спроектуйте розгортання SIEM для горизонтальної масштабованості, щоб впоратися з піковими змінами обсягів журналів та хмарної активності. Скористайтеся перевагами хмарних сервісів зберігання, потокової передачі та обчислень, щоб максимізувати ефективність та зменшити затримку.

Використовуйте розширене керування журналами та виявлення загроз у режимі реального часу за допомогою розробленого у даній роботі програмного забезпечення, для об'єднання моніторингу безпеки та відповідності вимогам у AWS, Azure, Google Cloud тощо.

Найкращі практики для конфігурації багатохмарної SIEM-системи

– Інтеграція з хмарними технологіями: широко використовуйте API хмарних постачальників та власні функції ведення журналу. По можливості уникайте залежності від агентів, зменшуючи операційні накладні витрати та розростання агентів.

– Послідовна синхронізація часу: Забезпечте використання синхронізованих позначок часу в журналах з усіх хмарних джерел для підтримки цілісності послідовності подій для точної кореляції.

– Контроль доступу на основі ролей (RBAC): Забезпечення дотримання політик найменших привілеїв у SIEM, розподіляючи обов'язки між аналітиками SOC, архітекторами безпеки та відповідальними за дотримання вимог.

– Зберігання даних та конфіденційність: Узгодьте політики зберігання

журналів із системами відповідності та законами про суверенітет хмарних даних, впроваджуючи вибіркову фільтрацію та маскування за потреби.

– Регулярне налаштування та моніторинг справності: Постійно налаштовуйте правила кореляції та моделі виявлення, щоб зменшити кількість хибнопозитивних результатів. Контролюйте справність хмарних конекторів та потоків журналів, щоб уникнути сліпих зон.

– Автоматизоване збагачення інцидентів: співвіднесення сповіщень SIEM із зовнішньою платформою розвідки загроз ThreatSearch та внутрішніми даними про вразливості для покращення контексту та визначення пріоритетів.

– Використовуйте поведінкову аналітику: використання можливостей UEBA допомагає виявляти загрози, які уникають виявлення на основі сигнатур, зосереджуючись на аномаліях у розподілених середовищах.

3.2 Розробка структурної схеми

Оцінка правильної SIEM для мультихмарної системи вимагає врахування можливостей постачальника, що виходять за рамки традиційної агрегації журналів:

– Хмарні конектори та нативні інтеграції: Чи надає SIEM готові конектори для основних хмарних платформ і сервісів? Наскільки добре він підтримує хмарну телеметрію?

– Масштабованість та продуктивність: Чи може платформа обробляти великі обсяги тимчасових журналів, поширених у контейнерних або безсерверних середовищах, без затримок?

– Розширена аналітика та UEBA: Чи вбудовані моделі машинного навчання та аналітика поведінки для зменшення втоми від тривоги та виявлення складних загроз?

– Готовність до відповідності: Чи автоматизує рішення зіставлення даних журналів з такими нормативними актами, як відповідність PCI DSS , HIPAA, GDPR та ISO 27001 у всіх хмарах?

– Інтеграція екосистеми SOC: підтримка SOAR, каналів інформації про загрози та інструментів управління вразливостями є критично важливою для автоматизованих робочих процесів та визначення пріоритетів.

Розробленого у даній роботі програмне забезпечення,позиціонується як комплексне рішення, що враховує весь спектр цих критеріїв, підкріплене досвідом у сфері дотримання вимог та операцій безпеки. Щоб отримати детальні приклади відмінностей SIEM, ознайомтеся з прикладами SIEM та зрозумійте, що таке SIEM та SIEM наступного покоління. Крім того, слабкі сторони SIEM та способи їх подолання пропонують критично важливе розуміння при виборі платформи для вимогливих багатохмарних середовищ.

Використання фреймворків відповідності в багатохмарній SIEM

Дотримання вимог системи відповідності є важливим у багатохмарній стратегії SIEM, враховуючи різнорідні середовища, в яких передаються та зберігаються дані. ThreatHawk SIEM підтримує автоматичне ведення журналу, аудит та звітність, що відповідають вимогам, включаючи відповідність SOC 2 , ISO 27001, PCI DSS, HIPAA, NIST NIST SP 800-53 та GDPR.

Ключові атрибути для відповідності в багатохмарній SIEM включають:

– Безперервний моніторинг відповідності: Автоматизуйте виявлення порушень політик та відхилень конфігурації в різних хмарних робочих навантаженнях.

– Збір доказів, готових до аудиту: Збирайте незмінні журнали та дані ланцюга зберігання для пришвидшення розслідувань та зовнішніх аудитів.

– Оповіщення на основі політик: генеруйте оповіщення, спеціально пов’язані з вимогами дотримання, що сприяє швидкому реагуванню на невідповідність.

– Усвідомлення місця зберігання даних: Забезпечте дотримання регіональних законів про конфіденційність під час обробки даних, включаючи маскування або шифрування даних за потреби.

Інтеграція автоматизації відповідності в SIEM зменшує ручне навантаження на менеджерів з IT-безпеки та спеціалістів з відповідності, дозволяючи аналітикам SOC зосередитися на виявленні реальних загроз.

Вирішення поширених помилок у розгортанні багатохмарних SIEM-систем

Незважаючи на ретельне планування, організації часто стикаються з підводними каменями під час розгортання SIEM у багатохмарних контекстах. Визнання та пом'якшення цих недоліків є життєво важливим для забезпечення сталого стану безпеки.

– Недостатнє охоплення журналами: Нездатність інтегрувати всі критичні джерела журналів призводить до появи сліпих зон – забезпечте безперервне виявлення та інтеграцію нових хмарних ресурсів.

– Надмірна гучність сповіщень: Надмірна кількість хибнопозитивних результатів призводить до втоми від сповіщень. Впроваджуйте стратегії налаштування та аналітику на основі поведінки, щоб покращити співвідношення сигнал/шум.

– Затримка у виявленні загроз: погано спроектовані канали передачі даних можуть затримувати виявлення. Використовуйте масштабовану обробку потоків та можливості аналітики в режимі реального часу.

– Недооцінка складності хмари: ігнорування нюансів моделі безпеки кожної хмари призводить до неповної контекстуалізації – використовуйте SIEM з власними, глибокими інтеграціями.

– Погана співпраця та обмін даними: SOC повинні встановити інтегровані робочі процеси з використанням SOAR та платформ розвідки загроз для автоматизації реагування та обміну інформацією.

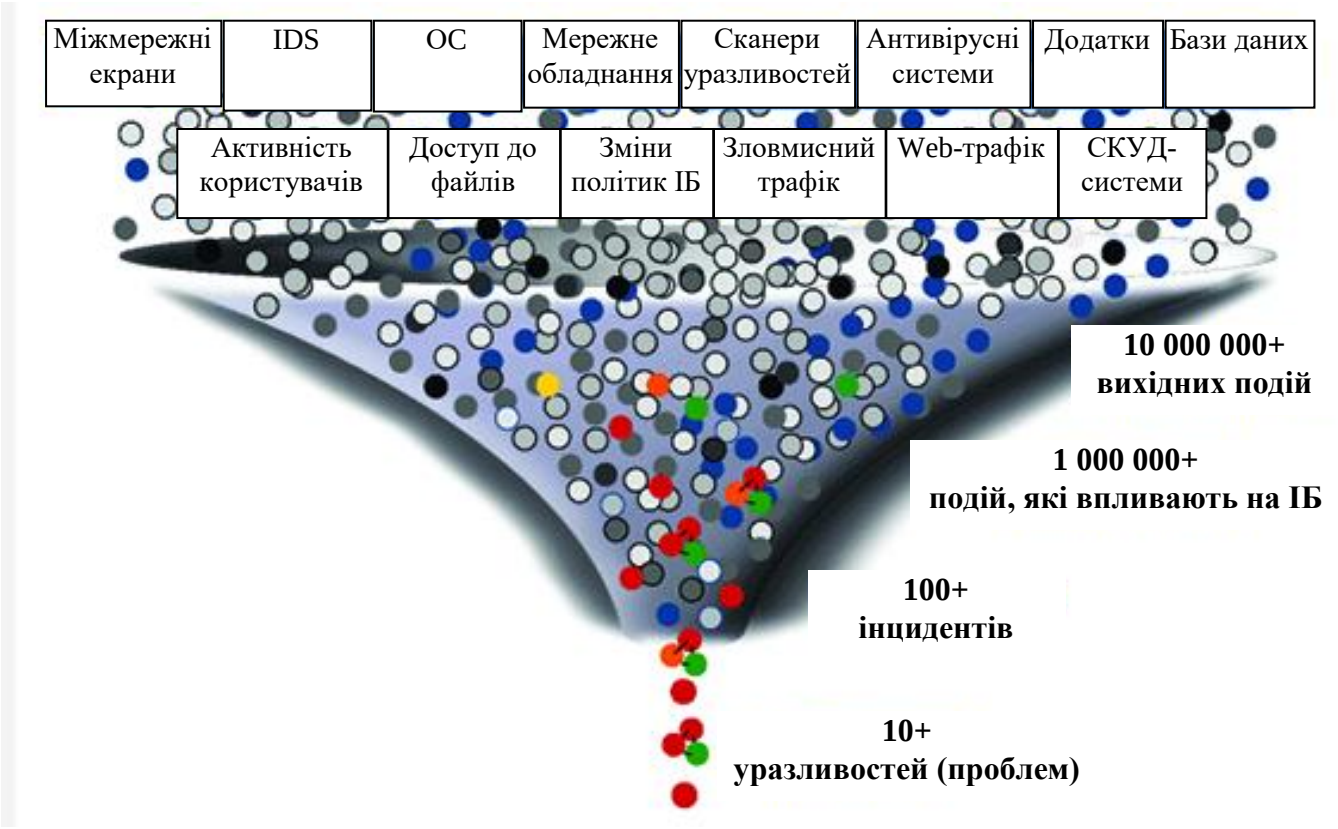


Рисунок 3.1 – Структурна схема системи

Критичне зауваження: У багатохмарних розгортаннях SIEM періодична перевірка повноти журналів та ефективності виявлення є важливою для підтримки гарантії безпеки та відповідності нормативним вимогам.

Майбутні тенденції, що впливають на багатохмарну SIEM у 2026 році

Еволюція хмарної безпеки визначатиме кілька тенденцій, що впливатимуть на використання SIEM у багатохмарних середовищах:

– Покращена інтеграція штучного інтелекту та машинного навчання: платформи SIEM наступного покоління поглиблять використання машинного навчання для прогнозного виявлення загроз та сортування інцидентів.

– Хмарно-орієнтовані архітектури SIEM: Моделі розгортання, що підкреслюють масштабованість за допомогою безсерверних та контейнерних компонентів SIEM, стануть поширеними.

– Інтеграція розширеного виявлення та реагування (XDR): Ширша інтеграція телеметрії кінцевих точок, мережі та хмари забезпечить єдину видимість загроз та швидше реагування.

– Розширені можливості автоматизації та SOAR: Автоматизовані сценарії та робочі процеси реагування скоротять час простою та операційні витрати.

– Регуляторний акцент на хмарній безпеці: Поступові вимоги до дотримання вимог вимагатимуть забезпечення дотримання вимог у режимі реального часу, вбудованого в платформи SIEM.

Організації, що впроваджують ThreatHawk SIEM, можуть використовувати його вбудовану UEBA та розширювані інтеграції SOAR для швидкої адаптації до цих тенденцій, що змінюються, підтримуючи ефективну захисну позицію.

Впровадження SIEM для багатохмарних середовищ у 2026 році вимагає стратегічного, масштабованого підходу, який охоплює комплексний збір даних, кореляцію в режимі реального часу та автоматизацію дотримання вимог на різних хмарних платформах. Підприємства повинні вибирати SIEM-рішення, які не лише обробляють різнорідні журнали, але й інтегрують розширену аналітику та поведінкові дані для ефективного виявлення складних загроз. Розроблене у цій роботі програмне забезпечення відповідає цим вимогам, поєднуючи управління журналами корпоративного рівня, сповіщення в режимі реального часу та моніторинг відповідності нормативним вимогам в єдину платформу, адаптовану для складних багатохмарних операцій.

Для керівників вищої ланки з безпеки та команд SOC інвестування в таке рішення забезпечує операційну узгодженість у хмарних середовищах, зменшує втому від сповіщень та оптимізує зусилля щодо дотримання вимог, надаючи організаціям можливість проактивно керувати новими кіберризиками та нормативними вимогами.

3.3 Розробка функціональної схеми

Функціональну схему розробленої системи наведено на рисунку 3.2. Сучасні корпоративні та гібридні мережеві інфраструктури активно використовують інтегровані маршрутизатори та шлюзи безпеки, які об'єднують функції міжмережевих екранів (файрволів), механізми трансляції мережевих адрес (NAT), динамічний інспекційний аналіз пакетів (SPI), а також фільтрацію трафіку за IP-адресами, застосунками та веб-ресурсами.

Для організації безпечного доступу із зовнішніх мереж до корпоративних серверів часто застосовується концепція демілітаризованої зони (DMZ). На рівні мережевого обладнання налаштування DMZ дозволяє ізолювати трафік, що спрямовується на конкретну статичну IP-адресу внутрішнього сервера, забезпечуючи його доставку лише на визначений порт комутатора, тоді як інші вузли залишаються під захистом периметрового файрволу. У найпростішій конфігурації активація DMZ відкриває зовнішнім вузлам доступ до всіх портів захищеного сервера (наприклад, 80 для HTTP, 21 для FTP або 110 для поштових сервісів).

Для підвищення рівня захисту використовується переадресація портів (Port Forwarding), яка реалізує більш сувору сегментацію трафіку: зовнішній доступ дозволяється виключно до чітко визначених портів, тоді як решта з'єднань блокується. Це дозволяє зменшити поверхню атаки в гібридній інфраструктурі.

Водночас бездротові точки доступу, інтегровані в мережеве обладнання корпоративного сегмента, часто розглядаються як продовження внутрішньої мережі. У разі неправильної конфігурації або відсутності належних протоколів шифрування (наприклад, у незахищеному режимі) підключені бездротові клієнти можуть отримати прямий доступ до захищених ресурсів компанії в обхід міжмережевих екранів. Подібні інциденти створюють критичні вразливості, які повинні фіксуватися і аналізуватися в реальному часі модулями збору подій та кореляції загроз розроблюваної мережевої SIEM-системи.

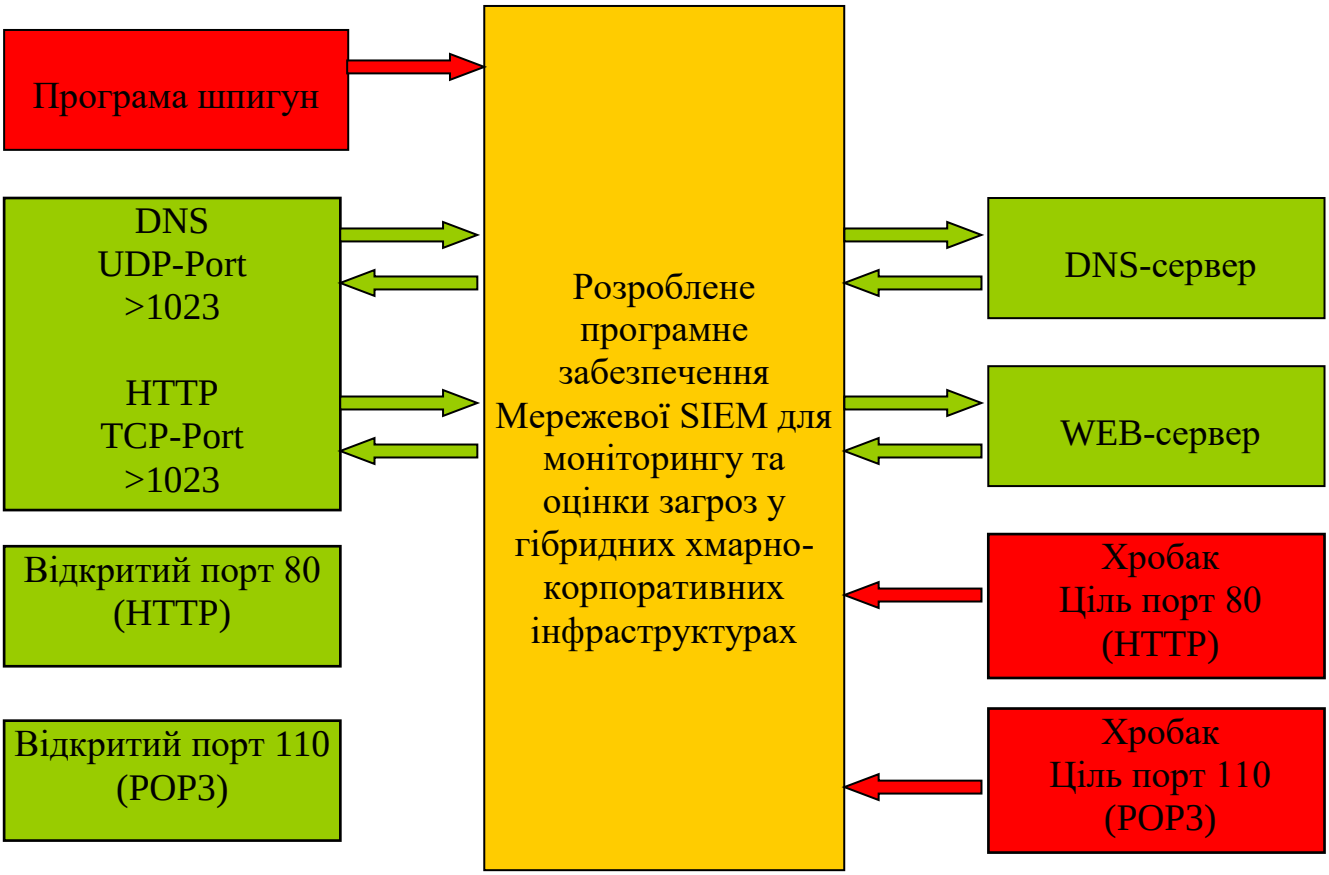


Рисунок 3.2 – Функціональна схема системи

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Для візуалізації процесів обробки даних у межах структурного проєктування використовується діаграма взаємодії процесів. Традиційно на початковому етапі розробки створюється контекстна діаграма потоків даних, яка ілюструє загальну взаємодію SIEM-системи із зовнішнім середовищем (джерелами подій, хмарними шлюзами та корпоративними мережевими сегментами). Надалі ця модель деталізується шляхом поетапної декомпозиції процесів і інформаційних потоків, що дозволяє повноцінно відобразити архітектуру та логіку збору, агрегації й кореляції подій безпеки.

Діаграму процесів розробленої системи наведено на рисунку 3.3. Її детальний аналіз дозволяє простежити характер взаємодії внутрішніх компонентів та маршрутизацію телеметричних даних усередині платформи. У межах проєктування застосовується модель візуалізації потоків даних (*Data Flow Diagram, DFD*), яка забезпечує наочне графічне представлення обміну інформацією та станів обробки інцидентів у розробленій гібридній системі моніторингу загроз.

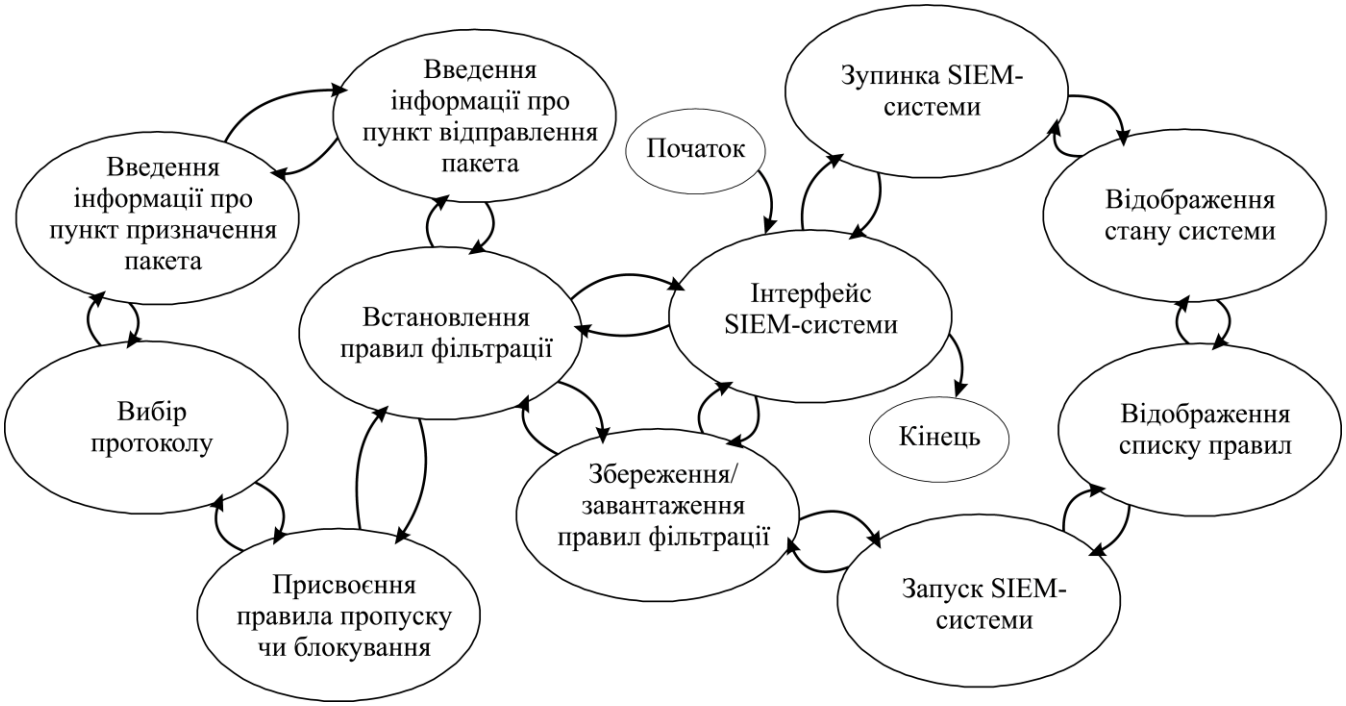


Рисунок 3.3 – Діаграма взаємодії процесів

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Алгоритмічне забезпечення мережевої системи Security Information and Event Management (SIEM) призначене для централізованого моніторингу подій інформаційної безпеки, виявлення потенційних кіберзагроз та оцінювання їхнього впливу на гібридну хмарно-корпоративну інфраструктуру. Основним завданням є об'єднання інформації, отриманої від локальних мережевих пристроїв, серверів, засобів захисту та хмарних сервісів, у спільному аналітичному середовищі. Особливістю такого підходу є можливість зіставлення подій, які виникають у різних сегментах інформаційної системи, але можуть бути пов'язані з однією загрозою. Алгоритми повинні забезпечувати своєчасне отримання даних, перевірку їхньої коректності, визначення підозрілої активності та формування результатів для подальшого реагування.

Загальну послідовність функціонування програмного комплексу відображено на рисунку 4.1. Основний алгоритм передбачає отримання подій від розподілених джерел, нормалізацію інформації, встановлення зв'язків між мережевими об'єктами та виконання аналітичних перевірок. Після виявлення ознак потенційної загрози здійснюється оцінювання її критичності з урахуванням характеристик відповідних ресурсів. Результати передаються до підсистеми керування інцидентами та відображаються в інтерфейсі моніторингу. Подальше надходження даних забезпечує можливість уточнення попередніх висновків і зміни стану зареєстрованих інцидентів.

Для організації роботи системи доцільно застосовувати розподілену архітектуру збору та оброблення подій.

Її основними функціональними складовими є мережеві сенсори, колектори журналів, модуль нормалізації, сховище подій та аналітичний компонент. Окремо передбачаються засоби керування правилами виявлення загроз і формування сповіщень.

Така організація дозволяє відокремити отримання телеметрії від виконання ресурсомістких операцій аналізу.

Внаслідок цього зміна інтенсивності надходження повідомлень не повинна безпосередньо порушувати логіку оцінювання вже отриманих подій.

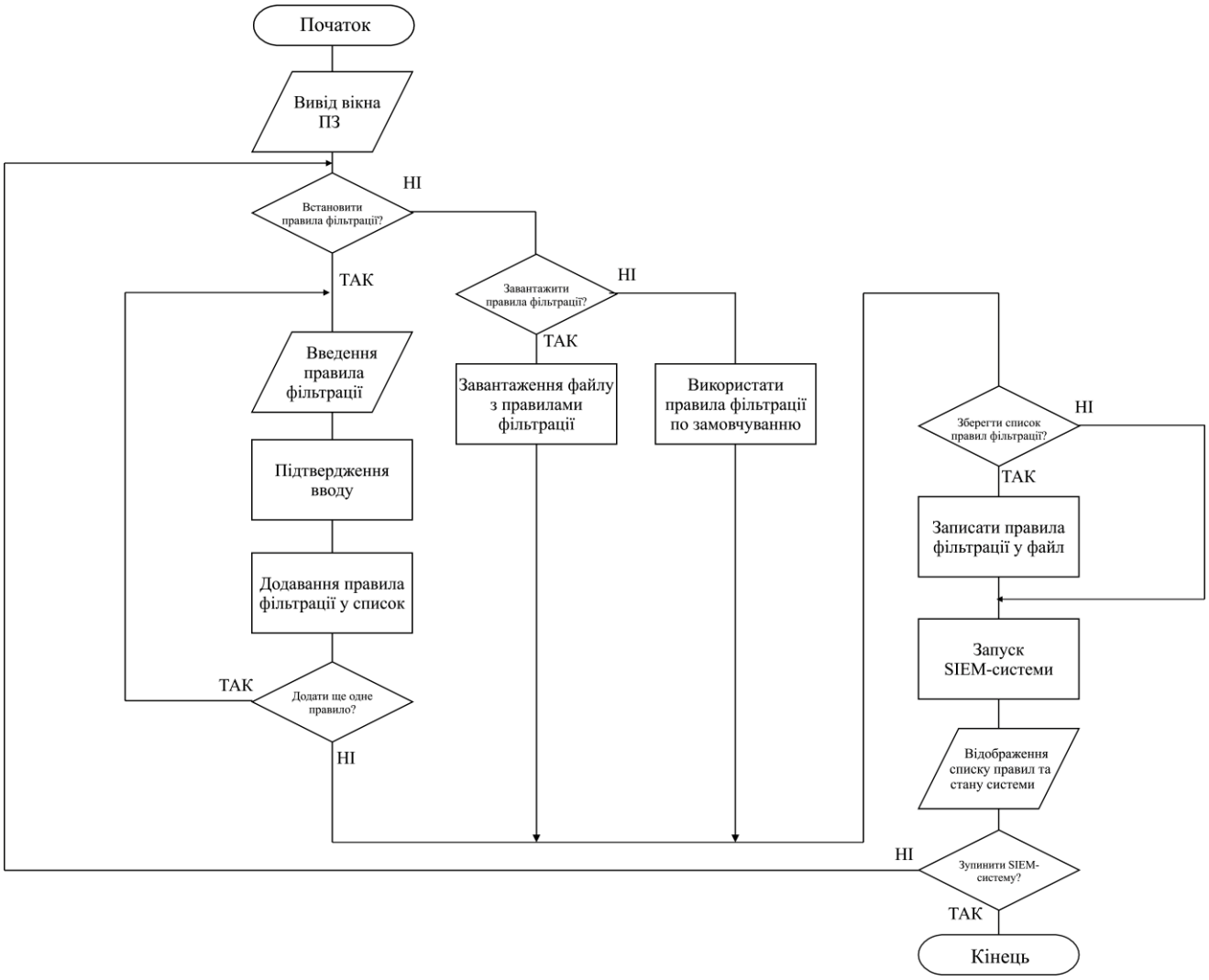


Рисунок 4.1 – Блок-схема основної програми

Для збору мережевої інформації як можливі технологічні рішення розглядаються Suricata та Zeek. Suricata може використовуватися для аналізу мережевих пакетів, виявлення підозрілої активності за правилами та формування структурованих повідомлень. Zeek забезпечує отримання відомостей про мережеві з'єднання та події прикладних протоколів.

Для журналів корпоративної інфраструктури можуть застосовуватися Syslog, агенти збору подій та спеціалізовані програмні інтерфейси. Інформація з хмарних середовищ отримується через відповідні сервіси аудиту й моніторингу. Зазначені компоненти становлять можливу технологічну основу системи, а їхній фактичний склад залежить від прийнятої програмної реалізації.

Одним із центральних елементів алгоритмічного забезпечення є підпрограма кореляції подій та оцінювання потенційних загроз. Принцип її роботи представлено на рисунку 4.2.

Підпрограма отримує нормалізовані повідомлення, визначає спільні ознаки, аналізує часову послідовність та перевіряє відповідність установленим сценаріям небезпечної активності.

Якщо декілька подій характеризують імовірний розвиток одного порушення, вони об'єднуються у пов'язану послідовність. Після цього виконується оцінювання загрози з урахуванням важливості задіяних ресурсів, достовірності ознак та можливих наслідків.

Особливістю гібридної інфраструктури є поєднання корпоративної мережі з ресурсами публічної або приватної хмари. Окремі застосунки можуть працювати на локальних серверах, а їхні бази даних або резервні компоненти розміщуватися в хмарному середовищі.

Взаємодія між ними здійснюється через захищені канали, VPN, приватні мережеві з'єднання або прикладні програмні інтерфейси. Тому потенційна атака може проявлятися одночасно в корпоративних журналах і подіях хмарного провайдера.

Для її виявлення необхідно забезпечити спільне представлення адрес, ідентичностей, ресурсів та часових характеристик.

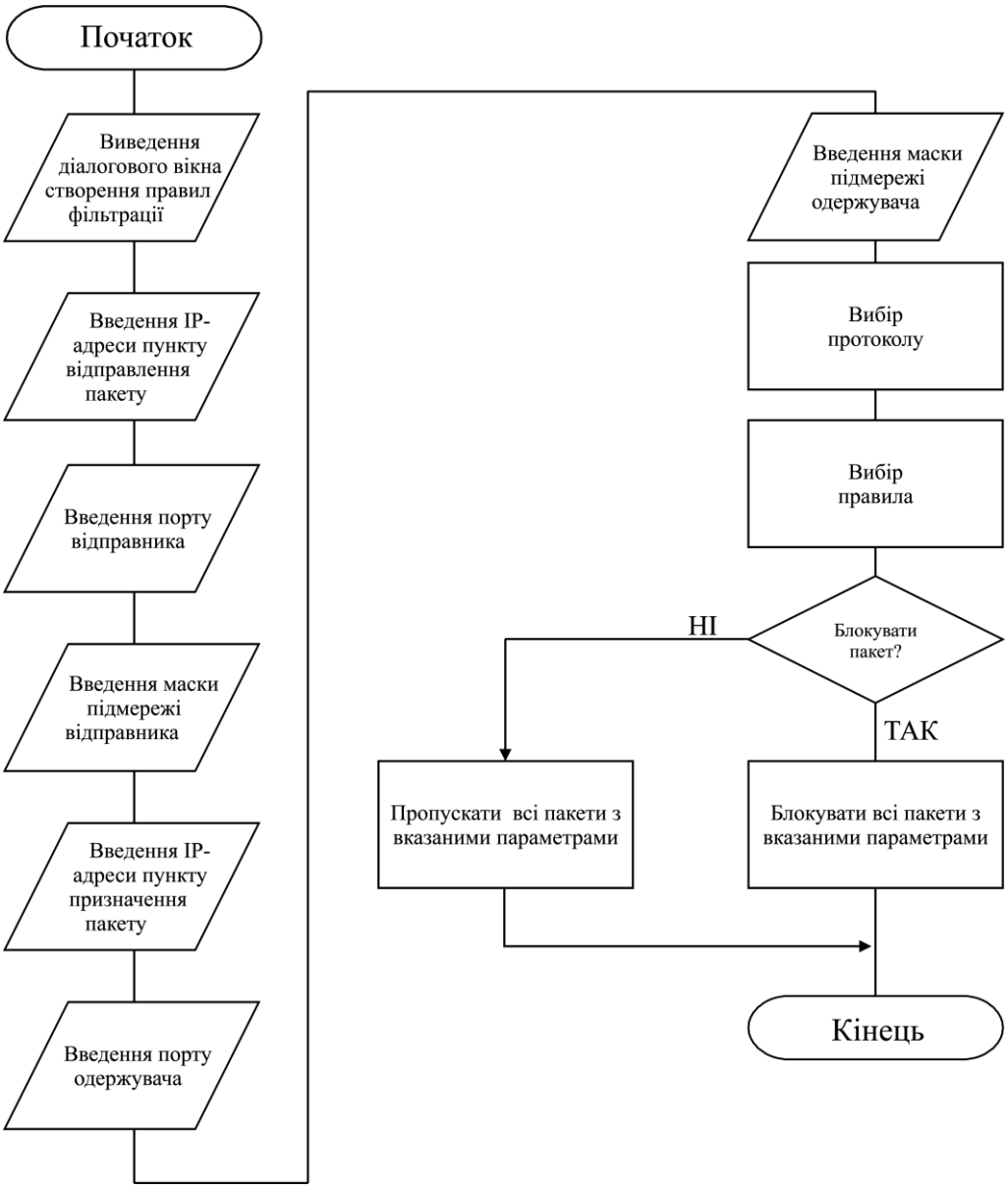


Рисунок 4.2 – Блок-схема роботи підпрограми

Алгоритм виявлення та реєстрації джерел подій

Початковим етапом функціонування мережевої SIEM є формування переліку джерел інформації, які підлягають моніторингу. До них належать міжмережеві екрани, маршрутизатори, комутатори, системи виявлення вторгнень, VPN-шлюзи, DNS-сервери та засоби автентифікації. У хмарному сегменті джерелами можуть бути журнали адміністративних операцій, мережевих потоків і звернень до керованих сервісів.

Вхідними даними алгоритму є конфігурація контрольованої інфраструктури та відомості про доступні засоби отримання подій. Для кожного джерела визначаються тип пристрою або сервісу, мережеві параметри, спосіб передавання журналів і відповідальна область інфраструктури.

Після отримання інформації виконується перевірка можливості підключення. Якщо джерело підтримує Syslog, визначаються адреса приймального колектора та відповідний транспортний протокол. Для хмарних сервісів перевіряються доступність програмного інтерфейсу та повноваження службової ідентичності. Для мережевих сенсорів контролюється наявність необхідного інтерфейсу спостереження.

Кожному джерелу призначається стабільний внутрішній ідентифікатор. Він дозволяє зберігати історію подій незалежно від зміни IP-адреси або мережевого розташування пристрою. Додатково фіксуються характеристики джерела, які впливають на інтерпретацію повідомлень.

Алгоритм повинен враховувати можливість появи нових хмарних ресурсів. Створення віртуальної машини або мережевого компонента може супроводжуватися появою додаткового джерела телеметрії. Для його реєстрації можуть використовуватися періодична інвентаризація та відповідні події хмарного керування.

Якщо джерело тимчасово недоступне, його не слід автоматично видаляти з реєстру. Натомість визначається стан втрати зв'язку та зберігається інформація про останнє успішне отримання повідомлень. Результатом алгоритму є актуальний перелік джерел безпекової інформації та їхніх характеристик.

Алгоритм збору мережевої телеметрії

Після реєстрації джерел здійснюється отримання мережевих подій. Основним завданням алгоритму є забезпечення передавання інформації від сенсорів і мережевого обладнання до централізованої системи оброблення.

Вхідними даними є повідомлення мережевих пристроїв, записи про з'єднання, результати перевірок систем виявлення вторгнень і службові журнали. Для кожного потоку даних встановлюється відповідний механізм приймання.

Мережеві сенсори можуть отримувати копії трафіку через SPAN-порт комутатора або спеціалізований засіб мережевого відгалуження. Такий спосіб дозволяє спостерігати за передаванням пакетів без необхідності розміщувати сенсор безпосередньо на маршруті користувацького трафіку.

Під час аналізу пакетів визначаються мережеві адреси, транспортні порти, протоколи, тривалість з'єднань та інші доступні характеристики. Якщо передбачено використання Suricata, результати можуть формуватися у форматі EVE JSON. Він підтримує структуровані записи про мережеві потоки, спрацювання правил і події прикладних протоколів. Відповідні можливості описані в документації Suricata.

Для зменшення навантаження на центральний компонент доцільно виконувати попередню обробку повідомлень на локальних колекторах. Вона може включати перевірку структури, додавання ідентифікатора джерела та відокремлення технічних повідомлень від подій безпеки.

Під час збору необхідно враховувати шифрування мережевого трафіку. Для TLS-з'єднань сенсор зазвичай не має доступу до відкритого вмісту прикладних повідомлень. Тому аналіз може спиратися на мережеві метадані, характеристики сеансу та інформацію, доступну без дешифрування. Перехоплення повного прикладного вмісту не слід вважати обов'язковою можливістю мережевої SIEM.

Після отримання повідомлень виконується їх передавання до колектора. Якщо приймальний компонент тимчасово недоступний, може застосовуватися обмежена буферизація. Результатом алгоритму є потік мережевих подій із визначеним походженням і часовими характеристиками.

Алгоритм інтеграції журналів хмарної інфраструктури

Для аналізу загроз у гібридному середовищі мережевої телеметрії корпоративного сегмента недостатньо. Значна частина адміністративних і прикладних операцій у хмарі виконується через програмні інтерфейси провайдера. Тому необхідно отримувати відповідні журнали та пов'язувати їх із локальними подіями.

Вхідними даними алгоритму є параметри підключення до хмарного облікового запису, перелік контрольованих ресурсів і доступні інтерфейси отримання журналів. Для AWS можуть розглядатися AWS CloudTrail та VPC Flow Logs. В Azure відповідні відомості можуть надходити з журналів активності та мережевих засобів моніторингу. Конкретний набір джерел визначається використовуваною платформою.

Після встановлення з'єднання алгоритм перевіряє наявність необхідних повноважень. Для звичайного моніторингу доцільно використовувати окрему службову ідентичність із правами читання потрібних журналів. Надання прав на зміну або видалення ресурсів не потрібне для отримання подій.

Далі виконується завантаження нових записів. Для запобігання повторному отриманню великого обсягу інформації можуть використовуватися ідентифікатори оброблених повідомлень, часові межі або інші механізми, передбачені API провайдера.

Особливістю хмарних журналів є можлива затримка між виникненням події та її доступністю для отримання. Тому час надходження до SIEM не повинен автоматично вважатися часом виконання операції. Для подальшої кореляції зберігається початкова часова позначка.

Після отримання журналу визначаються суб'єкт виконання операції, тип дії, цільовий ресурс і результат. Наприклад, зміна політики доступу до об'єктного сховища може бути пов'язана з попередньою автентифікацією користувача через корпоративний VPN.

Результатом алгоритму є уніфікований потік хмарних подій, придатний для спільного аналізу з інформацією корпоративної мережі.

Алгоритм нормалізації та перевірки подій безпеки

Події, отримані від різних джерел, можуть мати несумісні формати. Один пристрій передає текстові повідомлення Syslog, інший формує JSON, а хмарний сервіс використовує власну структуру журналу. Без нормалізації складно визначати спільні ознаки та застосовувати однакові правила виявлення загроз.

Вхідними даними алгоритму є повідомлення колекторів та відомості про тип джерела. На першому етапі визначається формат запису. Після цього застосовується відповідний синтаксичний аналізатор, який виділяє основні поля.

Для уніфікованого представлення можуть використовуватися принципи Open Cybersecurity Schema Framework (OCSF). Ця модель передбачає стандартизовані категорії, класи подій та структури атрибутів, придатні для різних засобів інформаційної безпеки. Відповідні визначення наведені в OCSF Schema.

Після синтаксичного аналізу визначаються час події, її джерело, категорія, мережеві адреси, користувач і результат операції. Якщо повідомлення містить лише частину цих відомостей, відсутні поля залишаються невизначеними. Їх не слід заповнювати вигаданими значеннями.

Окремо виконується приведення часових позначок до узгодженого представлення. Для розподілених інфраструктур доцільно використовувати UTC та зберігати інформацію про початковий часовий пояс, якщо вона доступна. Це дозволяє зіставляти події корпоративного й хмарного середовищ.

Для мережевих адрес перевіряється правильність представлення IPv4 та IPv6. Якщо повідомлення містить адреси, змінені внаслідок трансляції NAT, алгоритм не повинен автоматично вважати їх ідентичними внутрішнім адресам без відповідних відомостей про трансляцію.

Під час перевірки коректності контролюються типи полів, допустимість часових значень та відповідність категорії події її структурі. Некоректні повідомлення відокремлюються для діагностики. Результатом алгоритму є нормалізовані записи, які можуть використовуватися для кореляційного аналізу.

Алгоритм контролю достовірності та усунення дублювання подій

У розподіленій інфраструктурі одна мережева операція може бути зареєстрована декількома засобами. Наприклад, спроба підключення до сервера може одночасно потрапити до журналу міжмережевого екрана, мережевого сенсора та операційної системи. Це не обов'язково є помилковим дублюванням,

оскільки кожне джерело може характеризувати різні властивості тієї самої операції.

Алгоритм повинен розрізняти повторну доставку одного повідомлення та незалежну реєстрацію пов'язаної події. Вхідними даними є нормалізовані записи та відомості про їхнє походження.

Для визначення точних дублікатів використовуються стабільні ідентифікатори джерела, власні ідентифікатори повідомлень і додаткові атрибути. Якщо джерело не надає унікального ідентифікатора, може застосовуватися обчислення контрольного значення за визначеним набором полів.

Під час порівняння необхідно враховувати час події. Дві однакові спроби мережевого підключення, виконані в різні моменти, не повинні об'єднуватися лише через збіг адрес і портів.

Повторно доставлене повідомлення може бути позначене як уже оброблене. При цьому система зберігає інформацію про факт повторного надходження, якщо вона потрібна для контролю транспортного каналу.

Окремо перевіряється актуальність даних. Якщо повідомлення надійшло із значним запізненням, воно може використовуватися для історичного аналізу, але не повинно автоматично трактуватися як нова поточна загроза.

Результатом алгоритму є набір достовірних подій із контрольованим рівнем дублювання та збереженими відомостями про джерела.

Алгоритм ідентифікації мережевих ресурсів і користувачів

Для оцінювання загроз необхідно встановити, до яких саме ресурсів належать зареєстровані події. Одна IP-адреса не завжди однозначно визначає сервер або користувача. У хмарних середовищах адреси можуть змінюватися після перезапуску ресурсів, а в корпоративних мережах широко використовуються DHCP і NAT.

Вхідними даними алгоритму є інформація про мережеві адреси, ідентифікатори хмарних ресурсів, записи DNS, відомості систем автентифікації та інвентаризаційні дані.

На початковому етапі алгоритм визначає можливий об'єкт, якому належала адреса на момент виникнення події. Для цього враховуються часові характеристики призначення IP-адрес та доступні записи про мережеві підключення.

Якщо подія пов'язана з хмарною віртуальною машиною, пріоритет може надаватися стабільному ідентифікатору ресурсу, отриманому від провайдера. Для корпоративного сервера можуть використовуватися інвентарний ідентифікатор, назва вузла або відомості системи керування активами.

Після визначення ресурсу виконується прив'язування його характеристик. До них належать функціональне призначення, критичність, належність до підрозділу та мережевий сегмент. Ці характеристики використовуються на етапі оцінювання ризику.

Для подій автентифікації додатково визначається користувацька ідентичність. При цьому необхідно враховувати можливість різного представлення одного користувача в локальному каталозі та хмарному постачальнику ідентичності.

Якщо відповідність не можна встановити достовірно, алгоритм зберігає декілька можливих ознак або позначає ідентичність як невизначену. Помилкове ототожнення різних користувачів може призвести до неправильного об'єднання подій і необґрунтованих висновків.

Результатом є збагачені події, пов'язані з конкретними ресурсами та суб'єктами настільки, наскільки це дозволяють наявні дані.

Алгоритм кореляції подій між корпоративним і хмарним сегментами

Кореляція є одним із головних механізмів виявлення складних загроз. Окрема подія може не містити достатніх ознак порушення, проте її поєднання з іншими повідомленнями дозволяє встановлювати характерну послідовність дій.

Вхідними даними алгоритму є нормалізовані та збагачені записи. Для кожної події визначаються категорія, час виникнення, суб'єкт, ресурс і доступні мережеві характеристики.

На першому етапі повідомлення групуються за спільними ідентифікаторами. Це можуть бути IP-адреса, користувацький обліковий запис, хмарний ресурс або ідентифікатор мережевого сеансу. Далі визначається їхня належність до встановленого часового інтервалу.

Для аналізу використовуються ковзні часові вікна. Вони дозволяють оцінювати події, які виникли протягом близького періоду та можуть характеризувати один сценарій активності.

Особливістю гібридного середовища є затримка надходження частини хмарних журналів. Тому кореляція повинна враховувати час фактичної події, а не лише час її приймання. Для запізнілих повідомлень може застосовуватися допустиме вікно дообробления.

Наприклад, у корпоративному журналі може бути зафіксовано серію невдалих спроб автентифікації через VPN. Після цього з'являється успішний вхід відповідного облікового запису. Якщо невдовзі в хмарному журналі реєструється зміна повноважень цього користувача, система може розглядати сукупність подій як потенційно небезпечний сценарій.

Водночас наведена послідовність сама по собі не доводить факт компрометації. Вона може відповідати легітимним адміністративним діям. Тому алгоритм повинен враховувати додаткові ознаки, зокрема джерело підключення, тип облікового запису та наявність запланованих змін.

Для реалізації складніших сценаріїв доцільно використовувати правила кореляції з визначеними умовами, часовими обмеженнями та групуванням за відповідними полями.

Результатом алгоритму є пов'язані групи подій, які можуть відображати окремі етапи розвитку потенційної кіберзагрози.

Алгоритм виявлення загроз на основі правил

Для автоматизованого визначення відомих сценаріїв небезпечної активності передбачається використання правил виявлення. Кожне правило встановлює необхідні умови, за яких подія або група подій повинна розглядатися як ознака потенційного порушення.

Вхідними даними алгоритму є потік нормалізованих повідомлень і набір активних правил. На першому етапі визначається категорія події. Далі виконуються ті перевірки, які відповідають її типу та доступним атрибутам.

Для мережевого трафіку можуть використовуватися сигнатури систем виявлення вторгнень. Вони дозволяють визначати відомі ознаки мережевих атак, сканування або небезпечної протокольної активності. При цьому результати сигнатурного аналізу повинні розглядатися з урахуванням можливості хибнопозитивних спрацювань.

Для журналів операційних систем і хмарних сервісів може застосовуватися підхід, заснований на Sigma. Специфікація Sigma визначає універсальний формат опису правил виявлення, які можуть перетворюватися на запити конкретних аналітичних систем. Окремо підтримуються правила кореляції декількох подій, визначені у Sigma Correlation Rules Specification.

Під час застосування правил необхідно перевіряти сумісність доступних полів із вимогами відповідного сценарію. Якщо правило потребує атрибута, який не надходить від певного джерела, результат перевірки не слід вважати достовірним підтвердженням відсутності загрози.

Для кожного спрацювання формується запис із зазначенням правила, джерел даних, пов'язаних подій та причини прийняття рішення. Це дозволяє аналітику відтворити умови, які призвели до формування сповіщення.

Результатом алгоритму є перелік виявлених ознак загроз із відповідними технічними доказами.

Алгоритм виявлення аномальної мережевої активності

Сигнатурні правила не завжди дозволяють виявляти нові або модифіковані способи небезпечної взаємодії. Тому доцільно доповнювати їх аналізом відхилень від характерної поведінки мережевих ресурсів.

Вхідними даними алгоритму є історичні показники інтенсивності мережевих з'єднань, обсягів передавання, частоти DNS-запитів, кількості невдалих автентифікацій та інших контрольованих характеристик.

На початковому етапі формується базовий профіль активності. Для цього використовуються дані за попередні порівнянні періоди. Важливо враховувати добові та тижневі зміни навантаження. Наприклад, висока інтенсивність звернень у робочий час може бути звичайною, тоді як аналогічна активність у неробочий період потребуватиме додаткового аналізу.

Для оцінювання відхилень можуть використовуватися статистичні характеристики часового ряду. До них належать медіана, характерний діапазон коливань та швидкість зміни показника. За потреби можуть застосовуватися складніші методи виявлення аномалій, однак їхня придатність повинна перевірятися на даних конкретної інфраструктури.

Прикладом підозрілої активності є значне збільшення кількості вихідних з'єднань одного сервера з раніше невідомими адресами. Іншим сценарієм може бути різке зростання обсягу переданих даних із корпоративного сегмента до зовнішнього ресурсу.

Водночас такі зміни можуть бути пов'язані з легітимним резервним копіюванням, оновленням програмного забезпечення або іншими технологічними операціями. Тому статистичне відхилення повинно розглядатися як підстава для додаткової перевірки, а не як безумовне підтвердження атаки.

Для зменшення кількості помилкових спрацювань алгоритм зіставляє аномалії з відомими характеристиками ресурсу. Наприклад, сервер резервного копіювання може мати інший профіль мережевої активності, ніж робоча станція користувача.

Результатом алгоритму є набір аномальних спостережень, придатних для подальшої кореляції та оцінювання ризику.

Алгоритм класифікації загроз за тактиками та техніками атак

Для систематизації результатів виявлення доцільно використовувати загальноприйняту модель опису дій порушника. Одним із таких підходів є MITRE ATT&CK, який містить структурований опис тактик і технік, що можуть застосовуватися під час кібератак.

Алгоритм класифікації отримує результат спрацювання правила, відомості про відповідні події та доступні ознаки поведінки. На початковому етапі визначається, чи має виявлений сценарій встановлений зв'язок із певною технікою ATT&CK.

Наприклад, багаторазові спроби підбору облікових даних можуть бути пов'язані з техніками атак на автентифікацію. Незвичні звернення до адміністративних API можуть розглядатися в контексті можливого зловживання хмарними повноваженнями.

Відповідність техніці визначається на основі змісту виявленої поведінки, а не лише за назвою правила. Якщо наявних відомостей недостатньо для достовірної класифікації, алгоритм повинен залишати відповідний зв'язок непідтвердженим.

Для гібридних середовищ важливо враховувати можливість переходу активності між локальною та хмарною частинами інфраструктури. Наприклад, компрометація корпоративного облікового запису може передувати використанню пов'язаних із ним хмарних повноважень.

Класифікація дозволяє групувати результати моніторингу за типами потенційних дій порушника. Це може використовуватися для оцінювання покриття сценаріїв виявлення та визначення напрямів подальшого вдосконалення правил.

Результатом алгоритму є структурований опис виявленої активності з відповідними техніками та рівнем підтвердження класифікації.

Алгоритм оцінювання критичності кіберзагроз

Після виявлення підозрілої активності необхідно визначити її значущість для контрольованої інфраструктури. Однакові технічні ознаки можуть мати різні наслідки залежно від призначення ресурсу, його доступності та характеру оброблюваної інформації.

Вхідними даними алгоритму є результати виявлення загрози, відомості про активи, характеристики пов'язаних подій та встановлена політика оцінювання.

На першому етапі визначається технічна значущість спрацювання. Для цього враховуються тип виявленої активності, кількість підтверджених ознак і достовірність використаних джерел.

Далі аналізується важливість задіяного ресурсу. Наприклад, потенційне порушення на сервері автентифікації може мати ширший вплив, ніж аналогічна подія на ізольованій тестовій машині. Для хмарних ресурсів додатково враховується доступ до сховищ, адміністративних функцій та інших критичних сервісів.

Наступним етапом є оцінювання можливого поширення загрози. Якщо підозріла активність пов'язана з декількома сегментами мережі або обліковими записами, її пріоритет може підвищуватися. При цьому необхідно розрізняти встановлені факти та припущення про можливі подальші дії порушника.

Для прийняття рішення може використовуватися багатокритеріальна модель оцінювання. Вона враховує важливість активу, характер загрози, кількість незалежних підтверджень та доступність ресурсу. Вагові параметри такої моделі повинні визначатися за результатами налаштування та перевірки.

За результатами оцінювання події може призначатися низький, середній, високий або критичний рівень небезпеки. Конкретні умови переходу між рівнями визначаються політикою організації.

Для підвищення достовірності важливо не ототожнювати кількість спрацювань із рівнем ризику. Велика кількість однотипних повідомлень від одного сенсора не завжди є переконливішим підтвердженням атаки, ніж декілька незалежних подій з різних джерел.

Результатом алгоритму є визначений пріоритет загрози з поясненням чинників, які вплинули на оцінювання.

Алгоритм формування та керування інцидентами безпеки

Окремі спрацювання правил не завжди повинні створювати незалежні інциденти. Значна кількість повідомлень може характеризувати одну послідовність небезпечних дій. Тому передбачається алгоритм групування результатів аналізу та керування життєвим циклом інцидентів.

Вхідними даними є спрацювання правил, результати кореляції, оцінки критичності та відомості про вже зареєстровані інциденти.

На початковому етапі перевіряється наявність активного інциденту, пов'язаного з відповідним ресурсом або суб'єктом. Для цього використовуються ідентифікатори активів, категорії загроз, часові інтервали та інші доступні ознаки.

Якщо виявлена активність відповідає вже зареєстрованому інциденту, нові події додаються до його історії. У разі зміни характеру загрози може виконуватися повторне оцінювання критичності.

Якщо відповідного інциденту немає, створюється новий запис. Він повинен містити основні технічні відомості, перелік пов'язаних подій, час виявлення та поточний статус.

Для керування життєвим циклом доцільно передбачити стани реєстрації, перевірки, підтвердження, реагування та завершення. Перехід між ними виконується відповідно до результатів аналізу та дій уповноважених користувачів.

Важливо розмежовувати автоматично виявлену підозрілу активність і підтверджений інцидент інформаційної безпеки. Результат правила може потребувати додаткової перевірки фахівцем. Тому система повинна забезпечувати можливість позначення хибнопозитивних спрацювань і внесення обґрунтування відповідного рішення.

Після усунення проблеми інцидент може бути закритий. Його історія зберігається для подальшого аналізу та оцінювання ефективності механізмів виявлення.

Алгоритм формування рекомендацій і реагування

Після реєстрації потенційного інциденту система може формувати рекомендації щодо подальших дій. Їхнє призначення полягає в наданні адміністратору або аналітику інформації про можливі способи перевірки та локалізації загрози.

Вхідними даними алгоритму є тип інциденту, його критичність, характеристики відповідного ресурсу та встановлені правила реагування.

На першому етапі визначається категорія загрози. Для підозрілих мережевих з'єднань можуть рекомендуватися перевірка адресатів, аналіз активних сеансів та уточнення призначення сервера. Для подій автентифікації доцільно перевіряти історію входів і стан відповідного облікового запису.

Якщо інцидент пов'язаний із хмарним середовищем, рекомендації можуть включати перевірку змін політик доступу, службових ідентичностей та адміністративних операцій.

Окремі захисні дії можуть виконуватися автоматизовано за наявності відповідних механізмів. До них належать тимчасове блокування мережевого з'єднання, обмеження доступу або переведення ресурсу до контрольованого режиму.

Проте автоматичне реагування не є обов'язковою функцією SIEM. Воно потребує окремого механізму виконання дій і визначених адміністративних повноважень. Для цього може застосовуватися підхід Security Orchestration, Automation and Response (SOAR).

Під час виконання автоматичних дій необхідно враховувати можливі наслідки для доступності сервісів. Помилкове блокування мережевого маршруту може порушити роботу критичних систем. Тому для дій із суттєвими наслідками доцільно передбачити підтвердження відповідальної особи.

Результатом алгоритму є набір рекомендованих або дозволених захисних дій із можливістю фіксації їх виконання.

Алгоритм контролю працездатності джерел телеметрії

Достовірність SIEM залежить від повноти надходження інформації. Відсутність подій від мережевого сенсора або хмарного сервісу не означає автоматично відсутності загроз у відповідному сегменті.

Для контролю використовується алгоритм перевірки актуальності джерел. Вхідними даними є час останнього повідомлення, очікувана періодичність надходження та службові показники колекторів.

На першому етапі визначається, чи відповідає поточний інтервал без повідомлень характеру роботи джерела. Для постійно активного мережевого

сенсора тривала відсутність телеметрії може свідчити про порушення збору. Для журналу, який формується лише за певних подій, аналогічна ситуація не завжди є помилкою.

Тому доцільно використовувати спеціальні контрольні повідомлення або перевірку працездатності транспортного каналу. Додатково аналізуються внутрішні показники колекторів, зокрема кількість помилок експорту та обсяг накопиченої черги.

Якщо декілька джерел одночасно перестали передавати дані через один колектор, алгоритм перевіряє можливість спільної причини порушення. Це дозволяє відокремлювати відмову окремого сенсора від недоступності центрального компонента.

Після відновлення зв'язку накопичені повідомлення можуть надходити із затримкою. Їх необхідно обробляти з урахуванням початкового часу виникнення. Результатом алгоритму є актуальна інформація про повноту спостереження та стан телеметричних каналів.

Алгоритм оброблення високої інтенсивності подій

У великих корпоративних і хмарних середовищах кількість повідомлень може суттєво збільшуватися під час пікових навантажень або мережевих атак. Для запобігання перевантаженню аналітичного компонента необхідно передбачити контрольоване оброблення потоків даних.

Вхідними даними алгоритму є поточна інтенсивність надходження повідомлень, стан внутрішніх черг та доступні обчислювальні ресурси.

На першому етапі визначається можливість безпосереднього передавання подій до модуля аналізу. Якщо інтенсивність надходження перевищує поточну пропускну здатність, повідомлення можуть накопичуватися в проміжній черзі.

Як можливий технологічний варіант для такого механізму може використовуватися Apache Kafka або інша система потокового обміну повідомленнями. Вона дозволяє відокремлювати приймання подій від їхнього подальшого опрацювання.

Для паралельного аналізу потік може розподілятися між виконавцями. При цьому необхідно враховувати вимоги кореляції. Події, пов'язані з одним користувачем або мережевим ресурсом, повинні оброблятися таким чином, щоб зберігалася можливість встановлення їхньої часової послідовності.

За значного накопичення повідомлень система повинна контролювати затримку оброблення. Якщо результати аналізу формуються із суттєвим запізненням, їх необхідно відповідно позначати. Подія, отримана раніше, не завжди є актуальною підставою для негайного блокування ресурсу.

Відкидання повідомлень допускається лише відповідно до визначеної політики. Особливу увагу необхідно приділяти збереженню критичних подій і відомостей, необхідних для розслідування інцидентів.

Результатом алгоритму є кероване оброблення потоків інформації з контролем затримки та можливих втрат даних.

Особливості програмної реалізації SIEM

Програмна реалізація системи може передбачати окремі служби збору, нормалізації, кореляції, оцінювання ризиків і керування інцидентами. Такий підхід дозволяє розділяти обчислювальні навантаження та незалежно змінювати параметри відповідних компонентів.

Для зберігання й пошуку подій як один із варіантів може застосовуватися OpenSearch. Він підтримує індексацію структурованих документів і виконання пошукових запитів за відповідними полями. Вибір конкретного сховища залежить від обсягу телеметрії, вимог до швидкості пошуку та тривалості зберігання.

Модуль нормалізації повинен мати розширювану структуру. Для кожного нового формату подій може додаватися окремий аналізатор. При цьому результат перетворення повинен відповідати спільній внутрішній моделі даних.

Правила виявлення доцільно зберігати незалежно від програмного коду модуля кореляції. Це дозволяє змінювати умови перевірок без повного перевстановлення основних компонентів. Для кожного правила необхідно зберігати версію, опис призначення та перелік обов'язкових полів.

Під час виконання складних правил потрібно враховувати обчислювальну складність операцій групування та пошуку. Збільшення часового вікна кореляції підвищує обсяг даних, які необхідно аналізувати. Тому тривалість відповідних інтервалів повинна визначатися характером сценарію виявлення.

Для відображення результатів може використовуватися вебінтерфейс із відповідними інформаційними панелями. Він повинен забезпечувати перегляд поточних інцидентів, фільтрацію подій за джерелом і часом, аналіз пов'язаних записів та контроль стану телеметричних каналів.

Доступ до результатів моніторингу необхідно розмежовувати за ролями. Адміністратор інфраструктури, аналітик безпеки та користувач із правами перегляду можуть мати різні повноваження на зміну правил, закриття інцидентів і виконання захисних дій.

Забезпечення захисту інформації SIEM

Система моніторингу накопичує значний обсяг службової інформації. Вона може містити мережеві адреси, ідентифікатори користувачів, відомості про внутрішню структуру інфраструктури та результати перевірок безпеки. Тому сама SIEM повинна бути захищеною від несанкціонованого доступу.

На першому рівні необхідно забезпечити захист передавання журналів. Для каналів, які підтримують TLS, доцільно використовувати відповідні захищені з'єднання. Для окремих пристроїв можуть застосовуватися спеціалізовані мережеві сегменти або захищені транспортні канали.

Окремо встановлюються правила доступу до централізованого сховища. Користувачі не повинні отримувати необмежені повноваження на видалення або зміну історичних записів без відповідних підстав.

Для підвищення достовірності журналів можуть використовуватися механізми контролю цілісності. Вони дозволяють виявляти несанкціоновану модифікацію збережених даних. У разі необхідності можуть застосовуватися захищені сховища з обмеженою можливістю зміни раніше записаної інформації.

Під час оброблення телеметрії важливо не накопичувати конфіденційні відомості без практичної необхідності. Наприклад, для аналізу мережевих

з'єднань часто достатньо метаданих потоку. Збереження повного прикладного вмісту може створювати додаткові ризики та потребувати окремого обґрунтування.

Для кожної категорії даних визначається термін зберігання. Детальні мережеві записи можуть мати інший період доступності, ніж узагальнені інциденти або результати аналітичних перевірок.

Перевірка коректності алгоритмів і оцінювання ефективності

Для визначення правильності функціонування запропонованого алгоритмічного забезпечення необхідно передбачити комплекс функціональних і навантажувальних випробувань. Початковим етапом є перевірка збору телеметрії від корпоративних і хмарних джерел.

Для цього можуть використовуватися контрольовані повідомлення з відомими значеннями полів. Після надходження до SIEM перевіряється правильність нормалізації, часових позначок та встановлення джерела.

Наступним етапом є перевірка кореляції. Для цього формується набір пов'язаних подій, які моделюють визначений сценарій підозрілої активності. Наприклад, можна використати послідовність невдалих автентифікацій, успішного входу та подальшої зміни хмарних повноважень.

Під час випробування перевіряється можливість правильного об'єднання подій у межах установленого часового інтервалу. Додатково моделюється затримка надходження одного з повідомлень. Це дозволяє оцінити коректність оброблення хмарних журналів, які можуть надходити пізніше за локальні мережеві події.

Для перевірки механізму виявлення аномалій використовуються контрольовані зміни інтенсивності мережевого трафіку. Зокрема, можуть моделюватися збільшення кількості з'єднань, зміна структури DNS-запитів і зростання обсягу переданих даних.

Окремо необхідно оцінити кількість хибнопозитивних спрацювань. Для цього до тестового набору включаються легітимні адміністративні операції та

звичайні зміни навантаження. Результати порівнюються з очікуваною класифікацією.

Для оцінювання продуктивності можуть використовуватися показники кількості оброблених подій за секунду, затримки від отримання події до формування сповіщення та обсягу використаних обчислювальних ресурсів.

Важливо розрізняти час виникнення події, час її надходження до SIEM та час формування результату. Таке розмежування дозволяє визначити, чи пов'язана затримка виявлення з джерелом журналу, транспортним каналом або аналітичним компонентом.

Для перевірки стійкості до відмов можуть моделюватися тимчасова недоступність колектора, зупинка одного з виконавців аналізу та порушення з'єднання з хмарним API. Очікуваним результатом є контрольоване відновлення роботи та правильне відображення неповноти даних.

Кількісні висновки щодо продуктивності, точності виявлення та ефективності кореляції можуть бути сформовані після проведення відповідних експериментів. Для порівняння результатів необхідно використовувати однакові набори подій і визначені умови навантаження.

Запропоноване алгоритмічне забезпечення мережевої SIEM формує послідовний процес моніторингу гібридної хмарно-корпоративної інфраструктури від отримання розподіленої телеметрії до оцінювання загроз та керування інцидентами.

Основне значення має узгодження подій локального й хмарного сегментів, що дозволяє досліджувати пов'язані ознаки небезпечної активності.

Поєднання правил виявлення, статистичного аналізу та контекстного оцінювання створює основу для подальшої програмної реалізації системи й експериментальної перевірки її можливостей.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Практичне використання системи мережевої SIEM передбачає централізоване отримання та аналіз подій інформаційної безпеки з корпоративних і хмарних сегментів інфраструктури. Програмне забезпечення призначене для збору мережевої телеметрії, виявлення підозрілої активності, кореляції подій та оцінювання потенційних кіберзагроз. Його застосування дозволяє об'єднувати відомості від розподілених джерел у спільному середовищі моніторингу. Головне вікно програми показане на рисунку 5.1.

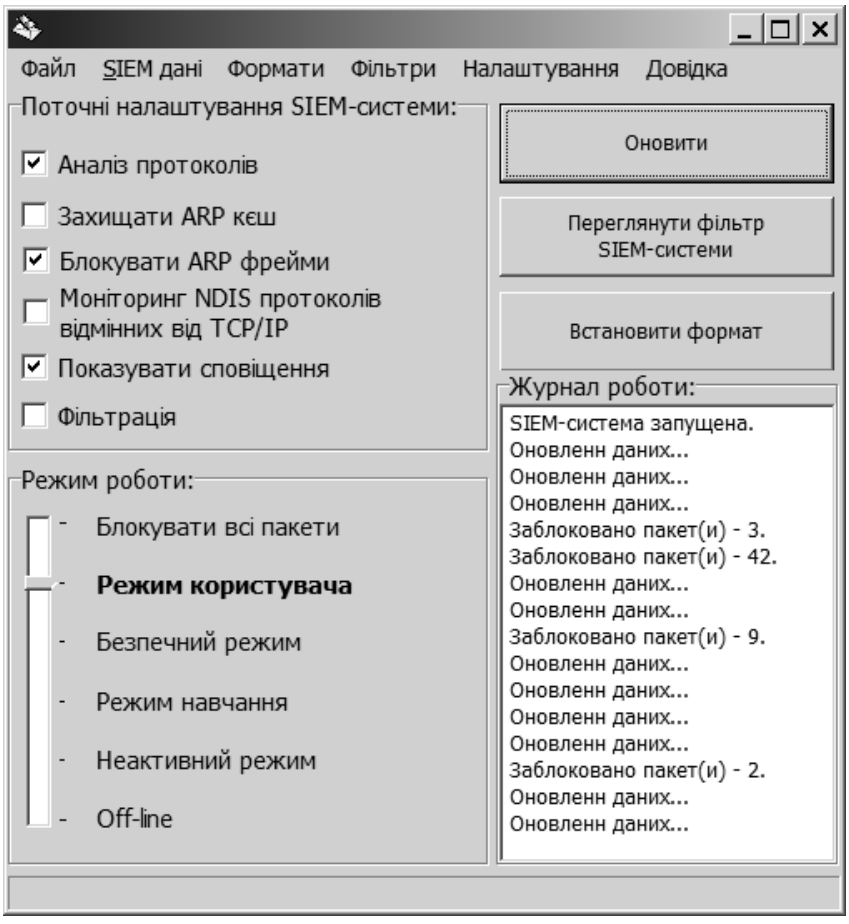


Рисунок 5.1 – Головне вікно ПЗ

Розгортання системи передбачає підготовку серверного середовища, налаштування джерел телеметрії та організацію взаємодії між компонентами оброблення даних. Для гібридної інфраструктури необхідно забезпечити отримання журналів локальних мережевих пристроїв і хмарних сервісів.

При цьому компоненти збору можуть розміщуватися безпосередньо в корпоративній мережі, а централізоване сховище й аналітичні служби на окремому сервері.

Як робоче середовище доцільно використовувати серверну операційну систему Linux із підтримкою необхідних мережевих служб і програмних залежностей. Для ізольованого розгортання компонентів може застосовуватися контейнеризація. Апаратні вимоги визначаються кількістю контрольованих вузлів, інтенсивністю надходження подій і тривалістю зберігання журналів. Особливу увагу необхідно приділити дисковій підсистемі, оскільки накопичення мережевої телеметрії потребує відповідної місткості та продуктивності сховища.

Як можливі засоби отримання мережевої інформації розглядаються Suricata та Zeek. Suricata забезпечує виявлення підозрілої активності за правилами та формування структурованих повідомлень. Zeek дозволяє отримувати відомості про мережеві з'єднання та події прикладних протоколів. Для приймання журналів маршрутизаторів, міжмережевих екранів і серверів може використовуватися Syslog. Конкретний склад інструментів залежить від фактичної реалізації програмного комплексу.

Для централізованого зберігання подій може застосовуватися OpenSearch або інше сховище, яке підтримує індексацію структурованих записів. За високої інтенсивності телеметрії можливе використання Apache Kafka як проміжного компонента передавання повідомлень. Він дозволяє відокремити приймання подій від їхнього подальшого аналізу. Застосування брокера визначається очікуваним навантаженням і прийнятою архітектурою системи.

Підготовка корпоративного сегмента починається з визначення мережевих ділянок, які підлягають моніторингу. Для мережевих сенсорів необхідно забезпечити доступ до копій трафіку через SPAN-порт комутатора або інший

підтримуваний механізм. Після цього перевіряється працездатність інтерфейсу захоплення та можливість формування подій. Для пристроїв, які передають журнали через Syslog, налаштовуються адреса приймального колектора, відповідний транспорт і дозволені мережеві з'єднання.

Окремим етапом є підключення хмарних джерел. Залежно від використовуваної платформи можуть застосовуватися журнали AWS CloudTrail, VPC Flow Logs або відповідні сервіси аудиту Microsoft Azure. Для отримання даних створюється службова ідентичність з обмеженими повноваженнями на читання необхідних журналів. У конфігурації визначаються хмарні облікові записи, контрольовані ресурси та параметри доступу до API. Секретні облікові дані не повинні включатися безпосередньо до вихідного коду.

Перед запуском системи необхідно забезпечити мережеву доступність її компонентів. Колектори повинні мати можливість передавати події до центрального вузла оброблення. Для взаємодії між корпоративним і хмарним сегментами доцільно застосовувати захищені канали. Параметри мережевого доступу визначаються з урахуванням політик міжмережевих екранів. Додатково забезпечується синхронізація системного часу серверів, необхідна для правильної кореляції подій.

Після підготовки транспортних каналів налаштовується компонент нормалізації. Для кожного типу джерела визначається спосіб оброблення повідомлень і зіставлення полів із внутрішньою моделлю даних. Як основа уніфікації може використовуватися Open Cybersecurity Schema Framework (OCSF). Особливу увагу необхідно приділити правильності визначення часу події, IP-адрес, ідентифікаторів користувачів і мережевих ресурсів. Некоректні повідомлення повинні відокремлюватися для діагностики.

Наступним етапом є налаштування правил виявлення загроз. Для аналізу журналів можуть використовуватися правила Sigma, адаптовані до обраного механізму пошуку. Мережеві спрацювання Suricata можуть передаватися до спільного аналітичного компонента. Для кожного правила визначаються

необхідні поля, умови спрацювання та рівень критичності. Кореляційні правила додатково потребують налаштування часових інтервалів і ознак об'єднання подій.

Для оцінювання загроз необхідно підготувати відомості про контрольовані інформаційні ресурси. До них належать сервери, мережеві сегменти, облікові записи та хмарні служби. Для кожного об'єкта за можливості встановлюються його функціональне призначення та критичність. Такі характеристики дозволяють враховувати значущість ресурсу під час визначення пріоритетності сповіщень. Без відповідних інвентаризаційних даних система повинна зберігати можливість аналізу подій з обмеженим контекстом.

Рекомендована послідовність запуску передбачає початкову активацію сховища подій і перевірку його доступності. Якщо використовується брокер повідомлень, він запускається до початку приймання основного потоку телеметрії. Далі активуються компоненти нормалізації та аналітичної обробки. Після перевірки їхньої працездатності запускаються мережеві колектори й адаптери хмарних сервісів. Завершальним етапом є запуск користувацького інтерфейсу та засобів керування інцидентами.

Після запуску виконується первинна перевірка надходження телеметрії. Для цього контролюється отримання повідомлень від кожного зареєстрованого джерела. Необхідно переконатися в правильності визначення типу події, її часової позначки та мережевих параметрів. Окремо перевіряється відповідність кількості активних джерел фактичній конфігурації інфраструктури. Відсутність повідомлень від окремого пристрою повинна відображатися як стан, що потребує перевірки. Для перевірки кореляційного механізму доцільно використовувати контрольовану послідовність тестових подій. Наприклад, можуть моделюватися декілька невдалих спроб автентифікації з подальшим успішним входом і зміною хмарних повноважень. Під час тестування перевіряється правильність об'єднання пов'язаних записів та формування відповідного сповіщення. Такі випробування необхідно проводити в дозволеному тестовому середовищі без порушення роботи продуктивної інфраструктури.

Окремо перевіряється оцінювання критичності. Для цього використовуються події, пов'язані з ресурсами різного функціонального призначення. Контролюється, чи враховує система важливість активу та наявність незалежних ознак загрози. Після формування сповіщення перевіряється створення інциденту, відображення пов'язаних подій і можливість зміни його стану уповноваженим користувачем.

Для ідентифікації створеного програмного продукту передбачається представлення відомостей про його розробника. Ці дані використовуються для встановлення авторства програмного забезпечення та його подальшого технічного супроводження. Інформація про автора системи мережевої SIEM представлена на рисунку 5.2.

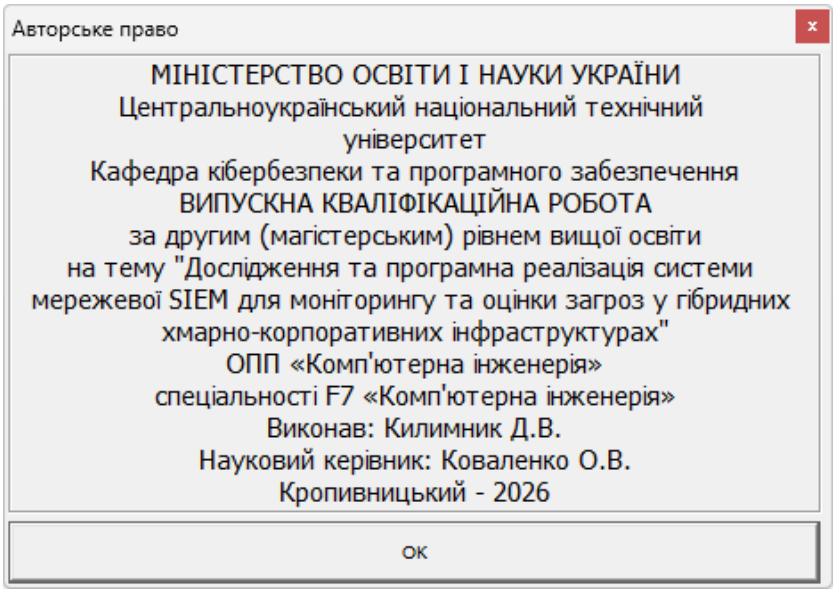


Рисунок 5.2 – Авторське право

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Метою розробки є дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Об'єктом дослідження є процес мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Предметом дослідження є методи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Методи дослідження базуються на методах побудови комп'ютерних мереж, методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

– Розроблено вітчизняний продукт мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

Комп'ютерні технології широко впроваджуються в усі сфери сучасної суспільної та виробничої діяльності. Впровадження комп'ютерних технологій принципово змінило характер праці різних категорій фахівців. Працівники, які використовують комп'ютерну техніку на своїх робочих місцях, на своєму досвіді оцінили її величезні можливості. Одночасно виникла певна безтурботність при її експлуатації.

Недотримання вимог безпеки призводить до того, що й через кілька днів роботи за комп'ютером співробітник починає відчувати певний дискомфорт: в нього виникає головний біль і різь у власних очах, з'являються почуття виснаження й дратівливість. В окремих людей порушується сон, погіршується зір, занедужують руки, шия, поперек тощо.

До недоліків умов праці користувачів комп’ютерної техніки можна віднести:

– недостатню площу і обсяг виробничого приміщення;

– недотримання вимог, мікроклімату на робочих місцях;

– низький рівень освітленості у приміщеннях і на робочих поверхнях апаратури;

– підвищений рівень низькочастотних магнітних полів від моніторів;

– порушення вимог організації робочих місць;

– недотримання вимог до режимам праці та відпочинку;

– надмірне виробничу навантаження працівників;

– відсутність навичок зниження впливу психоемоційного напруги.

Відповідно до ст.14 Закону «Про охорони праці» [1] на роботодавця покладено обов'язок забезпечити: безпеку працівників при експлуатації устаткування; застосування коштів індивідуальної захисту працівників;

відповідні вимоги охорони праці, умови праці в кожному робоче місце; дотримання режиму праці та відпочинку працівників; навчання безпечним методам і прийомам виконання; інструктаж з охорони праці; організацію контролю над станом умов праці в робочих місць; проведення атестації робочих місць в умовах праці.

Максимально зменшити кількість шкідливих впливів на людину при високій продуктивності праці, створити комфортні умови для роботи людей – ось одна з головних задач охорони праці.

7.2 Аналіз умов праці ІТ-працівників

Приміщення розташовано на третьому поверсі п'ятиповерхового будинку. У приміщенні розташовано 3 робочих місця з комп'ютерами (далі ПК). Відповідно до норм «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98 [2] площа, що відводиться для робочого місця з комп'ютером повинна бути не менше 6 м^2, об'єм не менше 20 м^3. Розміри даного приміщень складають: довжина – 6 м, ширина – 4,5 м, висота – 3,5 м, тобто загальна фактична площа складає 27 м^2. Необхідна площа на 3 робочих місця із установленими ПК складає 18 м^2, що не перевищує фактичну. Обсяг приміщення на одного працюючого складає 31,5 м^3, отже відповідає нормі ДСанПіН 3.3.2-007-98 – не менше 20 м^3.

При роботі з ПК людина може піддатися впливу шкідливих та небезпечних факторів. Під шкідливими виробничими факторами розуміють фактори, тривалий вплив яких викликає розвиток професійних захворювань. Небезпечні виробничі фактори – вплив яких на працюючого викликає травму, тобто пошкодження організму. Шкідливі і небезпечні чинники, з якими стикається ІТ-працівник при роботі з ПК, приведені в таблиці 7.1.

По категорії вибухо- і пожежонебезпеки, згідно дане приміщення відноситься до категорії В – пожежонебезпечне, тому що присутні тверді

матеріали, що горять, такі як дерев'яні столи, папір і інше. Виходячи з категорії пожежонебезпеки і поверховості будинку, ступінь вогнестійкості будівлі II. Згідно з ДБН В 1.1-7-2016 «Пожежна безпека об’єктів будівництва» [3] ЕОМ повинні розташовуватись в будівлі не менше ніж II ступню вогнестійкості.

Таблиця 7.1 – Перелік шкідливих та небезпечних виробничих факторів

Найменування факторів	Можливі джерела їх виникнення	Характер дії
Небезпека ураження електричним струмом	Мережа живлення	Небезпечний
Пожежонебезпечність приміщень	Наявність матеріалів, що згорають і джерел запалення (електроапаратура)	Небезпечний та шкідливий
Іонізація повітря	Статична електрика випромінювання	Шкідливий
Підвищений рівень шуму	Шум створюється перетворювачем напруги ЕОМ, її технічною периферією, а також людьми, що працюють в приміщенні	Шкідливий
Несприятлива освітленість	Недостатнє штучне і природне освітлення	Шкідливий
Незадовільні параметри мікроклімату	Незадовільний стан системи опалення і вентиляції	Шкідливий
Психофізіологічні напруження	Монотонність праці, перенапруженість зорових аналізаторів, розумова напруженість, незручність і статичність пози	Шкідливий

За ступенем небезпеки поразки людей електричним струмом відділ класифікується як приміщення з підвищеною небезпекою, тому що не

виключена можливість одночасного дотику людини до маючих з'єднання з землею конструкціям будинку, з одного боку, і до металевих корпусів електроустаткування, що можуть виявити під напругою – з іншого.

Для забезпечення вищевказаних оптимальних мікрокліматичних умов у помешканні передбачена система опалення (загальне парове) в холодному періоді, та вентиляція і кондиціювання в теплий період року, згідно ДБН2.5–67–2013 «Опалення, вентиляція та кондиціювання» [4]. При виконанні замірів параметрів мікроклімату, значення їх відповідали оптимальним та допустимим параметрам відповідно до ДСанПіН3.3.2.007 – 98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно – обчислювальних машин».

Припустимий рівень іонізації повітря помешкання відповідно до СН 21.52-80 повинен складати 1500 – 3000 один./м^3.

Нормування освітлення здійснюється відповідно до ДБН В.2.5 – 28 – 2006 «Природне та штучне освітлення». [5]

Відділ забезпечений комбінованим освітленням. В темний час доби передбачається загальне і/або місцеве рівномірне штучне, а в світлий – бокове одностороннє природне освітлення два віконних прорізи.

Одним з найбільш поширеніших чинників виробничого середовища, який несприятливо впливає на людину, є шум. Вплив шуму на організм людини залежить від рівня звукового тиску, частотних характеристик, тривалості дії, а також індивідуальних особливостей людини.

При тривалій дії шуму у оператора ЕОМ виявляються симптоми утомленості, нервового збудження, що сприяють погіршенню працездатності і допущенні помилок при роботі. Для уникнення шкідливої дії шуму на організм працюючого, необхідне дотримання нормованих параметрів, які не повинні перевищувати допустимих величин. При роботі на комп'ютері рівень шуму не повинен перевищувати 50 дБА. Приміщення розташоване вікнами у двір і знаходиться далеко від проїжджої частини вулиці. Основними джерелами шуму в приміщенні є устаткування і люди. Розглянуте приміщення не призначене для

прийому відвідувачів і тому в ньому не спостерігається великого скупчення людей. Тому основним джерелом шуму є комп'ютерна техніка.

Джерелами шуму при роботі ЕОМ є механічні частини принтера, що рухаються, і вентилятори (Lпк = 35 дБА, Lprn = 48 дБА) При роботі вентиляційної системи, що забезпечує оптимальний температурний режим електронних блоків ЕОМ і вмонтована в задню панель, створюється аеродинамічний шум. Шум, створюваний працюючим комп'ютером, може бути охарактеризований як широко смуговий постійний з аперіодичним посиленням при роботі принтера. Час роботи ПЕОМ – 6 – 8 год. за добу; принтери працюють не більш 1,5-2 год. за добу.

При наявності великої кількості джерел шуму еквівалентне значення шуму $L_{ЭКВ}$, дБА розраховують по наступній формулі:

$$L_{екв}=10\cdot\lg\left(\frac{1}{T}\sum_{i=1}^{n}\left(t_i\cdot 10^{0.1\cdot L_i}\right)\right) \qquad (7.1)$$

де:

L_i – рівень шуму і-го джерела (пристрою);

t_i – час роботи і-го джерела (пристрою);

T – загальний час роботи;

n – кількість джерел шуму даного типу.

Для даного приміщення ці значення складають:

Загальний час роботи – робочий день, тобто T=8 годин.

Для фонового шуму (вентиляторів):

L_1 = 35 дБА, T_1 = 8 годин, n_1=15 (5x3);

Для лазерного принтера Lexmark Jet:

L_2 = 48дБА, T2 = 2 години, n_2=1,

для сканера L_3 = 46дБА, T3 = 2 години.

Підставляємо отримані величини у формулу (7.1):

$$L_{екв}=10\cdot\lg\left(\frac{1}{8}\cdot\left(15\cdot 8\cdot 10^{0.1\cdot 35}+1\cdot 2\cdot 10^{0.1\cdot 48}+1\cdot 2\cdot 10^{0.1\cdot 46}\right)\right)=46{,}3\ \text{дБА}$$

Таким чином, еквівалентний рівень шуму в приміщенні за робочий день $L_{екв}$ = 46,3 дБА, тобто не перевищує норму 50 дБА.

7.3 Техніка безпеки та протипожежна профілактика

Відповідно ДБН В 1.1-7-2016 «Пожежна безпека об’єктів будівництва» будинок можна віднести до II групи по ступені вогнестійкості й до категорії Д по ступені пожежонебезпеки.

Від розподільного щита по праву й ліву сторони встановлені кондиціонери, зовнішня електропроводка, поміщена в ізольований кабель. Висота проводки становить 2,2 м від рівня підлоги, її кріплення здійснюється за допомогою металевих власників. Біля кожного стола організований розподільний щит, розташований на текстолітовій пластинці, закріпленої на стіні на рівні 1м від підлоги. Усього до складу входять п'ять розеток і дві клеми заземлення.

Всі обчислювальні машини з'єднані із клемами заземлення. Чотири з п'яти розеток забезпечують подачу напруги 220 V, а одна, забезпечує подачу напруги в 36 В. Про це є відповідні написи на кожному розподільному щиті.

Робота обслуговуючого персоналу полягає в інсталяції необхідного програмного забезпечення й наступному його використанні в діалоговому режимі роботи з ЕОМ. Іноді може виникати необхідність написання допоміжних програм для поліпшення роботи вузла або для зниження витрат.

З погляду забезпечення умов праці й вимог техніки безпеки для роботи програміста необхідно наступне: достатнє висвітлення екрана дисплея й робочого місця; повна технічна справність устаткування, його електробезпечність; достатня пожежобезпечність приміщення; оптимальний мікроклімат, що сприяє продуктивній роботі; відповідність робочого місця вимогам ергономіки.

До небезпечних і шкідливих факторів, дії яких піддається програміст, можна віднести: можливість поразки електричним струмом, при електроні

справності встаткування, порушенні заземлення або техніки безпеки; робота в мікрокліматі з неприпустимими параметрами; робота при недостатній освітленості екрана дисплея й робочого місця.

Відповідно НПАОП 40.1-1.21-98 “Правил безпечної експлуатації електроустановок споживачів” [6], приміщення можна віднести до приміщень без підвищеної небезпеки, оскільки це приміщення, сухе, з нормальною температурою й ізолюючими підлогами, що не має заземлених металоконструкцій.

Персональні ЕОМ можна віднести до першого класу електротехнічних виробів по способі захисту людини від поразки електричним струмом, оскільки їхні корпуси зроблені з ізолюючої пластмаси й кожен пристрій має заземлення. Відповідно правилам пристрою електроустановок ЕОМ можна віднести до електроустановок з робочою напругою до 1000 В.

Однієї з достовірних причин пожежі в приміщенні з обчислювальною технікою може бути коротке замикання, що спричиняє спалах електропроводки. Для його попередження вся обчислювальна техніка, а також інші електричні пристрої повинні бути обладнані плавкими запобіжниками, а на вході електромережі повинен бути передбачений автомат захисту.

Не слід користуватися електричними подовжувачами й трійниками, що не мають сертифікатів відповідності вимогам безпеки.

Необхідно передбачити наявність у межах досяжності первинних засобів гасіння пожежі (вогнегасників) для локалізації вогню власними засобами до приїзду команди пожежної охорони. Повинен бути розроблений план екстреної евакуації персоналу при виникненні загоряння. Кількість евакуаційних виходів повинне бути не менш двох. Допускається використання одного евакуаційного виходу, якщо відстань найбільш віддаленого робочого місця до цього виходу не перевищує 25 м.

7.4 Розробка заходів з охорони праці

Перерахуємо проведені заходи щодо забезпечення умов праці на робочому місці програміста.

Для зменшення шуму в приміщенні пропонується використовувати замість матричного принтера, що створює багато шуму, більш тихий – лазерний принтер.

З точки зору забезпечення електробезпеки до цих заходів можна віднести: устаткування розподільних щитів спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв; періодична перевірка всіх приладів і пристроїв; щорічна здача іспитів з охорони праці.

З точки зору забезпечення оптимальних умов мікроклімату і освітленості до цих заходів можна віднести: організацію природної вентиляції, за допомогою дефлектора, для забезпечення необхідного повітрообміну в приміщенні вузла; організацію системи центрального опалювання, для підтримки оптимальної температури в холодний період року; організацію штучного загального освітлення, для забезпечення необхідних умов зорової роботи, що відповідають, оформлення паспорта на приміщення вузла, з занесенням в нього вимірювань освітленості, проведених відділом охорони праці.

В якості мір по зниженню шуму можна запропонувати:

– облицювання стелі і стін звукопоглинаючим матеріалом (знижують шум на 6-8 до);

– екранування робочого місця (встановленням перегородок, діафрагм);

– установка в комп'ютерних приміщеннях устаткування, що викликає мінімальний шум;

– раціональне планування приміщення.

З точки зору забезпечення пожежної безпеки до цих заходів можна віднести наявність схеми евакуації з приміщення вузла, у випадку пожежі, повішену на вхідні двері.

7.5 Висновки до розділу

У даному розділі магістерської роботи були виконано аналіз умов праці користувачів ПК, які працюють у зазначеному приміщенні Проведено перевірка організації робочого місця із відповідними замірами параметрів мікроклімату, освітлення, рівня шуму та розрахунком рівня шуму.

Розроблені заходи щодо поліпшення умов праці дотримання техніки безпеки та проведення протипожежної профілактики дозволить створити умови, які будуть забезпечувати більш комфортну роботу.

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

– Досліджена система мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Visual C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Килимник Д.В. Дослідження та програмна реалізація системи мережевої SIEM для моніторингу та оцінки загроз у гібридних хмарно-корпоративних інфраструктурах // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.
2. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 p.
3. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
4. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
5. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
6. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
7. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p
8. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
9. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
10. Богаченко, С., Смірнов, О., Буравченко, К., Смірнова, Т., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С. «Обмеження ресурсів мобільних та edge-платформ при розробці програмного забезпечення для реалізації та оптимізації моделей машинного навчання». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, т. 2 № 34, С. 677-686.
11. Вінтенко Б.Ю., Смірнова Т.В., Миронець І.В., Смірнов О.А., Буравченко К.О. «Метод оцінки функціональної стійкості комп'ютерно-

орієнтованих процедур системи підтримки оперативного персоналу АЕС». *Системи управління, навігації та зв'язку,* 2026, вип. 2(84), С. 62-69.

12. Смірнова Т.В., Усік П.С., Лисенко І.А., Буравченко К.О., Смірнов О.А. «Методологія підтримки технологічних процесів у критичній інфраструктурі з забезпеченням безпеки інформації на основі хмарних технологій». *Безпека інформації.* 2025. Том 31 № 1. С. 49-60.

13. Смірнова Т.В., Буравченко К.О., Добринчук О.А., Смірнов С.А., Якименко Н.М., Смірнов О.А. «Хмарна технологія моніторингу ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі». *Центральноукраїнський науковий вісник. Технічні науки.* 2025. № 12(43), ч. II. С. 36-54.

14. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С. 413-427.

15. Vintenko, B., Myronets, I., Smirnov, O., Smirnova, T. «Enhancing the Reliability of Input Data for Nuclear Power Plant Operator Support Systems». *International Conference on Sensors, Devices and Systems. SDaS 2025. Lecture Notes in Electrical Engineering*, 2026. vol 1617. pp 3-12/

16. Kuznetsov O., Frontoni E., Arnesano M., Smirnov O., Khruskov B. «Biometric Authentication in TinyML: Opportunities and Challenges». *Tiny Machine Learning: Design Principles and Applications*, 2026, pp. 587-633.

17. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.

18. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». *Ceur Workshop Proceedings,* 2025, 4024, pp. 530–542.

19. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи

інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.

20. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025

21. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.

22. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

23. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.

24. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.

25. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop*

Proceedings, 2024, 3909, pp. 227–241.

26. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.

27. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.

28. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2024. № 2(26), С. 170–188.

29. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка.* 2024. №4(24), С. 6-27.

30. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка.* 2024. №3(23), С. 111-131.

31. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології,* 2024, № 13, с. 28-35.

32. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

33. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.

34. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56

35. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings,* Volume 3530, 2023, pp. 256-265.

36. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings,* Volume 3504, 2023, pp. 1-11.

37. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». *In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.

38. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.

39. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». *ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)»* м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

40. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». *VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення,* м. Кропивницький. 1

листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.

41. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». *VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення,* м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

42. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 170-178.

43. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings,* Volume 3187, 2022,

44. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.

45. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління,* № 2(70). 2022. С. 28-37.

46. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку,* 2022, № 3(69). С. 93-98.

47. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного

захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.

48. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

49. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021,* Cracow, Poland, 22-25 September 2021. P. 414-418

50. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) – 2021*, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

51. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020,* Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

52. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». *CEUR Workshop Proceedings* Volume 2805, 2020, Pages *44-58.*

53. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.

54. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.

55. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.

56. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 122-131.

57. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 1-14.

58. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». *Lecture Notes in Networks and Systems*, vol 152. Springer, Cham. 2021, pp 66-84.

59. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 161-165.

60. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 166-171.