

УНІВЕРСИТЕТ ІМЕНІ АЛЬФРЕДА НОБЕЛЯ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА
БАКАЛАВРА

на тему

**“Розробка та тестування системи виявлення
аномалій у мережевому трафіку”**

Виконав: здобувач 4 курсу, групи КН-21

Спеціальності 122 Комп'ютерні науки

Ліщинський Олександр Володимирович

Керівник: Косарєв Вячеслав Михайлович

к.т.н., доцент

м. Дніпро

2025

АНОТАЦІЯ

Ліщинський О.В. Система виявлення аномалій у мережевому трафіку на основі машинного навчання.

Метою кваліфікаційної роботи є розробка та реалізація програмної системи, що дозволяє виявляти аномальну мережеву активність з використанням алгоритмів машинного навчання. Об'єктом дослідження є мережевий трафік у комп'ютерних системах. У ході виконання дипломної роботи було реалізовано програмний комплекс, що складається з модуля збору трафіку, обробки, агрегації ознак та модуля аналізу з використанням моделі Isolation Forest. Результати тестування підтвердили здатність системи ефективно виявляти підозрілу активність, зокрема сканування портів, масові HTTP-запити, тунелювання DNS та нетипову нічну активність.

Ключові слова: виявлення аномалій, мережевий трафік, машинне навчання, Isolation Forest, кібербезпека.

SUMMARY

Lishchynskyi Oleksandr Anomaly detection system in network traffic based on machine learning.

The purpose of the degree work is to design and develop a software system for detecting anomalous network activity using machine learning algorithms. The object of the research is network traffic in computer systems. The developed software includes modules for traffic capture, preprocessing, feature aggregation, and analysis using the Isolation Forest model. Testing confirmed the system's ability to successfully detect suspicious activity such as port scanning, mass HTTP requests, DNS tunneling, and unusual night-time behavior.

Keywords: anomaly detection, network traffic, machine learning, Isolation Forest, cybersecurity.

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1 АНАЛІЗ ПРОБЛЕМИ ТА ВИБІР МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ	9
1.1 Аналіз мережевих загроз.....	9
1.2 Підходи до виявлення активних загроз у комп'ютерних мережах.....	14
1.3 Класифікація аномалій у мережевому трафіку.....	22
1.3.1 Об'ємні аномалії (Volume-based anomalies)	22
1.3.3 Поведінкові аномалії (Behavioral anomalies)	25
1.3.4 Контекстно-залежні аномалії (Contextual anomalies).....	27
РОЗДІЛ 2 ПРОЕКТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ	30
2.1 Постановка задачі та вимоги до системи	30
2.2 Архітектура системи виявлення аномалій у мережевому трафіку	32
2.3 Вибір технологій та інструментів реалізації.....	34
РОЗДІЛ 3 РОЗРОБКА ТА ТЕСТУВАННЯ СИСТЕМИ АНАЛІЗУ АНОМАЛІЙ В МЕРЕЖЕВОМУ ТРАФІКУ	40
3.1. Розробка компонентів системи	40
3.1.1 Розробка модуля збору трафіку	40
3.1.2 Розробка модуля попередньої обробки трафіку.....	41
3.1.3 Формування ознак та виявлення аномалій методом Isolation Forest.....	43
3.2 Тестування системи виявлення аномалій у мережевому трафіку.....	45
3.2.1 Сценарії виявлення аномальної активності	46
3.3 Потенційні можливості вдосконалення системи.....	51
ВИСНОВКИ	53
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	55

Додаток А Лістинг програми - сніфера трафіку	57
Додаток Б Лістинг С-програми для Erlang-порту	60
Додаток В Лістинг Erlang-код для взаємодії з портом	62