УДК 004.056.57:004.89

Аннюк П.Б., студент
Вовк Р.Б., к.т.н., доцент
Івано-Франківський національний технічний університет нафти і газу

ЕВОЛЮЦІЯ ТА АРХІТЕКТУРНІ ОСОБЛИВОСТІ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ У СУЧАСНОМУ КІБЕРПРОСТОРІ

Сучасний етап розвитку інформаційно-комунікаційних технологій характеризується експоненціальним розширенням поверхні атак. Традиційні системи виявлення вторгнень (IDS), засновані на детермінованих правилах та сигнатурному аналізі, демонструють низьку ефективність проти софістикованих векторів кібератак, зокрема вразливостей нульового дня (0-day), поліморфного шкідливого ПЗ та складних стійких загроз [1]. Концептуальний перехід від реактивного детектування до інтелектуального аналізу аномалій у великих масивах мережевого трафіку став можливим завдяки імплементації алгоритмів глибокого навчання. Ефективність захисту критичної інфраструктури корелює з обраною архітектурою IDS:

- мережеві системи (NIDS) - здійснюють моніторинг трафіку в реальному часі на рівні сегментів мережі. Основним деструктивним фактором для NIDS є широке застосування протоколів шифрування, що унеможливлює інспекцію корисного навантаження.

- вузлові системи (HIDS) функціонують безпосередньо на кінцевих точках, аналізуючи події операційної системи. Вони є високоефективними для ідентифікації інсайдерських загроз, проте характеризуються значною ресурсомісткістю та складністю адміністрування [2].

Оптимальним підходом вважається впровадження гібридних систем, що синтезують переваги обох архітектур. Емпіричні дані [3] свідчать, що поєднання сигнатурних методів (точність виявлення відомих загроз — 94%, рівень False Positive — 3%) з аномальними методами на базі штучного інтелекту дозволяє нівелювати ризики, пов'язані з невідомими атаками, попри вищий рівень хибнопозитивних спрацювань останніх (до 18%).

Вибір математичного апарату є визначальним для продуктивності IDS. У сучасних дослідженнях виокремлюють такі групи алгоритмів:

1. Навчання з учителем - методи опорних векторів та Випадковий ліс демонструють високу стійкість до шумів. Випадковий ліс забезпечує точність понад 99.9% на верифікованих бенчмарках [1].

2. Навчання без учителя - алгоритми кластеризації (K-Means, DBSCAN) застосовуються для виявлення прихованих закономірностей у немаркованому трафіку.

3. Глибоке навчання:

- CNN - ефективні для ідентифікації просторових кореляцій у структурах пакетів.

- RNN/LSTM спеціалізуються на аналізі часових послідовностей, забезпечуючи детекцію багатоетапних вторгнень із точністю до 99.94%.

- Autoencoders використовуються для ідентифікації аномалій на основі метрик похибки реконструкції вхідних даних.

4. Перспективні напрями - трансформери, великі мовні моделі та пояснювальний штучний інтелект.

Парадигмальний зсув 2026 року полягає в інтеграції архітектур трансформерів та великих мовних моделей як когнітивних контролерів для гетерогенних даних. Для вирішення проблеми непрозорості («чорної скриньки») нейромереж впроваджуються методи пояснювального ШІ, зокрема SHAP та LIME [3]. Це забезпечує інтерпретованість рішень IDS, що є критично важливим для цифрової криміналістики.

Окрему увагу приділено безпеці самих інтелектуальних систем. Захист від адверсаріальних атак (навмисного спотворення вхідних даних) реалізується через методи змагального тренування, ретельну санацію даних та ансамблювання моделей [1].

Отже, створення автономних когнітивних систем захисту вимагає комплексного поєднання гібридних архітектур, інноваційних моделей глибоко навчання та механізмів пояснювального штучного інтелекту. Такий підхід дозволяє трансформувати системи виявлення вторгнень із систем моніторингу в інструменти предиктивного аналізу, здатні блокувати загрози в превентивному режимі.

Список використаних джерел

1. Impact of Machine Learning on Intrusion Detection Systems [Електронний ресурс]. MDPI. 2026. URL: https://www.mdpi.com/2078-2489/16/7/515 (дата звернення: 18.03.2026).

2. AI-Powered Intrusion Detection Systems: Challenges and Opportunities [Електронний ресурс]. ResearchGate. 2026. URL: https://surli.cc/innphk (дата звернення: 18.03.2026).

3. Explainable AI for Forensic Analysis: A Comparative Study of SHAP and LIME in Intrusion Detection Models [Електронний ресурс]. MDPI. 2026. URL: https://www.mdpi.com/2076-3417/15/13/7329 (дата звернення: 18.03.2026).