УДК 004.8

***Рій А.І., аспірант,***
***Заблоцький С. О., аспірант,***
***Кирик М. І., д.т.н., професор,***
*Національний університет «Львівська політехніка»*

## ГІБРИДНА МОДЕЛЬ ISOLATION FOREST-GAN-TRANSFORMER ДЛЯ АНАЛІЗУ МЕРЕЖЕВИХ АНОМАЛІЙ

**Вступ**

Виявлення аномалій у багатовимірних часових рядах мережевого трафіку вимагає нових підходів, здатних адаптуватися до динамічних змін середовища. У цій роботі представлено гібридну архітектуру IF-DGT, яка поєднує методи статистичного аналізу та глибинного навчання. Такий комплексний підхід дозволяє підвищити точність детектування, ефективно ідентифікуючи як явні аномалії, так і складні, замасковані загрози, що залишаються непомітними для традиційних методів.

**Архітектура та принцип роботи**

Запропонований метод Isolation Forest-Dropout-GAN-Transformer (IF-DGT) є гібридною ансамблевою архітектурою, що аналізує трафік у двох паралельних потоках, як показано на (Рисунок 1 - ).

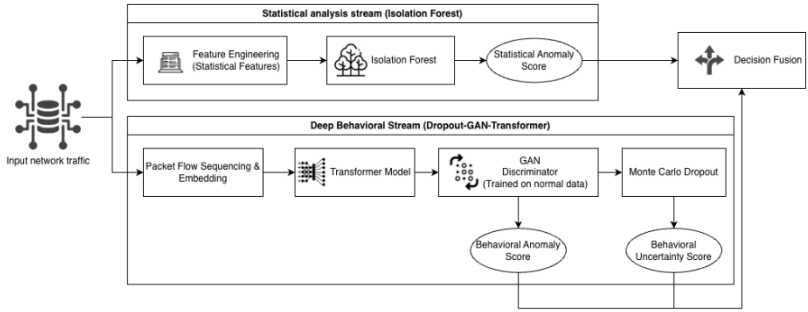


Рисунок 1 – Архітектура комбінованого методу

Перший потік використовує Isolation Forest для високоточного визначення явних статистичних викидів, з якими класичні методи справляються краще та стабільніше. Паралельний DGT-потік працює з прихованими залежностями: Transformer аналізує контекст послідовності, GAN [1] виявляє відхилення від нормального патерну, а MC Dropout оцінює надійність прогнозу [2]. Фінальне рішення формується шляхом об'єднання (стекінгу) цих сигналів. Це дозволяє

системі використовувати сильні сторони обох підходів: Isolation Forest гарантує виявлення "грубих" атак, а DGT розпізнає складні, замасковані вторгнення.

**Експериментальні результати**

Ефективність IF-DGT оцінено на датасеті CIC-IDS2017 та порівняно з двома базовими моделями: Isolation Forest (класичний ML) та Autoencoder (глибоке навчання). Валідація на спектрі атак (зокрема DDoS та Botnet) підтвердила стійкість методу в умовах реального дисбалансу даних. Результати оцінено за метриками F1-Score, Precision та Recall (Таблиця 1).

Таблиця 1 – Оцінка метрик ефективності запропонованих моделей

| Модель | Precision | Recall | F1-Score |
|---|---|---|---|
| Isolation Forest | 0.82 | 0.71 | 0.76 |
| Autoencoder | 0.89 | 0.86 | 0.87 |
| IF-DGT (Наша модель) | 0.91 | 0.88 | 0.89 |

IF-DGT перевершує базові методи за F1-Score, доводячи ефективність поєднання статистичного та поведінкового аналізу для виявлення складних загроз. Високий Precision (0.91) підтверджує мінімум хибних тривог, необхідний для практичного застосування. Водночас, зростання показника Recall до 0.88 (проти 0.71 у Isolation Forest) свідчить про здатність архітектури розпізнавати замасковані низькоінтенсивні аномалії, які губляться на фоні легітимного трафіку при використанні виключно статистичних підходів.

**Висновки**

Запропоновано гібридну архітектуру IF-DGT, що поєднує Isolation Forest та ансамбль Dropout-GAN-Transformer. Експерименти на датасеті CIC-IDS2017 демонструють суттєві переваги методу, показуючи високу точність та повноту виявлення. Здатність до адаптації дозволяє моделі ефективно ідентифікувати навіть нові, невідомі раніше типи загроз у динамічному трафіку. Це робить IF-DGT перспективним рішенням для захисту комп'ютерних мереж.

**Список використаних джерел:**

1. Schlegl T., Seeböck P., Waldstein S. M., Schmidt-Erfurth U., Langs G. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery // International Conference on Information Processing in Medical Imaging (IPMI). 2017. P. 146–157.

2. Shukla A., Jureček M., Stamp M. Social media bot detection using Dropout-GAN // Journal of Computer Virology and Hacking Techniques. 2024. Vol. 20, No. 4. P. 669–680.