УДК 004.056.5:004.7

АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ

Свєшніков Д.О.
e-mail: dmytro.svieshnikov@nure.ua
Науковий керівник – д.т.н., проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. Поповського
м. Харків, Україна

This work is devoted to comparative analysis of modern intrusion detection and prevention systems (IDS/IPS), both open source and commercial. The systems were evaluated according to various characteristics, including ML/AI support, the presence of DPI L7, and control types. As a theoretical basis for evaluating the effectiveness of ML-based IDS, a confusion matrix is introduced, with an emphasis on the trade-off between recall and false positive rate inherent in each ML paradigm. The result demonstrates a clear functional division between open and commercial solutions and provides practical recommendations for choosing a system according to your needs.

Через інтенсивний розвиток кіберзагроз зростає необхідність у розвинені систем виявлення та запобігання, оскільки класичні сигнатурні не можуть справлятися з, поширеними зараз, zero-day атаками. Впровадження компонентів ML формує нові класи IDS/IPS і тому вони потребують більш нової методології порівняльного аналізу. Метою роботи є проведення порівняльного аналізу сучасних рішень систем виявлення вторгнень з урахуванням нових характеристик та машинного навчання.

Класифікуються IDS/IPS за принципом виявлення, їх всього три – сигнатурний, аномальний та гібридний. Або ж за рівнем їх розгортання у мережі – мережевий, хостовий та бездротовий. Проте, оскільки сучасні системи отримали багато змін у своєї архітектурі, з’явилися нове покоління класів систем, а саме: NSM та NDR – нове покоління мережевих IDS, EDR та XDR – нове покоління хостових IDS.

Оцінка ML-орієнтованих систем виявлення вторгнень основана на confusion matrix яка має чотири результати класифікації – true positive, false positive, false negative, true negative. Ефективність систем виявлення вторгнень оцінюється за наступними метриками: accuracy, precision, recall, false positive rate, F1-score, ROC-AUC та PR-AUC.

Для порівняння застосовано набір характеристик який відповідає сучасному стану IDS/IPS. Клас визначає до якого типу та покоління відносить система. Рівень спостереження позначає де система розгортається в інфраструктурі – мережа, хост або бездротове середовище. Сигнатури, аномалії, поведінка – чи підтримує система ці методи. Машинне навчання – чи використовується ML як основний елемент архітектури. DPI-L7 – глибокий аналіз пакетів на прикладному рівні, що дозволяє виявляти атаки

приховані в пакетах протоколів цього рівня. Та архітектура: sensor – пасивні сенсори в мережі, agent – агент на хості, framework – модульна платформа, SaaS та Cloud хмарна обробка. Позначення «+» – підтримується, «−» – не підтримується, «+/−» – частково підтримується. Відповідно до цих характеристик складе список, з десяти актуальних у сучасних рішеннях, систем виявлення та запобігання вторгнень.

Таблиця 1 – Порівняльний аналіз систем виявлення вторгнень

Система	Клас системи	Рівень спостереження	Відкритий доступ	Сигнатури	Аномалії	Поведінка	Машине навчання	DPI L7	Архітектура
Snort 3	IDS	Мережа	+	+	−	−	−	+	Sensor
Cisco Secure IPS	IPS	Мережа	−	+	+	+	+/−	+	Appliance
CrowdStrike	EDR/XDR	Хост	−	+	+	+	+	−	Cloud
Darktrace	NDR	Мережа	−	−	+	+	+	+	SaaS
Kismet	WIDS	Бездротове середовище	+	−	+/−	+/−	−	−	Sensor
OSSEC	HIDS	Хост	+	+	−	−	−	−	Agent
Suricata	IDS	Мережа	+	+	+/−	+/−	−	+	Sensor
Vectra AI	NDR	Мережа	−	−	+	+	+	+	Appliance
Wazuh	HIDS	Хост	+	+	+	+	+/−	−	Agent
Zeek (Bro)	NSM	Мережа	+	+	+	+	−	+	Framework

З таблиці 1 можна побачити функціональну різниця між відкритими та комерційними рішеннями. Відкриті рішення краще справляються з виявленням атак сигнатурним методом, ML в них не підтримується або у якості додаткового модуля, наприклад, як у Wazuh та Zeek. У комерційних системах таких як Darktrace та CrowdStrike архітектура будується навколо машинного навчання.

Сигнатурні системи мають низький рівень FAR до відомих атак, але Recall для невідомих атак нульовий [2]. Системи які використовують машинне навчання без підкріплення, наприклад, Darktrace, можуть виявляти невідомі атаки, але при цьому мають високий FAR через те що часто класифікують легітимний трафік як загрозу. Системи з машинним навчанням з підкріпленням, такі як CrowdStrike та Cisco, тримає баланс між Precision та Recall для відомих класів атак, але неефективний для нових типів вторгнень. Теоретично, найбільшу стійкість мають гібридні системи, такі як Vectra AI та Wazuh, оскільки використовують обидва підходи, і закривають недоліки обох типів [3].

Основною властивістю будь-якого класифікатора є компроміс між Recall та FPR, який відображається через ROC криву. Якщо зробити упор на виявлення більшої кількості атак шляхом підвищення чутливості системи, це призведе до зростання хибних спрацьовувань [4]. З цього можна зробити висновок, що не існує кращої універсальної системи, тобто вибір системи залежить виключно від середовища розгортання. Системи, в яких використовується адаптивне навчання, такі як Wazuh, Darktrace та Vectra AI, здатні покращувати цей компроміс залежно від часу скільки вони працюють – з часом система накопичує дані про нормальну поведінку трафіку. Згодом модель буде краще відрізняти легітимний трафік, тобто FPR буде знижуватися, а recall навпаки – підвищуватися. Саме це і є перевагою ML-орієнтованих систем над сигнатурними, але тільки у довгостроковій перспективі [3].

Якщо дивитися зі сторони архітектури, то сенсорні системи забезпечують мережеве покриття і не впливають на продуктивність інфраструктури в цілому, але не мають видимості у кінцевих точках. Системи з агентами бачать усі події у кінцевих точках, проте необхідно встановлення цих агентів на кожен хост. Хмарні вирішують проблему завдяки наявності ML обробки централізовано на сервері зі сторони виробника цих систем, також плюсом буде і оновлення моделі навчання для клієнтів без необхідності власного навчання.

Список використаних джерел:

1. Терейковський І. А., Корченко А.О., Паращук Т.І., Педченко Є.М. Аналіз відкритих систем виявлення вторгнень // Безпека інформації. – 2018 – Т. 24, № 3. – С. 201-216. – DOI: 10.18372/2225-5036.24.13431 (Дата звернення: 07.02.2026).

2. A Survey of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions. – 2023 – URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9890381/pdf/nihms-1856717.pdf (Дата звернення: 21.02.2026).

3. Bampoe, D. K. O. The Advantages of Hybrid Intrusion Detection Systems: A Comparative Study of Anomaly-Based and Signature-Based Approaches / Daniel Kofi Odame Bampoe // Journal of Novel Research and Innovative Development. – 2025. – Vol. 3, Issue 1. – ISSN 2984-8687. – URL: https://tijer.org/jnrid/papers/JNRID2501013.pdf (дата звернення: 22.02.2026).

4. Anomaly detection optimization using big data and deep learning to reduce false-positive. Journal of Big Data. URL: https://arxiv.org/pdf/2209.13965 (Дата звернення: 22.02.2026).