УДК 004.056.53
М. Гладчук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИЯВЛЕННЯ АНОМАЛІЙ У ВЕЛИКИХ ДАНИХ ЯК ІНСТРУМЕНТ ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ

UDC 004.056.53
M. Hladchuk

DETECTION OF ANOMALIES IN BIG DATA AS A TOOL FOR CYBER THREAT PREDICTION

Виявлення аномалій у великих даних як інструмент прогнозування кіберзагроз

Сучасний стрімкий розвиток інформаційних технологій породжує як нові можливості, так і загрози, зокрема у сфері кібербезпеки. Основним завданням стає виявлення аномалій у великих даних, які часто сигналізують про можливі кіберзагрози. Зокрема, такі методи є ключовими для ідентифікації відхилень у поведінкових патернах мережевого трафіку або користувачів.

Аномалії у великих даних – це відхилення від нормальних патернів, які вимагають ефективних методів обробки. Використання алгоритмів машинного навчання, таких як кластеризація (K-means) та нейронні мережі, дозволяє аналізувати масиви інформації, які генеруються в реальному часі. Наприклад, кластеризація допомагає ідентифікувати точки даних, що не відповідають жодному кластеру, сигналізуючи про потенційні загрози. Методи на основі глибокого навчання забезпечують високу точність виявлення, проте є ресурсомісткими.

На практиці методи виявлення аномалій впроваджуються через платформи обробки великих даних, такі як Apache Spark. Наприклад, ізоляційні ліси (Isolation Forest) демонструють ефективність у реальному часі для виявлення рідкісних подій у фінансових та корпоративних системах. Водночас, проблеми шуму у даних або динамічних змін у поведінкових патернах можуть знижувати продуктивність алгоритмів.

Дослідження методів аналізу великих даних дозволяє ідентифікувати найефективніші алгоритми для різних задач кібербезпеки. Результати підтверджують, що поєднання традиційних підходів із сучасними алгоритмами забезпечує гнучкість та надійність системи. Подальший розвиток технологій, таких як квантові обчислення, відкриває нові можливості для вдосконалення прогнозування кіберзагроз.

Література

1. Xu, X., Wang, X. «Anomaly detection based on one-class SVM inwireless sensor networks» // Lecture Notes in Computer Science. – Berlin: Springer, 2005. – Vol. 3644. – P. 271–282.
2. Breunig, M.M. et al. «LOF: Identifying density-based local outliers» // ACM SIGMOD Record. – 2000. – Vol. 29, No. 2. – P. 93–104.
3. Song, X., Wu, M., Jermaine, C., Ranka, S. «Conditional anomalydetection» // IEEE Transactions on Knowledge and Data Engineering. – 2007. – Vol. 19, No. 5. – P. 631–645.
4. Pang, G. et al. «Deep learning for anomaly detection: A review» // ACM Computing Surveys. – 2021. – Vol. 54, No. 2. – P. 1–38.