Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ імені К. Д. УШИНСЬКОГО»

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ДРУГА ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

25 квітня 2025 р.

Одеса – 2025

Інформатика, інформаційні системи та технології: тези доповідей двадцять другої всеукраїнської конференції студентів і молодих науковців. Одеса, 25 квітня 2025 р. - Одеса, 2025. – 315 с.

Друкується за рішенням Вченої Ради
Університету Ушинського
(протокол № 16 від 29.05.2025 р.)

Організатори конференції продовжують традицію обміну досвідом у сфері освіти та використання інформаційних технологій. У конференції приймають участь студенти, аспіранти та молоді науковці вищих навчальних закладів України.

Тематика конференції охоплює наступне коло питань: сучасні інформаційні технології; інтелектуальні системи; методика викладання інформатики; інформаційні технології в освіті; психолого-педагогічне забезпечення інформатизації навчальної діяльності; дистанційна освіта і глобальні телекомунікаційні мережі; математичне моделювання й інформаційні технології; інформатизація системи керування освітою; інформаційні технології в менеджменті.

Наукові керівники:

завідувачка кафедри прикладної математики та інформатики
фізико-математичного факультету Університету Ушинського, д. т. н., проф. Т. Л. Мазурок,
завідувач кафедри математичного забезпечення комп'ютерних систем факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. т. н., проф. Є. В. Малахов

Оргкомітет:

Голова:

Ректор Університету Ушинського,
д. і. наук, доц. А. В. Красножон

Заступники голови:

Проректор з наукової роботи Університету Ушинського, д. політ. н., проф. Г.В. Музиченко
Декан факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. ф-м. н., проф. Ю. А. Ніцук

Члени оргкомітету:

д. т. н., проф.	Є. В. Малахов	д. т. н., проф.	Т. Л. Мазурок
д. т. н., проф.	Ю. О. Гунченко	к. п. н., доц.	А. О. Яновський
ст. викладач	І. М. Лісіцина	викладач	О. Я. Рубанська
ст. викладач	Н. Ф. Трубіна	к. ф.-м. н.	О. П. Бойко
ст. викладач	В. А. Корабльов	PhD, associated prof. (Poland)	A. Rychlik

Література

1. Теницька А.О. Система виявлення кібератак. Інформаційна технологія функціонування системи виявлення атак в режимі моніторингу / Сумський державний університет. Суми, 2021. С. 25-30.
2. Ковтун Р. О. Виявлення аномалій трафіку у комп'ютерних мережах. Харків : НТУ "ХПІ", 2017. С. 23-30.

АНАЛІЗ ПРОБЛЕМИ ВИСОКОГО РІВНЯ ХИБНОПОЗИТИВНИХ СПРАЦЮВАНЬ У СИСТЕМАХ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ

Свиридов І. І., Шпинарева І. М.

Національний університет «Одеська політехніка»

Анотація: У даній роботі аналізується проблема високого рівня хибнопозитивних спрацювань у системах виявлення аномалій у комп'ютерних мережах. Розглядаються основні причини виникнення помилкових спрацювань, зокрема недосконаліть моделей поведінки, якість вхідних даних та обмеження використовуваних алгоритмів. Проаналізовано підходи до зниження хибнопозитивних результатів, зокрема за допомогою гібридних методів, машинного навчання та адаптивного налаштування параметрів системи.

Ключові слова: хибнопозитивні спрацювання, виявлення аномалій, комп'ютерні мережі, мережевий трафік, машинне навчання, безпека, IDS, точність систем.

Системи виявлення аномалій (Anomaly Detection Systems, ADS) є важливим компонентом забезпечення інформаційної безпеки сучасних комп'ютерних мереж [1] (див. рис. 1). Їхнє призначення – виявлення відхилень у мережевій активності, які можуть сигналізувати про потенційні загрози, зокрема спроби вторгнення, мережеві сканування, витік даних або інші несанкціоновані дії [2].

Однією з найактуальніших проблем у функціонуванні ADS є високий рівень хибнопозитивних спрацювань – випадків, коли нормальна поведінка трактується як аномальна. Причинами цього можуть бути як надмірна чутливість системи, так і недосконаліть використовуваних алгоритмів. Згідно з дослідженнями, у деяких випадках хибнопозитиви становлять до 90% усіх спрацювань, що суттєво ускладнює оперативну роботу фахівців з безпеки [3].

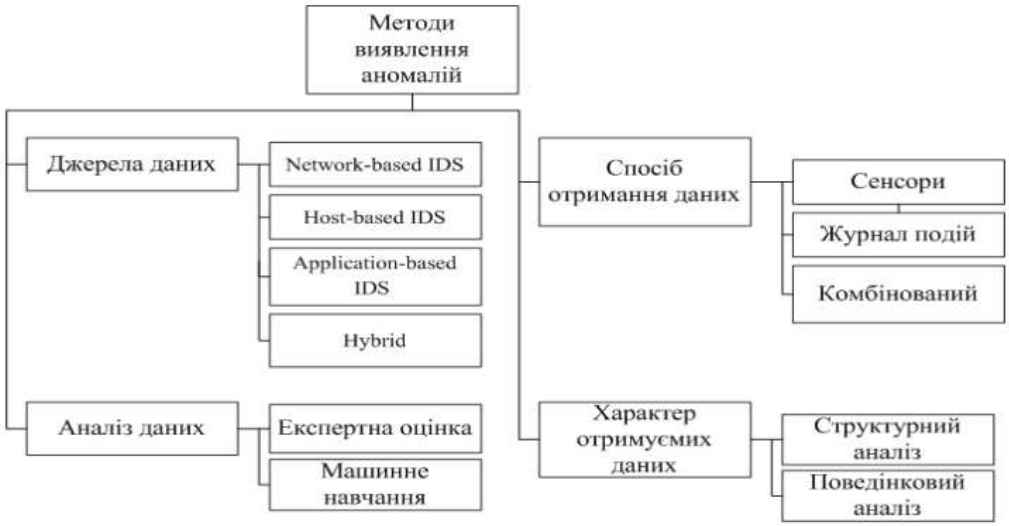

Рисунок 1 – Схема обробки спрацювань у системі виявлення аномалій

Основні фактори, що впливають на частоту хибнопозитивних реакцій:

- Неповнота або зашумленість вхідних даних. Якщо система навчається або працює на основі обмеженої або застарілої інформації, вона неправильно інтерпретує нову активність.
- Використання простих евристичних правил. Такі правила не здатні враховувати контекст подій і часто призводять до помилкових висновків.
- Відсутність адаптивності до змін у мережевому трафіку. Сучасні мережі динамічні, а системи з фіксованими порогами не встигають за цими змінами.

Для вирішення цієї проблеми застосовуються кілька підходів. По-перше, це якісне машинне навчання. Алгоритми класифікації (наприклад, SVM, random forest, нейронні мережі) можуть вчитися розрізняти нормальну та шкідливу активність з урахуванням контексту. Особливо ефективним є використання глибокого навчання (deep learning) для аналізу складних шаблонів трафіку.

По-друге, для уникнення означеної вище проблеми, ефективним є використання гібридних систем відстежування аномалій. Поєднання сигнатурного та поведінкового аналізу дозволяє досягти балансу між точністю і чутливістю. Наприклад, система може використовувати сигнатури для фільтрації відомих атак і поведінковий аналіз для виявлення нових загроз.

По-третє, це метод адаптивного навчання. Системи, які здатні враховувати зворотний зв’язок адміністратора (наприклад, "це спрацювання було хибним"), поступово зменшують кількість помилок у майбутньому.

Висновки: Проблема хибнопозитивних спрацювань є критичною для систем виявлення аномалій, оскільки напряму впливає на ефективність захисту мережевої інфраструктури. Її вирішення можливе завдяки використанню адаптивних, контекстно-орієнтованих підходів, заснованих на машинному навчанні. Надалі

доцільно поглибити дослідження в напрямку пояснюваності моделей та їхньої стійкості до змін у поведінці користувачів і зловмисників.

Література

1. Коробейнікова Т. І., Цар О. О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. *Грааль науки*. 2023. May 2023. С. 321–322. URL: https://doi.org/10.36074/grail-of-science.12.05.2023.050.
2. Хархонов А. В. Виявлення мережевих аномалій за допомогою систем штучного інтелекту / НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ. КИЇВ, 2023. С. 17-20.
3. *Intrusion Detection Systems: A Survey and Taxonomy* / S. Axelsson. Goteborg, Sweden, 2000. С. 5–10.

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В РОЗРОБЦІ МАСШТАБОВАНИХ РЕКОМЕНДАЦІЙНИХ ВЕБ-ПЛАТФОРМ

Привалов А. Г., Рудніченко М. Д.
Національний університет «Одеська політехніка»

Анотація: У статті розглянуто інноваційні технології, що використовуються при створенні масштабованих рекомендаційних веб-платформ. Особливу увагу приділено застосуванню мікросервісної архітектури, хмарних сервісів, алгоритмів машинного навчання, а також сучасних підходів до обробки великих обсягів даних. Проаналізовано приклади успішної інтеграції цих технологій у реальні платформи з персоналізованими рекомендаціями.

Ключові слова: рекомендаційні системи, масштабованість, інноваційні технології, хмарні обчислення, мікросервісна архітектура, машинне навчання.

Вступ. Сучасні веб-платформи, орієнтовані на персоналізацію контенту, активно використовують рекомендаційні системи як ключовий компонент користувацького досвіду. З огляду на зростання обсягів даних, збільшення кількості користувачів і вимоги до швидкодії, актуальним стає впровадження інноваційних технологій, що забезпечують масштабованість і ефективність таких систем [1].

Однією з найважливіших архітектурних концепцій є мікросервісна архітектура. Вона дозволяє розподілити функціональність системи між незалежними сервісами: збір даних, обробка, формування рекомендацій, інтерфейс користувача тощо. Завдяки цьому платформа легко масштабується, кожен компонент може оновлюватися чи масштабуватися незалежно [2].

Для обробки великих обсягів даних активно застосовуються хмарні обчислення, що забезпечують гнучке управління ресурсами. Такі сервіси як AWS, Google Cloud та Microsoft Azure дозволяють інтегрувати обчислювальні ядра, бази

Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ імені К. Д. УШИНСЬКОГО»

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ДРУГА ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Збірник робіт

Збірник робіт надрукований в авторській редакції
без внесення суттєвих змін оргкомітетом

Підписано до друку 25.04.2025
Здано у виробництво 25.04.2025
Формат 60x84/16. Папір офсетний. Друк офсетний.
Тираж 50 примірників

Надруковано з готового оригінал-макета