УДК 004:621.391]:004.056

МЕТОДИ ВИЯВЛЕННЯ У СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Лійко Д.О., Іваненко С.А.
e-mail: danylo.liiko@nure.ua, e-mail: stanislav.ivanenko@nure.ua
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна

This work focuses on intrusion detection systems (IDS) used to identify malicious activities in computer systems and networks. The main types of IDS, namely, network-based (NIDS) and host-based (HIDS), are considered. The key detection methods, including signature-based and anomaly-based approaches, are analyzed. The advantages and limitations of each method are discussed, with particular attention to the adaptability of anomaly detection in identifying new and unknown threats. The role of IDS in modern cybersecurity infrastructure is highlighted, demonstrating its importance in threat detection and mitigation.

Система виявлення вторгнень (Intrusion Detection System, IDS) призначена для виявлення зловмисної активності в комп'ютерній системі [1]. Її роль може виконувати програмне забезпечення або пристрій, який відстежує діяльність у системі або мережі на наявність порушень правил чи зловмисних дій і створює звіти для системи керування. IDS є важливим доповненням до інфраструктури безпеки майже кожної організації.

Залежно від досліджуваної системи, IDS можна поділити на мережеві та хост-орієнтовані [1]. Мережева IDS (Network-based IDS, NIDS) – це незалежна платформа, яка здійснює моніторинг мережевих магістралей і шукає сценарії атак, аналізуючи, досліджуючи та контролюючи дані мережевого трафіку. Хост-орієнтовані IDS (Host-based IDS, HIDS) знаходяться на конкретному комп'ютері і намагаються виявити шкідливу активність, забезпечити захист конкретної комп'ютерної системи шляхом моніторингу операційної та файлової систем на наявність ознак вторгнення.

Існує два основних методи, які використовуються для аналізу подій та виявлення атак у IDS: метод виявлення на основі сигнатур та метод виявлення на основі аномалій.

Метод виявлення на основі сигнатур використовує базу даних відомих загроз та їх індикаторів компрометації. Таким індикатором може бути певна поведінка, яка зазвичай передує зловмисній мережевій атаці, хеш файли, шкідливі домени, відомі байтові послідовності або навіть вміст заголовків тем електронних листів. IDS відстежує дані комп’ютерної системи або мережі та порівнює їх з базою даних, щоб позначити будь-яку підозрілу поведінку. Використання IDS на основі сигнатур не є ефективним для виявлення нових атак, для яких не існує певного шаблону сигнатур, тому більш популярними є методи виявлення на основі аномалій [2].

Метод на основі виявлення аномалій використовує машинне навчання, щоб навчити систему виявлення розпізнавати нормальний стан мережі або

хоста що називається базовим рівнем. Будь-яке відхилення від базового рівня вважається аномалією. У літературі з інтелектуального аналізу даних та статистики аномалії також називають відхиленнями, девіантами або викидами. Як показано на рисунку 1, N_1 і N_2 – це регіони, що складаються з більшості спостережень і, отже, вважаються нормальними регіонами екземплярів даних, тоді як регіон O_3 і точки даних O_1 і O_2 – це кілька точок даних, які розташовані далі від основної маси точок даних і, отже, вважаються аномаліями. аномалії виникають з кількох причин, таких як зловмисні дії, системні збої, навмисне шахрайство. Ці аномалії розкривають цікаву інформацію про дані і часто передають цінну інформацію про дані. Тому виявлення аномалій вважається важливим кроком у різних системах прийняття рішень [2].

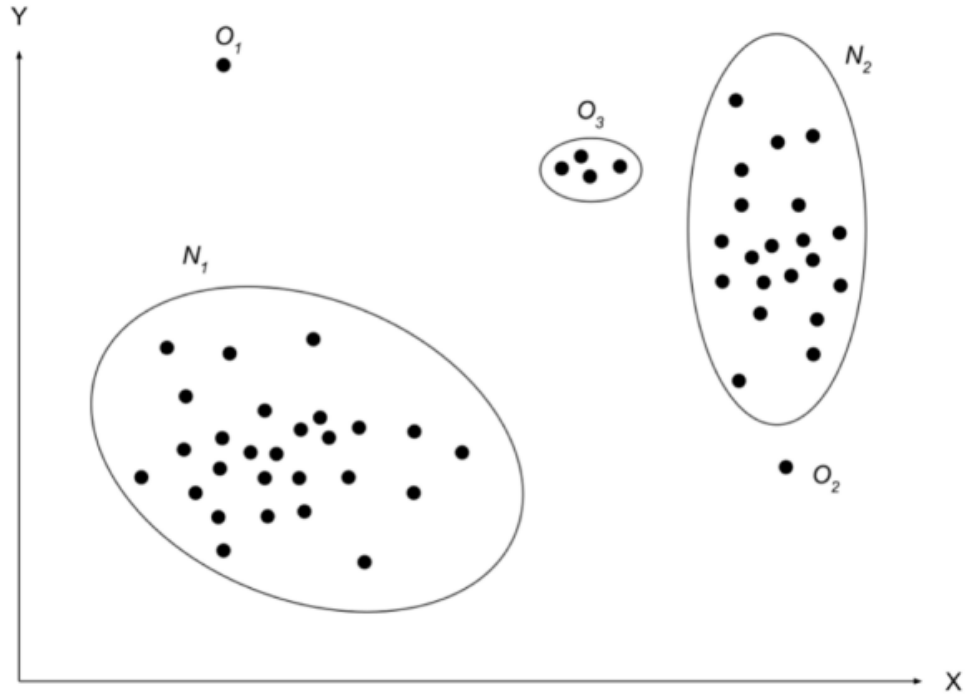

Рисунок 1 – Ілюстрація аномалій у двовимірному наборі даних

Недоліком цього методу є те, що багато нешкідливих дій можуть бути позначені як аномалії. Підвищена ймовірність помилкових спрацьовувань може вимагати додаткового часу та ресурсів для дослідження всіх сповіщень про потенційні загрози.

Список використаних джерел:

1. M K. Intrusion Detection System and Artificial Intelligent. *Intrusion Detection Systems*. 2011. С. 118–119. URL: https://doi.org/10.5772/15271 (дата звернення: 02.03.2025).

2. Chalapathy R., Chawla S. Deep Learning for Anomaly Detection: A Survey. *arXiv.org*. URL: https://arxiv.org/abs/1901.03407 (дата звернення: 02.03.2025).