МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет комп’ютерних наук та технологій
Кафедра «Комп’ютерні системи та мережі»

ЖИВОГЛЯД ВІТАЛІЙ АНДРІЙОВИЧ
Група КНТ-514м

ІНТЕГРОВАНА СИСТЕМА МОНІТОРИНГУ МЕРЕЖ З ПІДТРИМКОЮ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ

АВТОРЕФЕРАТ

дипломної роботи на здобуття освітньо-кваліфікаційного рівня
«магістр» 123 Комп’ютерна інженерія
освітньої програми Комп’ютерні системи та мережі

2025 р.

Дипломна робота є рукопис.

Робота виконана в національному університеті «Запорізька політехніка», на кафедрі комп’ютерних систем та мереж

Керівник	кандидат технічних наук, доцент **Киричек Галина Григорівна** Національний університет «Запорізька політехніка», доцент кафедри комп'ютерних систем та мереж
Офіційний рецензент:	**Щербаков Володимир Іванович,** Директор НВФ «Бізнес Комп’ютер Сервіс»

Захист відбудеться "26" грудня 2025 р.

Секретар екзаменаційної комісії, доцент кафедри комп’ютерних систем та мереж Т.В. Голуб

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У сучасному цифровому середовищі, де корпоративні та відомчі мережі стають дедалі складнішими та вразливішими до кіберзагроз, моніторинг мереж виступає ключовим елементом забезпечення стабільності та безпеки інформаційних систем. Традиційні методи моніторингу, такі як протоколи SNMP, NetFlow та Syslog, хоча й дозволяють збирати дані про трафік та стан пристроїв, часто стикаються з критичними проблемами при обробці великих обсягів даних у реальному часі. Основними недоліками існуючих підходів є недостатня інтеграція з сучасними системами сповіщень та обмежена адаптивність до динамічних інфраструктур, зокрема хмарних та IoT-середовищ.

Проблеми сучасної мережевої безпеки посилюються стрімким зростанням обсягів трафіку та поширенням складних розподілених атак, таких як DDoS та brute-force. Це вимагає від систем моніторингу не лише виявлення аномалій, а й наявності механізмів автоматизованої передачі повідомлень для забезпечення миттєвого втручання адміністраторів. Аналіз існуючих систем, зокрема Zabbix та Nagios, свідчить про те, що їм бракує гнучкої маршрутизації сповіщень через сучасні комунікаційні канали, такі як Telegram, а також глибокої інтеграції з джерелами загрозової розвідки. Такі обмеження призводять до затримок у реагуванні на інциденти та збільшення кількості помилкових алертів.

Актуальність дослідження зумовлена необхідністю створення інтегрованих рішень, які об'єднують класичний моніторинг продуктивності з інноваційними механізмами безпеки та оперативної комунікації. В умовах, коли щосекунди обробляються тисячі мережевих подій, традиційні системи не завжди справляються з навантаженням, що може призвести до пропуску критичних інцидентів. Це особливо важливо для організацій малого бізнесу, де оперативне інформування про загрози (наприклад, SQL-ін'єкції чи DDoS-атаки) може запобігти значним фінансовим та репутаційним збиткам.

Мета і завдання дослідження. Метою роботи є підвищення ефективності та оперативності реагування на інциденти інформаційної безпеки шляхом створення інтегрованої системи моніторингу мереж. Розроблене рішення має поєднувати в собі

глибокий аналіз мережевого трафіку, агрегацію даних із зовнішніх гетерогенних джерел (зокрема систем Zabbix та Nagios) та механізми гнучкої інтелектуальної маршрутизації сповіщень.

Для досягнення поставленої мети передбачається створення інтегрованого програмного продукту, який забезпечує:

- проведення комплексного аналізу та дослідження мережевого середовища на наявність ознак кіберзагроз;
- поєднання функцій моніторингу продуктивності інфраструктури з активними механізмами забезпечення безпеки;
- автоматизацію процесу інформування відповідальних осіб через сучасні канали комунікації для мінімізації часу на усунення інцидентів.

Кінцевим результатом дослідження є реалізація та впровадження програмного комплексу «CyberGuard Pro», що дозволяє не лише виявляти аномалії в реальному часі, а й проактивно реагувати на критичні події в мережах підприємств

Об’єктом дослідження є процес реалізації інтегрованої системи моніторингу мереж з підтримкою передачі повідомлень.

Це охоплює сукупність процедур та технологічних рішень, спрямованих на:

- систематичний збір і нормалізацію даних про стан мережевої інфраструктури;
- інтеграцію різнорідних джерел інформації в єдине аналітичне середовище;
- функціонування механізмів оперативного сповіщення та автоматизованого реагування на виявлені інциденти

Предметом дослідження є моделі, методи, програмні засоби, алгоритми та архітектурні рішення системи моніторингу мереж у реальному часі.

Методи дослідження. Дослідження базується на системному аналізі мережевих протоколів та існуючих систем моніторингу, що дозволило виявити обмеження у швидкості інформування про загрози. Проєктування системи здійснювалося із застосуванням принципів об’єктно-орієнтованого програмування та методів асинхронної обробки даних (Python, Celery, Redis), що забезпечило високу стабільність роботи при інтенсивному трафіку.

Наукова новизна отриманих результатів. Наукова новизна отриманих результатів полягає у теоретичному обґрунтуванні та

реалізації підходів до побудови високонавантажених систем моніторингу, а саме:

Удосконалено архітектурну модель інтегрованої системи моніторингу мереж шляхом впровадження асинхронного ядра обробки подій (на базі стеку Celery/Redis). Це дозволило забезпечити паралельний збір даних із гетерогенних джерел (Zabbix, Nagios, прямий аналіз трафіку) без втрати продуктивності при інтенсивних навантаженнях (до 10 000 подій/с).

Дістала подальший розвиток методика гібридного аналізу мережевих загроз, яка, на відміну від існуючих рішень, поєднує сигнатурний аналіз із поведінковими алгоритмами детекції в реальному часі. Це підвищило точність виявлення складних атак, таких як низькоінтенсивний Brute-force та розподілені DDoS-атаки.

Запропоновано алгоритм інтелектуальної дедуплікації та динамічної маршрутизації сповіщень через сучасні канали комунікації (Telegram API). Алгоритм забезпечує агрегацію однотипних інцидентів у часовому вікні, що дозволяє критично знизити інформаційне навантаження на адміністратора, не втрачаючи при цьому важливі дані про аномалії.

Практичне значення отриманих результатів. Розроблено повнофункціональну вебсистему, яка дозволяє суттєво скоротити час на налагодження проєктів та написання тестбенчів. Система забезпечує візуалізацію помилок та надання навчальних порад, що дозволяє використовувати її як ефективний допоміжний інструмент у підготовці фахівців з комп’ютерної інженерії.

Апробація результатів дипломної роботи. Основні положення дипломної роботи та результати досліджень подано до участі на конференції:

- Modern Trends In Information Technology Development у секції «Artificial Intelligence» (19 листопада, Дніпро).

Структура та обсяг роботи. Робота складається зі вступу, п'яти розділів, висновків, переліку джерел та додатків. Пояснювальна записка містить 95 сторінок тексту, 27 рисунків, 5 лістингів та 3 таблиці.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У першому розділі проведено ґрунтовний аналіз сучасного стану розвитку систем моніторингу комп’ютерних мереж та інформаційних систем, а також визначено їх роль у забезпеченні стабільності та безпеки IT-інфраструктур. Моніторинг мереж є критично важливим процесом, що дозволяє своєчасно виявляти збої, перевантаження, аномальну поведінку та потенційні загрози безпеці.

Розглянуто основні поняття та завдання мережевого моніторингу, зокрема контроль доступності ресурсів, аналіз продуктивності, відстеження мережевого трафіку та реєстрацію подій безпеки. Проаналізовано відмінності між активним і пасивним моніторингом, а також їх вплив на точність і повноту отримуваних даних.

Особливу увагу приділено аналізу існуючих програмних рішень моніторингу, таких як Zabbix, Prometheus, Nagios, SolarWinds, які широко використовуються в корпоративних та хмарних середовищах. Порівняльний аналіз показав, що комерційні рішення зазвичай мають розвинені інтерфейси та готові шаблони, але є менш гнучкими та обмеженими ліцензійними умовами. Водночас відкриті системи характеризуються високою адаптивністю, проте потребують значних зусиль для налаштування та інтеграції.

У розділі також проаналізовано сучасні загрози інформаційній безпеці, які можуть бути виявлені за допомогою систем моніторингу, зокрема атаки типу DoS/DDoS, несанкціонований доступ, аномальні пікові навантаження та збої сервісів. Зроблено висновок, що ефективна система моніторингу повинна поєднувати функції збору технічних метрик і механізми оперативного сповіщення відповідальних осіб.

На основі проведеного аналізу сформульовано основні вимоги до розроблюваної системи, зокрема масштабованість, модульність, підтримку інтеграції з зовнішніми сервісами та наявність гнучких каналів доставки повідомлень.

Сформульовано мету та завдання роботи, а також обґрунтовано актуальність розробки інтегрованої системи моніторингу з підтримкою ефективної передачі повідомлень.

Другий розділ присвячено проєктуванню архітектури інтегрованої системи моніторингу мереж із підтримкою передачі

повідомлень у реальному часі. Запропонована система орієнтована на використання в умовах розподіленої IT-інфраструктури та передбачає модульний підхід до побудови.

Розроблено загальну архітектурну модель системи, яка включає такі основні компоненти:

- модуль збору даних;
- модуль нормалізації та обробки подій;
- підсистему зберігання даних;
- модуль маршрутизації та доставки сповіщень;
- інтерфейс взаємодії з користувачем.

Загальна структурна схема системи наведена на рисунку 1, де відображено основні інформаційні потоки між компонентами.

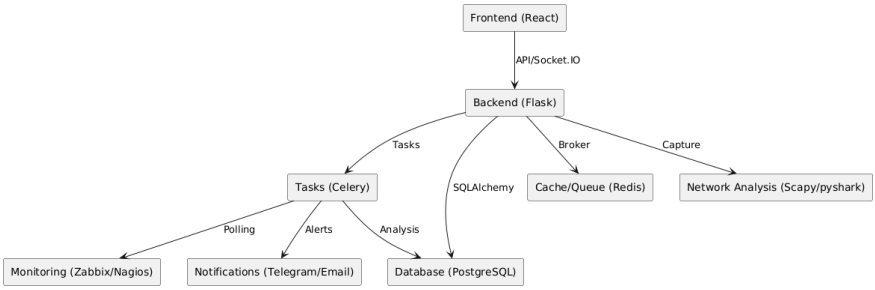

Рисунок 1 – Архітектура технологічного стеку системи

Модуль збору даних відповідає за інтеграцію з зовнішніми системами моніторингу, такими як Zabbix та Nagios, і забезпечує отримання інформації про стан хостів, сервісів та тригерів. Для зменшення навантаження на систему застосовано принципи асинхронної обробки та черг повідомлень.

У розділі також описано логіку формування подій безпеки та їх класифікацію за рівнями важливості. Це дозволяє реалізувати адаптивну модель сповіщень, коли критичні події обробляються негайно, а менш важливі можуть агрегуватися або відкладатися.

Окрему увагу приділено питанням масштабованості та надійності системи. Передбачено можливість горизонтального масштабування окремих компонентів, що дозволяє використовувати систему в мережах з великою кількістю вузлів.

У третьому розділі розглянуто практичну реалізацію розробленої архітектури. Система реалізована з використанням сучасних відкритих технологій, що забезпечують гнучкість та простоту розгортання. Програмний комплекс побудовано на базі мови Python з використанням мікрофреймворку Flask, що забезпечує високу швидкість обробки запитів та легкість масштабування.

Описано реалізацію модуля збору та нормалізації даних із використанням API Zabbix та файлів статусу Nagios. Розроблений алгоритм дозволяє перетворювати різнорідні метрики у єдиний формат внутрішніх подій системи, що є критично важливим для їх подальшої кореляції. Процес ініціалізації системи та послідовність обробки подій у ядрі представлено на рисунку 2.

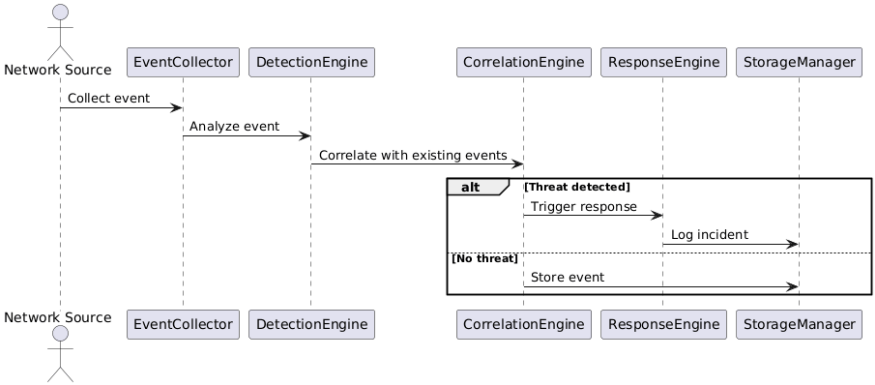

Рисунок 2 – Схема послідовності обробки подій у ядрі системи

Для забезпечення високої відмовостійкості при пікових навантаженнях реалізовано асинхронну модель обробки подій за допомогою черг повідомлень Celery та брокера Redis. Це дозволяє розділити процеси моніторингу та безпосередньої доставки сповіщень, запобігаючи блокуванню основного потоку програми. Логіку маршрутизації та обробки інцидентів залежно від їх пріоритету (Critical, High, Medium) наведено на рисунку 3.

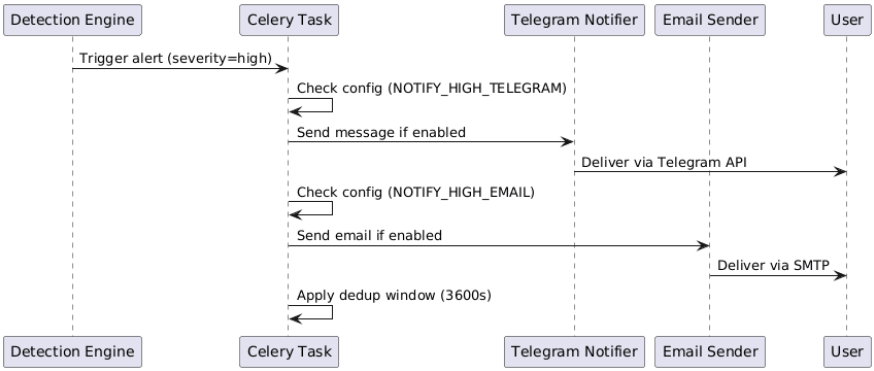

Рисунок 3 – Схема інтеграції каналів доставки сповіщень.

У розділі детально описано механізми інтеграції з каналами доставки повідомлень, зокрема Telegram та електронною поштою. Реалізовано централізований модуль конфігурації, який дозволяє змінювати параметри каналів без редагування програмного коду.

Розглянуто питання надійності системи, зокрема механізми дедуплікації подій та обробки помилок при надсиланні повідомлень. Запропонований підхід гарантує своєчасне інформування відповідальних осіб про критичні інциденти безпеки навіть у разі часткових збоїв мережевої інфраструктури.

У четвертому розділі наведено результати тестування та експериментальної оцінки ефективності розробленої системи моніторингу CyberGuard Pro. Проведено серію функціональних, інтеграційних та системних тестів відповідно до розробленого плану.

Послідовність етапів перевірки, що охоплює модульне, інтеграційне та апаратне тестування, відображено на діаграмі плану тестування на рисунку 4.

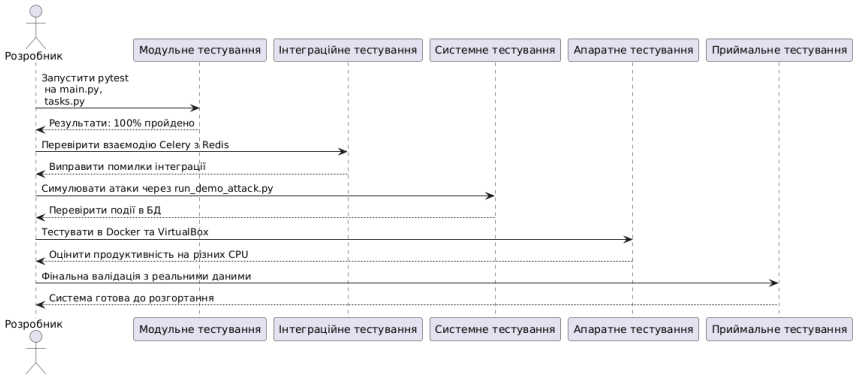

Рисунок 4 – Діаграма плану тестування системи

Функціональне тестування підтвердило коректність роботи основних модулів системи. Результати перевірки підсистеми візуалізації та моніторингу в реальному часі представлено на головній панелі Dashboard на рисунку 5, , яка демонструє загальну статистику інцидентів та часову лінію подій на русунку 6.

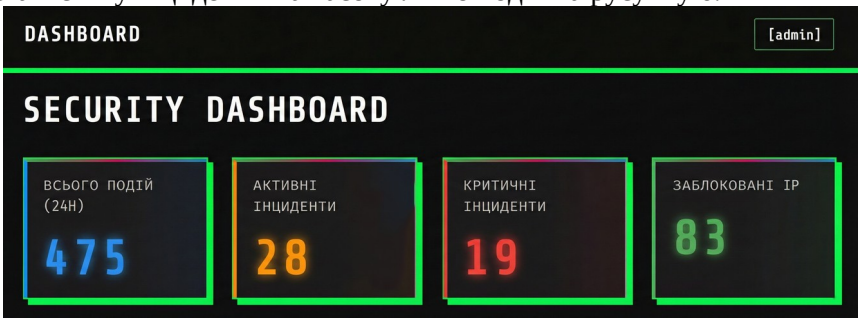

Рисунок 5 – Dashboard

Рисунок 6 – Dashboard – часова лінія подій

Ефективність відстеження топології мережі та аналізу вузлів підтверджується візуалізацією інтерактивної мережевої карти зображено на рисунку 7.

Окрему увагу приділено перевірці підсистеми сповіщень. Коректність формування подій та оперативність доставки повідомлень продемонстровано на прикладі синхронізації журналу атак (Attack LOG) із push-повідомленнями у Telegram під час симуляції загрози на рисунку 8. Встановлено, що використання асинхронної обробки дозволяє здійснювати сповіщення із затримкою менше 5 секунд.

За результатами аналізу безпеки розроблено комплексну схему заходів захисту інформації в системі, яка охоплює рівні моніторингу, автентифікації та шифрування даних.

На основі отриманих результатів зроблено висновок про доцільність використання запропонованої архітектури для побудови інтегрованих систем моніторингу мереж з підтримкою оперативного реагування на інциденти безпеки.

Рисунок 7 – Мережева карта – візуалізація карти

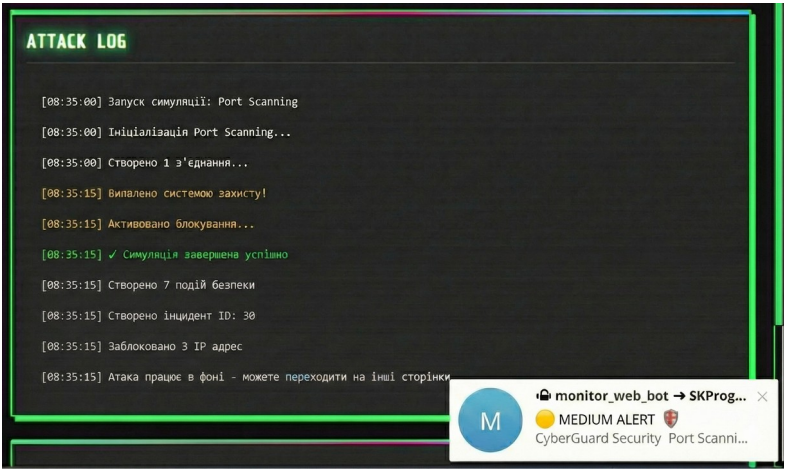

Рисунок 8 – Демо – Attack LOG з прикладом миттєвого сповіщення в Telegram

ВИСНОВКИ

Результати, отримані в магістерській роботі, є комплексним рішенням практичної задачі підвищення ефективності моніторингу та оперативності реагування на інциденти інформаційної безпеки.

Отримані теоретичні та практичні результати дозволяють зробити наступні висновки:

1. Проведено ґрунтовний аналіз існуючих методів та інструментальних засобів моніторингу мереж (Zabbix, Nagios, SolarWinds). Виявлено, що основним недоліком наявних систем є низький рівень інтеграції з сучасними каналами оперативних сповіщень та складність кореляції даних з гетерогенних джерел у реальному часі.

2. Обґрунтовано та спроектовано архітектуру інтегрованої системи моніторингу, яка базується на модульному принципі та асинхронній обробці подій. На відміну від традиційних рішень, запропонований підхід дозволяє розділити процеси збору метрик та логіку реагування, що мінімізує ризик втрати критичних даних при пікових навантаженнях.

3. Розроблено та реалізовано програмний комплекс «CyberGuard Pro», що використовує сучасний технологічний стек (Python, Flask, Celery, Redis). Впроваджено уніфікований модуль нормалізації, який дозволяє інтегрувати дані з різних систем моніторингу в єдиний потік інцидентів.

4. Реалізовано інтелектуальну систему маршрутизації сповіщень, яка забезпечує миттєву доставку критичних алертів через Telegram-ботів та електронну пошту. Впроваджені алгоритми дедуплікації та фільтрації повідомлень дозволили суттєво зменшити інформаційне навантаження на оператора.

5. Експериментально підтверджено ефективність системи. Встановлено, що час реакції на критичний інцидент (від моменту виявлення до отримання push-сповіщення) складає менше 5 секунд. Система продемонструвала стабільну роботу при обробці потоків даних обсягом до 10 000 подій на секунду.

6. Запропоновано та впроваджено заходи із захисту інформації всередині системи, включаючи багаторівневу автентифікацію та

шифрування каналів зв’язку, що гарантує цілісність та конфіденційність моніторингових даних.

Результати роботи підтверджують, що створена система може бути успішно впроваджена на підприємствах для автоматизації процесів кібербезпеки та оптимізації роботи IT-департаментів.