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

ВИКОРИСТАННЯ ІНКРЕМЕНТАЛЬНО ПІДТРИМУВАНИХ МАТЕРІАЛІЗОВАНИХ ПОДАНЬ У КОРПОРАТИВНИХ ЗАСТОСУНКАХ 239
Пасенченко Т. О., Гунченко Ю. О. 239

АРХІТЕКТУРА ІТ-РІШЕННЯ ЗАБЕЗПЕЧЕННЯ КРОВ'Ю ВІЙСЬКОВИХ МЕДИЧНИХ ШПИТАЛІВ 240
Кашуба М. Д., Чиркова К. С. 240

КОНЦЕПЦІЯ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ ЗАПАСАМИ КОМПОНЕНТІВ КРОВІ 244
Чиркова К. С. 244

ДОСЛІДЖЕННЯ МЕТОДІВ І АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ У СИСТЕМАХ REAL-TIME BIDDING 246
Іванов О. О., Мартинович Л. Я. 246

TEACHERDESMOS ЯК ІНСТРУМЕНТ АКТИВНОГО НАВЧАННЯ: СТВОРЕННЯ ІНТЕРАКТИВНИХ УРОКІВ З МАТЕМАТИКИ 248
Лобушко М. Є., Рикова Л. Л. 248

ОГЛЯД ТЕХНОЛОГІЙ РОЗРОБКИ СИСТЕМИ ВИЯВЛЕННЯ АНОМАЛІЙ У КОМП'ЮТЕРНИХ МЕРЕЖАХ 250
Свиридов І. І., Шпинарева І. М. 250

АНАЛІЗ ПРОБЛЕМИ ВИСОКОГО РІВНЯ ХИБНОПОЗИТИВНИХ СПРАЦЮВАНЬ У СИСТЕМАХ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ 252
Свиридов І. І., Шпинарева І. М. 252

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В РОЗРОБЦІ МАСШТАБОВАНИХ РЕКОМЕНДАЦІЙНИХ ВЕБ-ПЛАТФОРМ 254
Привалов А. Г., Рудніченко М. Д. 254

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ ЗБУРЕНОГО РУХУ ТВЕРДОГО ТІЛА У СЕРЕДОВИЩІ З ОПОРОМ 256
Явдощук І. С., Рачинська А. Л. 256

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ РУХУ СУПУТНИКА-ГІРОСТАТА З ПОРОЖНИНАМИ 257
Кобзар К. В., Рачинська А. Л. 257

ІНФОРМАЦІЙНА СИСТЕМА ПРОГНОЗУВАННЯ ПОПИТУ НА МЕДИЧНІ СТРАХОВКИ СЕРЕД ЛІКАРІВ 258
Федорова К. А. 258

ПРОГРАМУВАННЯ "РОЗУМНОГО АКВАРІУМА" З ВИКОРИСТАННЯМ ARDUINO ЯК ЗАСОБУ НАВЧАННЯ ІНФОРМАТИКИ 260
Реулець М., Корабльов В. А. 260

ЦИВІЛЬНЕ ЗАСТОСУВАННЯ ДРОНІВ У СФЕРІ ОСВІТИ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ 262
Ковальчук Б., Корабльов В. А. 262

2. Графічний калькулятор Desmos. Мобільний додаток. URL: https://play.google.com/ store/apps/developer?id=Desmos+Inc&hl=uk&gl=US (дата звернення 20.04.2025).

ОГЛЯД ТЕХНОЛОГІЙ РОЗРОБКИ СИСТЕМИ ВИЯВЛЕННЯ АНОМАЛІЙ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Свиридов І. І., Шпинарева І. М.

Національний університет «Одеська політехніка»

Анотація: У даній роботі розглядаються основні технології, що використовуються для розробки систем виявлення аномалій у комп'ютерних мережах. Аналізуються методи обробки мережевого трафіку, алгоритми машинного навчання, архітектурні підходи та інструменти для побудови ефективних систем виявлення. Основна увага приділяється точності, швидкодії та здатності таких систем адаптуватися до змін у мережевому середовищі.

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

Системи виявлення аномалій у комп'ютерних мережах (Anomaly Detection Systems – ADS) є важливим елементом комплексного захисту інформаційної інфраструктури. На відміну від сигнатурних систем, які орієнтовані на виявлення відомих атак, ADS фокусуються на виявленні нетипової активності, яка може свідчити про невідомі або нові загрози [1].

Основні етапи побудови ADS включають:

Перший етап побудови ADS заснований на зборі та обробці даних. Важливою передумовою є якісний і репрезентативний набір мережевого трафіку. Для цього застосовуються системи моніторингу (Wireshark, Zeek), мережеві датчики та пакети з відкритими наборами даних [2].

Після цього виконується попередня обробка. До обробки входить нормалізація, фільтрація шуму, агрегація подій та виділення ключових характеристик (features). Це дозволяє підготувати дані до ефективного аналізу без втрати значущої інформації.

Далі моделюється нормальна поведінки. Один із ключових підходів – створення моделі "нормального" стану мережі, що дозволяє виявляти відхилення. Для цього використовуються статистичні методи, правила, дерева рішень, кластеризація та глибокі нейронні мережі [1]. У цьому етапі застосовуються алгоритми машинного навчання, а саме: K-means, DBSCAN – для кластеризації; Random Forest, Decision Trees – для класифікації; Autoencoders, LSTM – у глибокому навчанні; One-Class SVM – для побудови моделей з аномаліями як відхиленням.

Для якісної взаємодії користувача з системою створюється інтерфейс, що включає в себе візуалізація та реакція на аномалії. Ефективна система повинна не лише виявляти аномалії, а й відображати їх у зручному вигляді. Для цього застосовують дашборди (Kibana, Grafana), інтеграцію з SIEM-системами (наприклад, Splunk, Wazuh) тощо.

Також слід зазначити, що надзвичайно важливим є вибір архітектури. Сучасні ADS орієнтовані на мікросервісні або модульні рішення, що дозволяє масштабувати систему залежно від обсягу трафіку (див. рис. 1). Для високонавантажених мереж використовується розподілене обчислення з використанням Apache Kafka, Spark, Flink [1].

Ключовим викликом при створенні таких систем залишається баланс між точністю виявлення та кількістю хибнопозитивних спрацювань. Для досягнення високої ефективності важливе поєднання декількох методів аналізу та можливість адаптивного налаштування моделей.

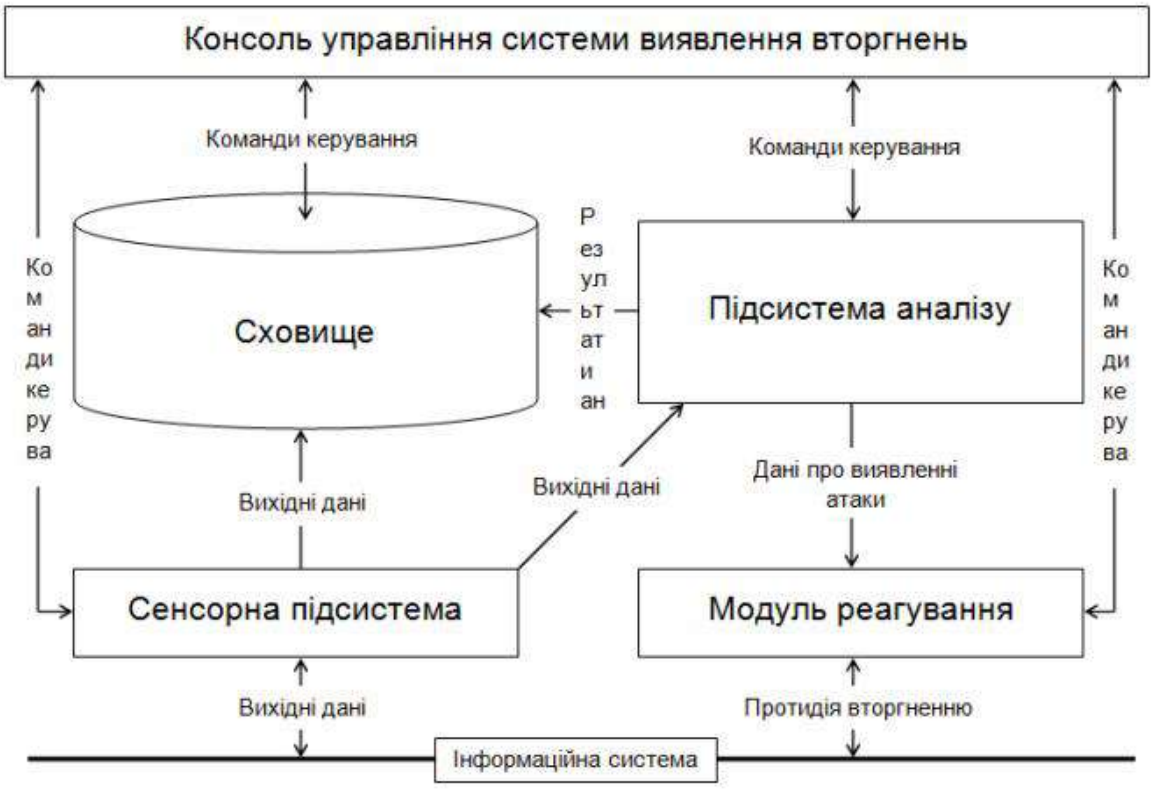

Рисунок 1 – Загальна архітектура системи виявлення аномалій

Висновки: Розробка систем виявлення аномалій вимагає поєднання знань у сфері аналізу даних, мережевих технологій та штучного інтелекту. Використання сучасних архітектурних рішень, інструментів обробки трафіку та алгоритмів машинного навчання дозволяє створювати ефективні системи, здатні адаптуватися до змін у мережевому середовищі та своєчасно виявляти потенційні загрози.

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].

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