УДК 004.7

Лелета В.Р., здобувачка
Колощук М.С., ст. викладач
Дячук О.Ю., ст. викладач
Державний університет "Житомирська політехніка"

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ DDOS-АТАК У МЕРЕЖАХ КОРПОРАТИВНОГО РІВНЯ

Актуальність дослідження зумовлена стрімким зростанням кількості та складності розподілених атак типу відмови в обслуговуванні (Distributed Denial of Service, DDoS), які становлять одну з ключових загроз для сучасних інформаційно-комунікаційних систем. Такі атаки спрямовані на перевантаження мережевих ресурсів і можуть призводити до повної або часткової недоступності сервісів, що, у свою чергу, спричиняє фінансові втрати, порушення бізнес-процесів та зниження рівня довіри користувачів до цифрових платформ. Згідно з сучасними аналітичними звітами, у 2025 році спостерігається суттєве зростання інтенсивності та масштабів DDoS-атак порівняно з попередніми роками, що зумовлює необхідність удосконалення методів їх виявлення та протидії [1].

Традиційні методи виявлення мережевих атак, зокрема сигнатурні та порогові підходи, широко використовуються у системах мережевої безпеки. Проте їх ефективність значно знижується у випадку нових або модифікованих атак, які не мають попередньо відомих сигнатур або характеризуються динамічною поведінкою. Крім того, класичні методи часто потребують значного обсягу ручного налаштування та не здатні адаптуватися до змін у мережевому середовищі. У зв'язку з цим все більшої актуальності набувають підходи, засновані на використанні штучного інтелекту та машинного навчання, які дозволяють автоматизувати процес виявлення аномалій у мережевому трафіку [2].

Одним із перспективних напрямів є застосування методів аналізу потокових даних (flow-based підхід), що базується на агрегованих характеристиках мережевого трафіку, отриманих за допомогою технологій NetFlow, sFlow або IPFIX. На відміну від аналізу повного вмісту пакетів, такий підхід дозволяє істотно зменшити обсяг оброблюваних даних, знизити навантаження на обчислювальні ресурси та забезпечити масштабованість рішень. Це особливо важливо для корпоративних мереж із великим обсягом трафіку, де повний аналіз пакетів є технічно складним або економічно недоцільним.

Додатковою перевагою flow-based підходу є можливість ефективного виявлення аномалій на рівні поведінкових характеристик

трафіку. Зокрема, аналіз таких параметрів, як кількість пакетів у потоці, тривалість сесії, співвідношення вхідного та вихідного трафіку, дозволяє ідентифікувати нетипову активність навіть без доступу до корисного навантаження пакетів. Це є особливо важливим у контексті поширення технологій шифрування, які обмежують можливість глибокого аналізу пакетів (Deep Packet Inspection).

Крім того, flow-based підхід забезпечує сумісність із сучасними мережевими пристроями, оскільки більшість маршрутизаторів і комутаторів підтримують експорт потокових даних. Це дозволяє інтегрувати системи виявлення атак у вже існуючу інфраструктуру без значних додаткових витрат.

Важливим етапом побудови систем виявлення атак є використання навчальних наборів даних. У сучасних дослідженнях широко застосовуються відкриті датасети, зокрема CIC-DDoS2019 та CAIDA DDoS Dataset, які містять як нормальний, так і аномальний мережевий трафік різних типів. Використання таких наборів дозволяє проводити експериментальні дослідження, оцінювати ефективність моделей та порівнювати результати різних підходів у стандартизованих умовах [3, 4].

У межах даного дослідження розглядається підхід до виявлення DDoS-атак, який поєднує використання варіаційного автоенкодера (Variational Autoencoder, VAE) для виявлення аномалій та подальшу класифікацію із застосуванням моделей машинного навчання. Варіаційні автоенкодери належать до класу глибоких генеративних моделей і дозволяють ефективно моделювати нормальну поведінку мережевого трафіку. У процесі навчання модель формує латентний простір, що відображає статистичні характеристики нормальних даних. Відхилення від цього простору можуть інтерпретуватися як аномалії, що потенційно відповідають атакам [5, 6].

Важливою особливістю варіаційних автоенкодерів є їх здатність працювати в умовах відсутності повністю розмічених даних, що часто має місце в задачах інформаційної безпеки. Оскільки реальні мережеві середовища характеризуються високою динамічністю, отримання повноцінних навчальних вибірок з усіма можливими типами атак є складним завданням. У цьому контексті використання напівконтрольованих або неконтрольованих методів навчання дозволяє підвищити адаптивність систем виявлення [5, 6].

Крім того, застосування латентного простору VAE відкриває можливості для подальшого аналізу структури трафіку та виявлення прихованих закономірностей. Це може бути використано не лише для

виявлення атак, але й для класифікації типів аномалій та прогнозування потенційних загроз.

Після етапу виявлення аномалій застосовується другий рівень обробки, який передбачає класифікацію трафіку за допомогою моделей глибокого навчання (Deep Neural Networks) або ансамблевих методів, зокрема XGBoost. Така комбінована архітектура дозволяє поєднати переваги різних підходів: здатність автоенкодера виявляти невідомі атаки та високу точність класифікації, притаманну сучасним алгоритмам машинного навчання [6-9].

Використання ансамблевих методів, таких як XGBoost, дозволяє ефективно обробляти табличні дані та враховувати складні нелінійні залежності між ознаками. У поєднанні з результатами, отриманими на етапі виявлення аномалій, це забезпечує підвищення загальної точності системи. Водночас глибокі нейронні мережі демонструють високу ефективність при роботі з великими обсягами даних, що робить їх доцільними для використання у високонавантажених мережах.

Комбінування різних типів моделей у межах єдиної архітектури дозволяє досягти балансу між швидкістю обробки даних, точністю виявлення та стійкістю до змін у мережевому середовищі.

Запропонований підхід має низку переваг. По-перше, він забезпечує можливість виявлення нових, раніше невідомих типів атак, що є важливим у контексті постійної еволюції кіберзагроз. По-друге, використання агрегованих потокових даних дозволяє зменшити залежність від аналізу повного вмісту пакетів, що позитивно впливає на продуктивність системи та спрощує її впровадження. По-третє, архітектура є масштабованою та може бути інтегрована у сучасні корпоративні мережі без суттєвих змін існуючої інфраструктури.

Водночас слід враховувати й певні обмеження. Зокрема, ефективність моделей машинного навчання значною мірою залежить від якості та репрезентативності навчальних даних. Крім того, використання глибоких нейронних мереж потребує значних обчислювальних ресурсів, що може ускладнювати їх застосування у реальному часі без відповідної оптимізації. Також важливим аспектом є проблема хибнопозитивних спрацювань, яка потребує додаткового дослідження та вдосконалення алгоритмів.

Практичне застосування запропонованого підходу можливе у системах моніторингу корпоративних мереж, центрах обробки даних, а також у хмарних середовищах. Інтеграція таких рішень із системами управління інформаційною безпекою (SIEM) дозволяє автоматизувати

процес виявлення інцидентів та підвищити швидкість реагування на кіберзагрози.

Зокрема, використання потокових даних у поєднанні з методами машинного навчання дає змогу реалізувати безперервний моніторинг мережевого трафіку та оперативно виявляти аномальні події, що є критично важливим для забезпечення стійкості інформаційних систем.

У результаті проведеного аналізу встановлено, що використання методів штучного інтелекту є перспективним напрямом розвитку систем виявлення DDoS-атак. Поєднання генеративних моделей для виявлення аномалій і класифікаційних алгоритмів дозволяє підвищити точність виявлення атак і адаптивність систем до нових типів загроз. Запропонований підхід може бути використаний як основа для побудови інтелектуальних систем мережевої безпеки, орієнтованих на захист корпоративних інформаційних систем.

Перспективи подальших досліджень полягають у розширенні експериментальної бази, оптимізації моделей для роботи в режимі реального часу, а також інтеграції запропонованого підходу з існуючими системами моніторингу та реагування на інциденти інформаційної безпеки [7-9].

Список використаних джерел

1. Cloudflare. DDoS threat report 2025 Q4. – URL: https://radar.cloudflare.com/reports/ddos-2025-q4

2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST SP 800-94).– URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf

3. Canadian Institute for Cybersecurity. CICDDoS2019 dataset. – URL: https://www.unb.ca/cic/datasets/ddos-2019.html

4. CAIDA. The CAIDA DDoS Attack 2007 Dataset. – URL: https://www.caida.org/catalog/datasets/ddos-20070804_dataset/

5. Zavrak S., İskefiyeli M. Anomaly-Based Intrusion Detection From Network Flow Features Using Variational Autoencoder // IEEE Access. – 2020.

6. Kandiero A., Chiurunge P., Munodawafa J. Detection of DDoS Attacks Using Variational Autoencoder-Based Deep Neural Network // Applied Sciences. – 2023.

7. Batool S. et al. A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments // Electronics. – 2025.

8. Ganeshan S., Ramasamy R. A Systematic Review of Machine-Learning-Based Detection of DDoS Attacks // Future Internet. – 2026.

9. Hernandez D. V. et al. Real-Time DDoS Detection in High-Speed Networks Using Deep Learning // Electronics. – 2025.