УДК 004.056.53:004.42

Д. О. Пінчук
І. О. Бондаренко

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК У СИСТЕМАХ IDS

Вінницький національний технічний університет

Анотація

Зростання кількості кіберзагроз у сучасних інформаційних системах обумовлює необхідність використання ефективних механізмів моніторингу та виявлення атак у мережевій інфраструктурі. Одним із ключових інструментів забезпечення кібербезпеки є системи виявлення вторгнень (Intrusion Detection Systems, IDS), які аналізують мережеву активність та визначають підозрілі або шкідливі дії. У роботі розглянуто основні алгоритми виявлення атак у системах IDS, зокрема сигнатурні методи, методи виявлення аномалій та методи на основі машинного навчання. Проведено порівняльний аналіз зазначених алгоритмів за критеріями ефективності виявлення атак, точності та кількості хибних спрацювань.

Ключові слова: системи виявлення вторгнень (IDS), сигнатурні алгоритми, алгоритми виявлення аномалій, модель Denning, машинне навчання, виявлення мережевих атак, кібербезпека, порівняльний аналіз

Abstract

The growing number of cyber threats in modern information systems necessitates the use of effective mechanisms for monitoring and detecting attacks in network infrastructure. One of the key tools for ensuring cybersecurity is intrusion detection systems (IDS), which analyse network activity and identify suspicious or malicious actions. This paper discusses the main algorithms for detecting attacks in IDS systems, in particular signature-based methods, anomaly-based approaches, and machine learning-based methods. A comparative analysis of these algorithms is performed based on the criteria of attack detection efficiency, accuracy, and number of false positives.

Keywords: intrusion detection systems (IDS), signature-based algorithms, anomaly-based algorithms, Denning model, machine learning, network attack detection, cybersecurity, comparative analysis

Вступ

З розвитком інформаційних технологій та збільшенням обсягів мережевого трафіку зростає і кількість кіберзагроз, спрямованих на інформаційні системи та комп'ютерні мережі. Сучасні атаки можуть призводити до порушення конфіденційності, цілісності та доступності інформації, що створює значні ризики для організацій та державних установ. У зв'язку з цим, одним із ключових напрямів забезпечення кібербезпеки є використання систем моніторингу та виявлення вторгнень, які дозволяють своєчасно ідентифікувати підозрілу активність у мережі та запобігати реалізації атак [1].

Системи виявлення вторгнень (IDS) є програмно-апаратними засобами, призначеними для автоматизованого моніторингу подій у комп'ютерних системах та мережах та аналізу цих подій з метою виявлення можливих інцидентів інформаційної безпеки. Такі системи здійснюють збір та аналіз даних про мережевий трафік, системні журнали та інші події, що дозволяє виявляти спроби несанкціонованого доступу, експлуатації вразливостей або інші шкідливі дії [2].

Результати дослідження

Залежно від способу розгортання системи IDS поділяються на мережеві (Network-based IDS, NIDS) та хостові (Host-based IDS, HIDS). Мережеві системи здійснюють аналіз мережевого трафіку з метою виявлення атак, що спрямовані на мережеву інфраструктуру, тоді як хостові системи контролюють події, що відбуваються безпосередньо на окремих вузлах або серверах, включаючи системні журнали, зміни файлів та поведінку процесів [3].

Ефективність систем IDS значною мірою залежить від алгоритмів виявлення атак, які використовуються для аналізу даних. У сучасних системах застосовуються різні підходи до детектування вторгнень, серед яких найбільш поширеними є сигнатурні алгоритми, методи виявлення аномалій та алгоритми на основі машинного навчання. Кожен із цих підходів має власні переваги та обмеження, що зумовлює необхідність їх детального порівняльного аналізу [4].

Одним із найбільш поширених підходів до виявлення мережевих атак у системах IDS є сигнатурний метод. Його принцип роботи полягає у порівнянні мережевого трафіку або системних подій із заздалегідь визначеною базою сигнатур відомих атак. Сигнатура представляє собою характерний шаблон або послідовність дій, що відповідає конкретному типу шкідливої активності. Якщо аналізований трафік відповідає одній із сигнатур у базі, система генерує попередження про можливу атаку [2].

Сигнатурні алгоритми широко застосовуються у сучасних системах виявлення вторгнень, таких як Snort та Suricata. Основною перевагою такого підходу є висока точність виявлення відомих атак та низька кількість хибних спрацювань. Водночас суттєвим обмеженням є неможливість виявлення нових або модифікованих атак, сигнатури яких відсутні у базі даних. Тому ефективність сигнатурних систем значною мірою залежить від регулярного оновлення бази сигнатур [5].

Іншим важливим підходом до виявлення вторгнень є використання методів виявлення аномалій. Ці методи ґрунтуються на формуванні моделі нормальної поведінки системи або мережі, після чого будь-яке значне відхилення від цієї моделі розглядається як потенційна загроза безпеці. Системи аналізують такі параметри, як частота мережевих з'єднань, обсяг переданих даних, поведінка користувачів та інші характеристики трафіку [6].

Однією з перших концептуальних моделей виявлення атак є модель, запропонована Dorothy Denning. У своїй роботі «A Model for Intrusion Detection» дослідниця описала підхід до моніторингу системної активності на основі статистичних показників та профілів поведінки користувачів. Згідно з цією моделлю, система IDS формує базовий профіль нормальної роботи системи, після чого аналізує відхилення від нього, що можуть свідчити про несанкціоновану діяльність або мережеву атаку [7].

Основною перевагою підходу виявлення аномалій є здатність виявляти нові та раніше невідомі атаки. Однак недоліком таких алгоритмів є висока кількість хибних спрацювань, оскільки навіть легітимні зміни у поведінці користувачів або системи можуть інтерпретуватися як потенційна загроза. Крім того, побудова коректної моделі нормальної поведінки потребує значних обсягів даних та тривалого періоду навчання системи [4].

У сучасних системах кібербезпеки дедалі ширше використовуються алгоритми машинного навчання для виявлення мережевих атак. Такі алгоритми дозволяють автоматично аналізувати великі обсяги мережевого трафіку та визначати складні закономірності, що можуть свідчити про наявність шкідливої активності. Використання машинного навчання дає можливість підвищити точність детектування атак і зменшити кількість хибних спрацювань у порівнянні з традиційними методами [1].

У системах IDS можуть застосовуватися різні алгоритми машинного навчання, зокрема метод опорних векторів (SVM), дерева рішень, Random Forest, а також нейронні мережі. Такі методи дозволяють здійснювати класифікацію мережевого трафіку та визначати, чи належить певна активність до нормальної поведінки або до категорії атак. Для навчання моделей часто використовуються спеціалізовані набори даних, наприклад KDD Cup 1999 або NSL-KDD, які містять приклади різних типів мережевих атак [1].

Попри високу ефективність, використання алгоритмів машинного навчання має певні обмеження. Зокрема, такі методи потребують значних обчислювальних ресурсів, великих навчальних вибірок та ретельної підготовки даних. Крім того, складність інтерпретації результатів деяких моделей може ускладнювати практичне використання таких систем у реальних мережевих середовищах [6].

Для оцінки ефективності різних підходів до виявлення мережевих атак доцільно провести їх порівняння за основними характеристиками, такими як здатність виявляти нові атаки, точність детектування та кількість хибних спрацювань. Узагальнення характеристик сигнатурних, алгоритмів виявлення аномалій та методів машинного навчання наведено в таблиці 1 [4].

Таблиця 1 – Порівняльна характеристика алгоритмів виявлення атак у системах IDS

Тип алгоритму	Принцип роботи	Переваги	Недоліки
Сигнатурний	Порівняння трафіку з базою сигнатур відомих атак	Висока точність для відомих атак, низька кількість хибних спрацювань	Не виявляє нові атаки
Виявлення аномалій	Аналіз відхилень від моделі нормальної поведінки	Виявлення нових та невідомих атак	Велика кількість false positives

Продовження таблиці 1

Машинне навчання	Класифікація трафіку за допомогою ML-алгоритмів	Висока точність, здатність аналізувати великі обсяги даних	Потреба у великих датасетах та обчислювальних ресурсах

Проведений аналіз свідчить, що жоден із розглянутих підходів не є універсальним. У сучасних системах кіберзахисту все частіше використовуються гібридні IDS, які поєднують кілька методів виявлення атак для підвищення загальної ефективності системи [6].

Висновки

Зростання кількості кіберзагроз та ускладнення мережевого трафіку обумовлює необхідність використання ефективних систем виявлення вторгнень (IDS) для забезпечення безпеки інформаційних систем. Аналіз показав, що сигнатурні алгоритми є ефективними для виявлення відомих атак і характеризуються високою точністю, проте не здатні виявляти нові види вторгнень. Алгоритми виявлення аномалій дозволяють виявляти раніше невідомі атаки, але мають значну кількість хибних спрацювань. Алгоритми на основі машинного навчання демонструють високу точність і здатність обробляти великі обсяги даних, проте потребують ресурсів та якісних навчальних даних.

Найефективнішими в сучасних системах кібербезпеки є гібридні IDS, які поєднують кілька методів виявлення атак. Такий підхід дозволяє зменшити недоліки окремих алгоритмів і підвищити загальну ефективність системи. Вибір конкретного алгоритму або комбінації методів залежить від специфіки мережевої інфраструктури, доступних ресурсів та типів атак, характерних для організації. Впровадження ефективної IDS забезпечує своєчасне реагування на кіберзагрози та зменшує ризики інформаційних інцидентів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Andrea Pinto. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. MDPI. URL: https://www.mdpi.com/1424-8220/23/5/2415 (дата звернення: 05.03.2026).
2. Karen Scarfone. Guide to Intrusion Detection and Prevention Systems. NIST Technical Series Publications. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf (дата звернення: 05.03.2026).
3. Karen A. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST. URL: https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps (дата звернення: 06.03.2026).
4. Yogita Sharma. Intrusion Detection System: A Survey Using Data Mining and Learning Methods | Sharma | Computer Engineering and Intelligent Systems. Academic Hosting & Event Management Solutions. URL: https://iiste.org/Journals/index.php/CEIS/article/view/38615 (дата звернення: 06.03.2026).
5. Martin Roesch. SNORT – LIGHTWEIGHT INTRUSION DETECTION FOR NETWORKS. USENIX Home | USENIX. URL: https://www.usenix.org/legacy/events/lisa99/full_papers/roesch/roesch.pdf (дата звернення: 07.03.2026).
6. D. Milovanovic. A third order sigma-delta modulator. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/1314900 (дата звернення: 07.03.2026).
7. Dorothy Denning. An Intrusion-Detection Model. Department of Computer Science | CSU – Department of Computer Science at Colorado State University. URL: https://www.cs.colostate.edu/~cs656/reading/ieee-se-13-2.pdf (дата звернення: 08.03.2026).

Пінчук Дар'я Олександрівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Бондаренко Ірина Олексіївна **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Pinchuk Daria O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Bondarenko Iryna O. **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua