

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА**

Факультет прикладної математики та інформатики

(повне найменування назва факультету)

Кафедра програмування

(повна назва кафедри)

**КУРСОВА РОБОТА**

**РОЗРОБКА SIEM СИСТЕМИ ДЛЯ МОНТОРИНГУ ПОДІЙ БЕЗПЕКИ  
ОРГАНІЗАЦІЙ**

Виконала: студентка групи ПМІ-31

спеціальності 122 Комп'ютерні науки

(шифр і назва спеціальності)

Харитонов А. Ю.

(підпис)

(прізвище та ініціали)

Керівник Рикалюк Р. Є.

(підпис)

(прізвище та ініціали)

## ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ПОРІВНЯННЯ ТА АНАЛІЗ.....	4
1.1 Порівняння існуючих застосунків.....	4
1.2 Аналіз проблеми.....	5
РОЗДІЛ 2. МЕТОДИ, АРХІТЕКТУРА ТА ТЕХНОЛОГІЇ РОЗРОБКИ.....	7
2.1 Технології.....	7
2.2 База даних.....	9
2.3 Архітектура застосунку.....	10
РОЗДІЛ 3. ОГЛЯД ОСНОВНИХ ФУНКЦІЙ ТА МОЖЛИВОСТЕЙ ЗАСТОСУНКУ.....	12
3.1 Основні функції.....	12
3.2 Тестування роботи.....	18
ВИСНОВКИ.....	21
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	22

## ВСТУП

В наш час безпека є однією з найважливіших складових як особистого так і професійного життя. Зростаюча кількість кібератак на приватні та державні структури створює постійну загрозу втрати даних та підриву довіри до цифрових сервісів. У цих умовах важливо не лише виявляти, а й здійснювати моніторинг та попередження загроз. У цьому допомагають системи управління інформаційною безпекою, зокрема SIEM (Security information and event management) системи.

Актуальність. Власне виробництво такого продукту, орієнтованого на український ринок і розробленого з урахуванням локальних особливостей інфраструктур, має стратегічне значення: воно знижує ризики витоку конфіденційної інформації за межі країни, також зменшить залежність організацій від іноземного програмного забезпечення та сприяє розвитку національної цифрової безпеки.

Мета роботи. Розробка функціональної системи, яка збирає, обробляє, аналізує та реагує на загрози, характерні для інформаційних систем. Особливість – простота застосування, мінімальні вимоги до ресурсів та можливість подальшого розширення можливостей.

Завдання роботи. Аналіз вимог до сучасних систем захисту від кібер атак; побудова архітектури та модулів системи; розробка інтерфейсу користувача; тестування на типових сценаріях.

## РОЗДІЛ 1

### ПОРІВНЯННЯ ТА АНАЛІЗ

#### 1.1 Порівняння існуючих застосунків

На сучасному ринку інформаційної безпеки представлено широкий спектр SIEM – систем, кожна з яких має свої переваги та недоліки[1]. Ці системи забезпечують комплексну безпеку інформаційних інфраструктур організацій, надаючи можливість збору та аналізу подій безпеки.

##### 1) Splunk Enterprise Security

Переваги:

- Потужні аналітичні можливості та гнучка мова пошуку (SPL).
- Широка екосистема з понад 2,800 додатками та інтеграціями.
- Підтримка хмарних, локальних та гібридних розгортань.

Недоліки:

- Висока вартість, особливо при великому обсязі даних.
- Складність у налаштуванні та потреба в навчанні персоналу.

##### 2) IBM QRadar

Переваги:

- Глибока інтеграція з іншими продуктами IBM.
- Потужна кореляція подій та поведінковий аналіз.
- Підтримка хмарних та локальних розгортань.

Недоліки:

- Обмежена кількість інтеграцій з сторонніми рішеннями (близько 600).
- Складна структура ціноутворення та потенційно високі витрати.
- Менш активна спільнота порівняно зі Splunk.

##### 3) LogRhythm NextGen SIEM

Переваги:

- Інтуїтивно зрозумілий інтерфейс та простота використання.
- Вбудовані аналітичні можливості та автоматизація реагування.
- Підходить для середніх та великих організацій.

Недоліки:

- Може бути ресурсомістким та вимагати значних інфраструктурних витрат.
- Обмежена масштабованість для дуже великих середовищ.

#### 4) AlienVault USM (AT&T Cybersecurity)

Переваги:

- Комплексне рішення з вбудованими можливостями виявлення загроз.
- Доступна ціна, що робить його привабливим для малих та середніх бізнесів.
- Швидке розгортання та простота налаштування.

Недоліки:

- Обмежені можливості масштабування для великих організацій.

Сучасні системи розвиваються у напрямку інтеграції технологій штучного інтелекту та машинного навчання. Це дозволяє уникнути кількості хибних спрацювань та підвищити ефективність виявлення складніших загроз. Наступний рівень – SOAR – система (security orchestration, automation, and response) – набір служб та інструментів, які автоматизують запобігання та реагування на кібератаки.

## 1.2 Аналіз проблеми

Через збільшення складності IT-інфраструктур організації все частіше стикаються із великою кількістю кібератак. Основна проблема – відсутність централізованого підходу до моніторингу та аналізу подій у реальному часі. Це ускладнює своєчасне виявлення та реагування на атаки, збільшує час на розслідування та усунення наслідків.

Інша проблема – великий обсяг даних про події безпеки. Навіть з незначною кількістю пристроїв їх аналіз кожного займатиме час, який у критичній ситуації є дуже важливим.

Недостатня видимість загальної картини безпеки організації ускладнює процес прийняття рішень щодо вдосконалення рівня захисту IT-інфраструктури,

тому використання єдиної системи збору подій безпеки допоможе оцінити реальний стан захищеності.

Мій продукт — це легка SIEM-система, створена для українського ринку з урахуванням локальних особливостей:

- Доступність: безкоштовний веб застосунок, орієнтований на малі організації.
- Локалізація: інтерфейс українською мовою, адаптація під локальні стандарти.
- Простота впровадження: не вимагає складної інфраструктури.
- Основні функції: збір логів, базова нормалізація, фільтрація за ключовими подіями, генерація та надсилання звітів у Telegram – бот.

## РОЗДІЛ 2

### МЕТОДИ, АРХІТЕКТУРА ТА ТЕХНОЛОГІЇ РОЗРОБКИ

#### 2.1 Технології

- Мова програмування: Python

Python – універсальна мова, яку можна використовувати для розробки веб – додатків, автоматизації завдань. Також наявна велика система бібліотек і фреймворків, які дозволяють працювати з шифруванням, мережевими протоколами та аналізом даних.

Підтримка різних операційних систем дозволить користувачам користуватись продуктом незалежно від операційної системи.

Крім цього, Python активно використовується у сфері комп'ютерної криміналістики [5].

- СКБД: PostgreSQL

PostgreSQL – об'єктно-реляційна система керування базами даних. Об'єктно – реляційна СКБД подібна до реляційної, але з об'єктно-орієнтованою моделлю бази: класи та наслідування підтримуються в схемі даних та мові запитів.

Для розробки SIEM систем така СКБД підходить [7] тому, що:

- 1) підтримує транзакції, складні запити та індексацію, повна реалізація ACID властивості
- 2) можливість створювати власні типи даних
- 3) керування паралельним доступом за допомогою багатоверсійності (MVCC – multi version concurrency control)
- 4) три рівні безпеки: мережевий, транспортний та рівень даних

*ACID (Atomicity, Consistency, Isolation, Durability)* – це набір властивостей, що гарантують надійну роботу транзакцій бази даних [5].

- *Атомарність (Atomicity)*. Забезпечує, що кожна транзакція розглядається як один блок, тобто вона або виконується повністю, або взагалі не виконується. Якщо станеться помилка всередині роботи транзакції, база даних повернеться назад і зміни в даних не відбудуться.

- *Узгодженість (Consistency)*. Після виконання транзакції, база даних переходить з одного правильного стану в інший. Навіть якщо є складні залежності чи умови результат буде правильним.

- *Ізоляція (Isolation)*. Транзакції виконуються незалежно одна від одної. Проміжні результати однієї транзакції не повинні бути доступні іншим.

- *Довговічність (Durability)*. Гарантує, що результати виконаних транзакцій будуть збережені.

- Flask – мікрофреймворк, що дозволяє легко та швидко створити веб-додаток. Для SIEM систем часто треба інтегрувати різні джерела і формати, також flask підтримує багато бібліотек для роботи з базами даних. Можна інтегрувати машинне навчання.

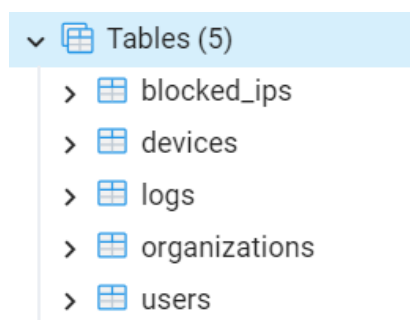
- Jinja – шаблонізатор, інтегрований у Flask і використовується для формування динамічних HTML-сторінок. Для систем моніторингу це важливо, адже інформація про логи, пристрої та атаки постійно змінюється і її потрібно оперативно відображати. Використання Jinja у поєднанні з Flask робить систему гнучкою, швидкою та зручною.

- JavaScript – забезпечує асинхронну взаємодію з сервером, дозволяє оновлювати список подій у реальному часі, блокувати IP-адреси, переглядати деталі атак.



## 2.2 База даних

Структура бази даних:



База даних складається з 5 таблиць: організації, користувачі, пристрої, логи та заблоковані IP-адреси:

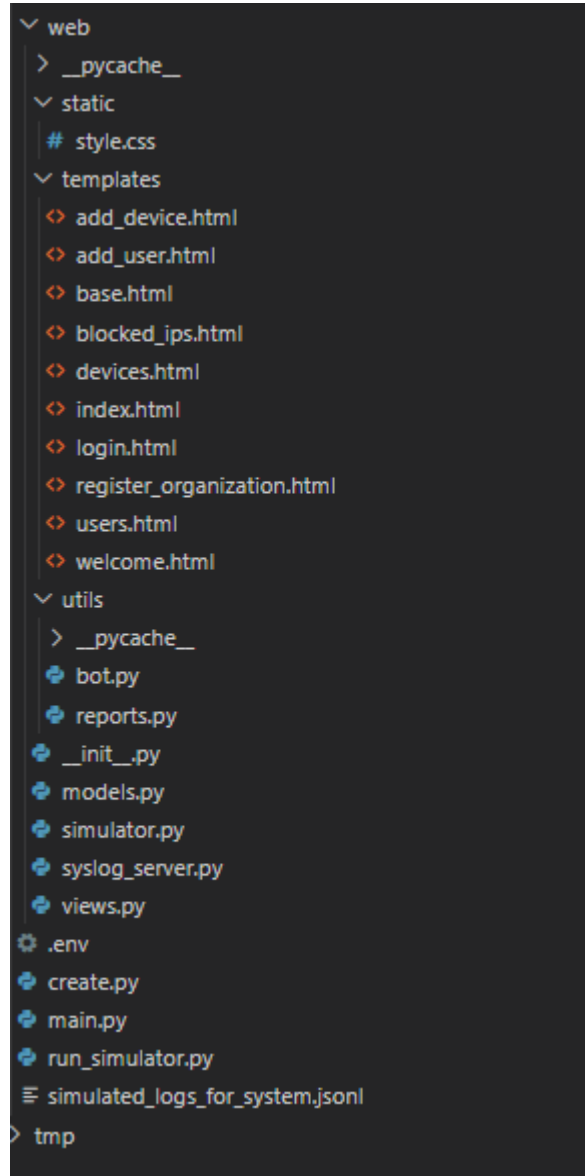
- Таблиця “organizations”:
  - id: унікальний ідентифікатор організації
  - name: назва
  - created\_at: дата та час реєстрації організації
- “users”:
  - id: унікальний ідентифікатор користувача
  - email: унікальна електронна адреса користувача
  - role: роль користувача (admin, user)
  - organization\_id: зовнішній ключ, посилання на таблицю *organizations*
  - created\_at: дата та час створення(додавання) облікового запису
  - last\_login: дата та час останнього входу
- “devices”:
  - id: унікальний ідентифікатор пристрою
  - organization\_id: зовнішній ключ, посилання на таблицю *organizations*
  - name: назва пристрою
  - ip\_address: IP-адреса
  - mac\_address: MAC-адреса пристрою
  - type: тип пристрою
  - last\_seen: час останньої активності

- is\_active: значення активності пристрою
- “logs”:
  - id: унікальний ідентифікатор журналу
  - organization\_id: зовнішній ключ, посилання на таблицю *organizations*
  - device\_id: зовнішній ключ, посилання на таблицю *devices*
  - event\_type: тип події
  - severity: рівень важливості
  - details: деталі події
  - created\_at: дата та час створення логу
- “blocked\_ips”
  - id: унікальний ідентифікатор запису блокування
  - ip\_address: IP-адреса, яка була заблокована
  - reason: причина блокування
  - blocked\_by: зовнішній ключ, посилання на таблицю *users*, вказує хто заблокував
  - blocked\_at: дата і час блокування

## 2.3 Архітектура застосунку

Архітектура мого застосунку – клієнт-серверна. Модель такої системи полягає в тому, що клієнт відправляє запит на сервер, де він обробляється і готовий результат надсилається назад клієнтові. Сервер може обробляти запити кількох клієнтів одночасно, що забезпечує масштабованість.

Серверна частина реалізована з використанням Flask, який обробляє запити, взаємодіє з базою даних. Клієнтська частина – веб-інтерфейс, де інформація динамічно оновлюється за допомогою JavaScript, що дозволяє відображати логи у реальному часі.



*Структура файлів та директорій проекту*

## РОЗДІЛ 3

### ОГЛЯД ОСНОВНИХ ФУНКЦІЙ ТА МОЖЛИВОСТЕЙ ЗАСТОСУНКУ

#### 3.1 Основні функції

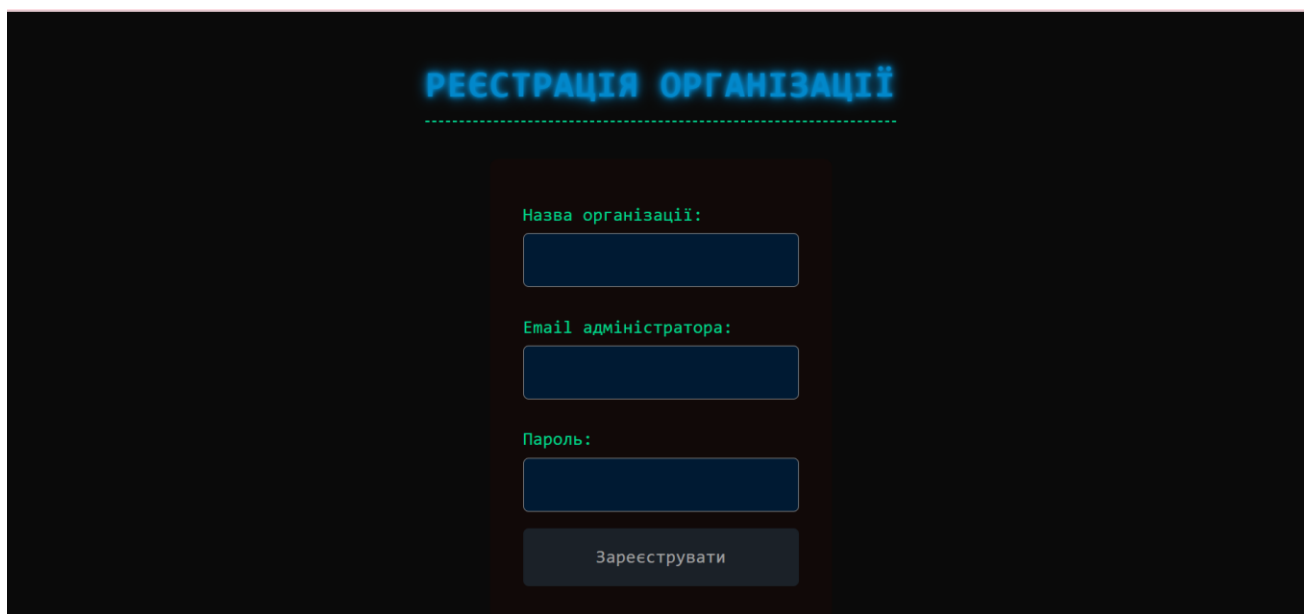
Застосунок має простий інтерфейс, з чітким розташуванням основних елементів: меню навігації, таблиці подій, що дозволяє користувачеві легко та швидко зрозуміти функціонал.

Адаптивний дизайн забезпечує коректну відображення на різних пристроях та орієнтаціях екрану. Підсвічування активних елементів та спливаючі повідомлення допомагають користувачеві орієнтуватись у процесі роботи із системою.

Комбінація простоти та адаптивності робить інтерфейс зручним, зменшує час на навчання аналітиків та дозволяє ефективно працювати із системою з перших днів використання.

Огляд сторінок веб-застосунку:

*Сторінка реєстрації:*



РЕЄСТРАЦІЯ ОРГАНІЗАЦІЇ

Назва організації:

Email адміністратора:

Пароль:

Зареєструвати

Сторінка містить форму реєстрації нової організації. Адміністратор вводить назву організації, свою електронну адресу та пароль. Дані надсилаються на сервер методом 'POST'.

На сервері форма обробляється маршрутом '/register\_organization', перевіряється коректність введеної інформації, якщо все вірно – створюється новий

запис у базі даних, надсилається відповідь про успішну реєстрацію і користувача перенаправляє на сторінку входу.

*Сторінка входу:*

Адміністратор вводить свої дані у поля форми, після натискання кнопки ‘Увійти’ вони надсилаються методом ‘POST’ на сервер, де перевіряється коректність інформації. у разі успішного входу адміністратор отримує доступ до системи.

*Головна сторінка звичайного користувача:*

ПРИСТРІЙ	ТИП ПОДІЇ	РІВЕНЬ	ДЕТАЛІ	ЧАС	ДІЇ
Religious-64	Security Alert	critical	Деталі	18.05.2025, 12:53:11	Заблокувати IP

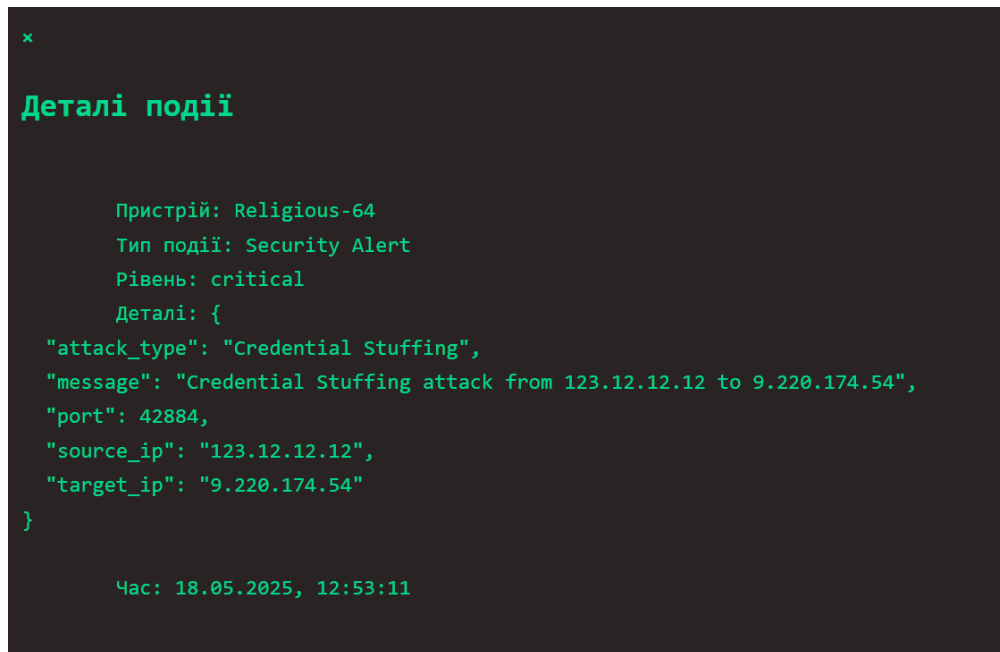
**Всі події**

ПРИСТРІЙ	ТИП ПОДІЇ	РІВЕНЬ	ДЕТАЛІ	ЧАС	ДІЇ
Couple-13	Network Traffic	info	Деталі	18.05.2025, 12:53:31	Заблокувати IP
printer	Authentication	info	Деталі	18.05.2025, 12:53:31	Заблокувати IP
Couple-13	Network Traffic	info	Деталі	18.05.2025, 12:53:21	Заблокувати IP
printer	Network Traffic	info	Деталі	18.05.2025, 12:53:21	Заблокувати IP

На цій сторінці відображається основна інформація – таблиці подій, кнопки керування пристроями та користувачами. В залежності від ролі користувача, можуть з'являтися функціональні кнопки для додавання нових користувачів, перегляд та додавання пристроїв, блокування IP-адрес та генерування звіту.

- Pinned logs – закріплені події. Виводяться критичні події поточного дня.
- Всі події – повна таблиця журналу подій.

При натисканні кнопки ‘Деталі’ відкривається вікно з повним описом про обрану подію.



Сторінка для перегляду та додавання нових пристроїв:

СПИСОК ПРИСТРОЇВ						
+ Додати новий девайс						
НАЗВА	ІР-АДРЕСА	MAC-АДРЕСА	ТИП	АКТИВНИЙ	ОСТАННЯ АКТИВНІСТЬ	ДІЇ
Despite-8	107.232.121.13	c2:fb:5c:27:bf:04	printer	Hi	2025-05-16 17:39:30	Видалити
Also-11	49.145.253.158	08:a8:4f:02:ec:01	camera	Hi	2025-05-16 17:22:05	Видалити
Space-43	175.161.112.150	0c:65:e6:fb:0b:35	router	Hi	2025-05-16 17:34:29	Видалити
Value-54	59.38.40.234	28:05:16:b5:18:19	camera	Hi	2025-05-16 17:29:57	Видалити
Ever-2	65.54.8.87	5c:44:15:ae:d0:95	workstation	Hi	2025-05-16 18:00:46	Видалити
Away-39	179.82.91.252	d2:20:d5:d8:70:72	camera	Hi	2025-05-16 17:25:16	Видалити
Resource-87	83.63.133.33	6a:b7:90:ae:77:c4	server	Hi	2025-05-16 17:24:15	Видалити
Tough-95	115.72.217.187	62:d9:54:3b:e3:85	server	Hi	2025-05-16 18:14:13	Видалити
pc 1	192.168.1.10	None	None	Hi	2025-05-16 17:20:04	Видалити
Someone-100	24.195.219.239	92:31:9a:ae:e2:b4	server	Hi	2025-05-16 18:07:57	Видалити
Participant-19	15.243.46.124	1c:e4:9f:58:7b:b6	printer	Hi	2025-05-16 17:48:43	Видалити
Set-35	69.2.203.25	b4:64:aa:6f:59:79	workstation	Hi	2025-05-16 17:55:24	Видалити

На цій сторінці відображаються всі пристрої, зареєстровані у цій організації. Поля ‘Остання активність’ та ‘Активний’ дозволяють проаналізувати стан пристроїв та у разі підозрілої активності чи кібератаки провести швидке розслідування, не витрачаючи час на пошук атакованого чи зараженого пристрою у всій системі.

Після натискання кнопки ‘Додати новий девайс’ користувач перенаправляється на відповідну сторінку.

### Сторінка додавання девайсів:

**ДОДАТИ НОВИЙ ПРИСТРІЙ**

Назва пристрою:

IP адреса:

MAC-адреса:

Тип пристрою:

-- Виберіть тип --

Додати пристрій

Адміністратор вводить усі необхідні дані у форму, яка надсилається на сервер, де обробляється – перевіряється унікальність MAC- та IP-адрес та назв пристрою. Якщо виникають помилки, система виводить повідомлення, що допомагає виправити недоліки без окремої перевірки бази даних.

### Сторінка списку користувачів:

EMAIL	РОЛЬ	ДАТА СТВОРЕННЯ	ДІЇ
me1@gmail.com	admin	2025-05-16 16:42:09	(ви)
tyler16@example.org	auditor	2025-05-16 17:06:49	Видалити
gwebster@example.net	user	2025-05-16 17:06:49	Видалити
twerner@example.org	user	2025-05-16 17:06:49	Видалити
kenneth57@example.org	user	2025-05-16 17:06:49	Видалити
knelson@example.org	user	2025-05-16 17:06:49	Видалити
fgarrison@example.net	user	2025-05-16 17:06:49	Видалити
patricia61@example.net	auditor	2025-05-16 17:06:49	Видалити
lynchlisa@example.org	user	2025-05-16 17:06:49	Видалити
rheath@example.org	user	2025-05-16 17:06:49	Видалити
chebert@example.org	auditor	2025-05-16 17:06:49	Видалити
anastasia@ex.com	user	2025-05-16 17:33:39	Видалити

Тут адміністратор бачить усіх користувачів організації, їхні ролі, дату та час додавання користувача в саму систему та кнопка видалити.



## Сторінка заблокованих IP-адрес:

SIEM DASHBOARD

Організація: my1

Головна

Пристрої

+ Додати користувача

Користувачі

Вийти

Заблоковані IP-адреси

IP-АДРЕСА	ДІЯ
111.131.142.55	<div>Розблокувати</div>
65.54.8.87	<div>Розблокувати</div>
175.161.112.150	<div>Розблокувати</div>
62.190.37.171	<div>Розблокувати</div>
9.220.174.54	<div>Розблокувати</div>

Якщо адміністратор виявляє шкідливу активність він може заблокувати IP – адресу з якої надходять підозрілі події. Це ізолює атакований або заражений пристрій, запобігаючи подальшому розповсюдженню загроз у мережі, а формування та аналіз звітів допомагає провести швидке розслідування.

## Приклад згенерованого звіту, надісланого через Telegram бот:

```

report (18): Блокнот
Файл Редагування Формат Вигляд Довідка
{
  "reason": "DDoS attack"
}

Тип події: DDoS
Кількість: 2
-----
2025-05-18 15:29:27
Подія: DDoS
Рівень: CRITICAL
Пристрій: Ever-2
Деталі: {
  "message": "DDoS attack on Ever-2 (65.54.8.87) with 72 threads",
  "attack_type": "DDoS",
  "target_ip": "65.54.8.87",
  "attacker_ips": [
    "169.130.87.114",
    "159.86.65.118",
    "114.28.176.254",
    "51.76.181.233",
    "22.109.241.188",
    "110.179.77.70",
    "58.77.214.128",
    "114.1.47.72",
    "172.147.246.144",
    "117.250.71.183",
    "162.11.3.18",
    "100.222.218.72",
    "141.206.83.248",
    "163.176.44.198",
    "136.217.166.65",
    "159.177.17.92",
    "149.254.66.233",
    "182.66.71.57",
    "17.100.25.104"
  ]
}

```

Уся інформація у звіті відсортована за типом події, що дозволяє сконцентруватись суто на тих подіях, які несуть загрозу роботі ІТ інфраструктури організації.

### 3.2 Тестування роботи

Для тестування роботи системи було написано скрипт `simulator.py`, який генерує події у середовищі, наближеному до реального. Скрипт виконує автоматизоване моделювання поведінки користувачів, пристроїв, атак та взаємодій у системі організації.

#### Структура симулятора

Симулятор реалізовано як клас `DeviceSimulator`, який взаємодіє з базою даних PostgreSQL через ORM SQLAlchemy. У класі реалізовано:

- 1) Підключення до бази даних
- 2) Створення тестових пристроїв та користувачів
- 3) Генерація нормальної та аномальної активності

#### Нормальна активність:

##### -TCP/UDP трафік

TCP (Transmission Control Protocol) – протокол транспортного рівня призначений для керування передаванням даних у комп'ютерних мережах. Забезпечує надійне передавання даних від відправника до отримувача.

UDP (User Datagram Protocol) – один з основних мережевих протоколів в стеку TCP/IP. Працює без встановлення з'єднання, на відміну від TCP. Працює на транспортному рівні.

##### - Аутентифікації

##### - Системні події

- 4) Імітація атак між пристроями, атак на користувачів, компрометацій

#### Tuni атак [12]:

- SSH Brute Force (SSH – Secure Shell) – атака при якій зловмисник методом перебору підбирає логін і пароль до SSH, використовуючи скрипти або боти для

перебору комбінацій. SIEM-система розпізнає аналізуючи логи автентифікації з WSL (Windows Security Log)

- SQL Injection – вразливість веб-додатків, коли зловмисник вставляє шкідливий SQL-запит у поле введення, що дозволяє отримати доступ і маніпулювати базою даних. Розпізнаються після аналізу HTTP-запитів з логів веб-сервера.

- Port Scanning (Сканування портів) – техніка пошуку відкритих портів у мережі з метою проникнення в систему та пошуку інших вразливостей. Система виявлення вторгнень (IDS, Intrusion Detection System) аналізує мережевий трафік і шукає підозрілі, а система отримує логи для подальшого аналізу.

- Malware Download – завантаження шкідливого програмного забезпечення без відома і згоди користувача. Антивірус фіксує завантаження/виконання шкідливого файлу, а SIEM система їх отримує.[11]

- Credential Stuffing (Підстановка облікових даних) – автоматичне введення викрадених пар логін і пароль з метою отримання входу у систему та викрадення даних.

- Phishing (Фішинг) – соціотехнічна атака, при якій зловмисник обманом змушує користувача надіслати конфіденційну інформацію (логіни, паролі), часто через електронні листи та фальшиві веб-сайти.

- DDoS (Distributed Denial of Service – розподілена атака на відмову в обслуговуванні) – атака на веб-сайти та сервери з метою порушення роботи мережевих служб. Під час атаки боти надсилають величезний обсяг запитів тим самим перевантажують веб-сайт чи службу. Система розпізнає цей тип атак аналізуючи трафік, різкій кількості з'єднань на сервері, повторювані запити на один ресурс із різних адрес.

- Compromise – стан, при якому система або обліковий запис були успішно зламані або скомпрометовані внаслідок атаки. Система розпізнає цю атаку аналізуючи входи користувача в систему з незвичних IP-адрес чи геолокацій, логіни у незвичний час, виконання команд не характерних для користувача або системи, велика кількість невдалих спроб входу за яким йде успішний вхід.

### Процес симуляції:

- створюється атака
- формується лог-повідомлення
- відправляється через UDP на Syslog Server
- сервер читає та записує дані у базу даних
- SIEM-система читає логи.

## ВИСНОВКИ

У процесі виконання цієї роботи було розглянуто принцип роботи систем виявлення та логування подій безпеки. Проведений аналіз сучасних підходів до управління інформаційною безпекою показав важливість комплексного моніторингу подій безпеки та вчасного виявлення інцидентів.

У ході практичної частини було реалізовано прототип симулятора, який генерує різні види активностей мережевих пристроїв. За допомогою протоколу Syslog трафік надсилався на сервер де логи оброблялись і зберігались у базу даних. Симульовані атаки дозволили створити наближене до реальності середовище для дослідження поведінки систем безпеки.

Створений веб-застосунок дозволяє візуалізувати події безпеки у реальному часі, відстежувати активність пристроїв, користувачів та формувати звіт за заданий період. Інтерфейс системи надає можливість швидко аналізувати ситуацію в організації завдяки поділу подій за типами та рівнями небезпеки.

Завдяки модульній архітектурі легко додавати новий функціонал. Такий підхід забезпечує масштабованість та адаптацію під потреби різних організацій. Особливо це важливо в умовах зростання кількості кібератак на ІТ інфраструктуру українських організацій.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. “The Intelligence Handbook Fourth Edition. A Roadmap for Building an Intelligence-Led Security Program”
2. Splunk  
[https://www.splunk.com/en\\_us/solutions/splunk-vs-ibm-qradar.html](https://www.splunk.com/en_us/solutions/splunk-vs-ibm-qradar.html)
3. IBM Qradar  
<https://www.ibm.com/products/qradar-siem>
4. LogRhythm  
<https://www.exabeam.com/platform/logrhythm-siem/>
5. AlienVault  
<https://www.billows.com.tw/en/download/dm/AlienVault-SIEM.pdf>
6. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ МОВИ ПУТОН ДЛЯ СТВОРЕННЯ ДОДАТКІВ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ  
<https://journals.dut.edu.ua/index.php/dataprotect/article/view/2788/2687>
7. PostgreSQL  
<https://www.postgresql.org/support/security/>
8. “Modern Types of Databases for SIEM System Development” Sergiy Gnatyuk, Rat Berdibayev, Ivan Azarov, Nazerke Baisholan, and Iryna Lozova  
<https://ceur-ws.org/Vol-3187/paper12.pdf>
9. ACID  
[https://www.vpnunlimited.com/ua/help/cybersecurity/acid?srsId=AfmBOopaCjUO6vH0imW2-tfokXGnm\\_90-1FZRx9\\_OedeMk63HApgVBEE](https://www.vpnunlimited.com/ua/help/cybersecurity/acid?srsId=AfmBOopaCjUO6vH0imW2-tfokXGnm_90-1FZRx9_OedeMk63HApgVBEE)
10. “The Practice of Network Security Monitoring Understanding Incident Detection and Response” by Richard Bejtlich
11. Drive-by download attacks  
[https://www.reddit.com/r/AskNetsec/comments/11ahqz4/drive\\_by\\_download\\_attacks/](https://www.reddit.com/r/AskNetsec/comments/11ahqz4/drive_by_download_attacks/)
12. What is a cyberattack?  
<https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cyberattack.html>

13. “A Security Architecture for Computational Grids” Ian Foster, Carl Kesselman, Gene Tsudik, Steven Tuecke

<https://scispace.com/pdf/a-security-architecture-for-computational-grids-3uzm9yyae5.pdf>