*УДК 004.056.53*

# МЕТОДИ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

*Хлівенко Р.А.*
r.hlivenko@gmail.com
*Черкаський державний фаховий бізнес-коледж*
*Бреус Р.В.*
*м. Черкаси, Україна*

Зі зростанням масштабів використання комп'ютерних мереж та цифрових сервісів значно підвищується кількість і складність кіберзагроз. Сучасні атаки характеризуються високим рівнем автоматизації, адаптивністю та здатністю обходити традиційні засоби захисту. У зв'язку з цим методи виявлення кіберзагроз стають критично важливим компонентом систем інформаційної безпеки. Ефективність цих методів визначає здатність своєчасно ідентифікувати потенційні атаки, мінімізувати їх наслідки та забезпечити безперервність функціонування інформаційних систем.

Основною метою даного дослідження було проаналізувати основні методи виявлення кіберзагроз у комп'ютерних мережах, дослідити їх особливості реалізації та визначити ключові переваги й обмеження з точки зору ефективності, точності та продуктивності.

Методи виявлення кіберзагроз у комп'ютерних мережах поділяються на кілька основних класів, серед яких найбільш поширеними є сигнатурні, аномалійні та гібридні підходи [1].

Сигнатурний підхід базується на використанні заздалегідь визначених шаблонів атак (сигнатур). Кращі результати цей метод демонструє при виявленні відомих загроз, оскільки дозволяє швидко ідентифікувати характерні ознаки шкідливої активності. Проте його ефективність суттєво знижується у випадку нових або модифікованих атак, для яких сигнатури ще не сформовані [2].

Аномалійний підхід орієнтований на аналіз поведінки мережі та виявлення відхилень від нормального стану. Фактично це означає, що система формує модель «нормальної» активності, після чого всі нетипові дії розглядаються як потенційні загрози. Кращі результати досягаються при використанні

статистичних методів і алгоритмів машинного навчання, що дозволяє виявляти раніше невідомі атаки. Водночас цей підхід характеризується підвищеною кількістю хибних спрацювань [3].

Гібридні методи поєднують сигнатурний та аномалійний підходи, що дозволяє компенсувати їхні недоліки. У таких системах одночасно використовується база відомих атак і механізми аналізу поведінки, що підвищує загальну ефективність виявлення загроз.

Порівняльна характеристика основних методів виявлення кіберзагроз наведена в табл. 1.

Таблиця 1 – Порівняльна характеристика методів виявлення кіберзагроз

| № | Функціональний компонент | Сигнатурний метод | Аномалійний метод | Гібридний метод |
|---|---|---|---|---|
| 1 | Принцип роботи | Пошук відомих сигнатур | Виявлення відхилень від норми | Комбінування підходів |
| 2 | Ефективність | Висока для відомих атак | Висока для нових атак | Висока загальна |
| 3 | Хибні спрацювання | Низькі | Високі | Середні |
| 4 | Складність реалізації | Низька | Висока | Висока |

Значну роль у реалізації методів виявлення кіберзагроз відіграють системи виявлення та запобігання вторгненням (IDS/IPS). Вони аналізують мережевий трафік у режимі реального часу та дозволяють ідентифікувати підозрілу активність. Кращі результати досягаються при інтеграції таких систем із централізованими платформами моніторингу, такими як SIEM, що забезпечують кореляцію подій безпеки з різних джерел [4].

Сучасні підходи активно використовують технології машинного навчання, які дозволяють автоматизувати процес аналізу великих обсягів даних. Алгоритми класифікації, кластеризації та нейронні мережі забезпечують більш точне виявлення складних атак, зокрема багатовекторних і розподілених. Однак їх застосування пов’язане з високими вимогами до обчислювальних ресурсів та необхідністю якісних навчальних вибірок [5].

Таким чином, ефективність систем виявлення кіберзагроз визначається вибором відповідної архітектури, яка повинна враховувати баланс між точністю, швидкодією та складністю реалізації.

У роботі проаналізовано основні методи виявлення кіберзагроз у комп'ютерних мережах та визначено їх ключові характеристики. Встановлено, що сигнатурні методи є ефективними для відомих атак, тоді як аномалійні підходи дозволяють виявляти нові загрози. Найбільш перспективним є використання гібридних систем, які поєднують переваги обох підходів. Подальший розвиток цієї галузі пов'язаний із впровадженням технологій штучного інтелекту та вдосконаленням алгоритмів аналізу мережевих даних.

**Список використаних джерел:**


1. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. Pearson, 2017. 816 p.
2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (дата звернення: 18.03.2026).
3. Behl A., Behl K. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2017. 320 p.
4. Garfinkel S., Spafford G. Practical UNIX and Internet Security. 3rd ed. O'Reilly Media, 2003. 988 p.
5. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010. URL: https://ieeexplore.ieee.org/document/5504793 (дата звернення: 18.03.2026).