УДК 004.65:004.89]:004.056

Орлівська Вікторія Олегівна
(наук. керівник – канд. техн. наук, доцент Загоруйко Л. В.)
Донецький національний університет імені Василя Стуса, м. Вінниця

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У СФЕРІ КІБЕРБЕЗПЕКИ

Сучасні комп'ютерні системи, що використовуються в різних галузях, стають не лише складнішими, але й вразливішими перед різноманітними кіберзагрозами. Через це застосування інтелектуального аналізу даних набуває критичного значення для забезпечення безпеки цих систем.

Інтелектуальний аналіз даних системних журналів дає змогу не лише виявляти незвичайні події та аномалії в реальному часі, але й активно реагувати на них, сприяючи запобіганню кібератакам та непередбаченим проблемам, що може забезпечити більшу ефективність і надійність функціонування комп'ютерних систем.

Інтелектуальний аналіз даних дає змогу виявляти аномальні зміни в поведінці системи чи мережі, що можуть свідчити про можливі кіберзагрози. Шляхом аналізу історичних даних та виявлення патернів системи можуть прогнозувати майбутні атаки, це також допомагає автоматизувати процес виявлення аномалій і атак, що значно підвищує ефективність та швидкість реагування на кіберзагрози. Також аналіз отриманих даних дає змогу виявляти слабкі місця у системі безпеки та розробляти стратегії їх покращення [1].

Методи машинного навчання та штучного інтелекту використовуються для виявлення аномалій у комп'ютерних системах у кібербезпеці. Серед них варто зазначити навчання з учителем та без учителя, а також глибоке навчання.

Навчання з учителем – це процес, у якому модель навчається на основі попередньо позначених прикладів вхідних даних та відповідних їм вихідних міток й встановлює зв'язок між ними. Навчання без учителя – це процес, під час якого модель навчається на непозначених даних, тобто на даних, де аномалії або класифікаційні мітки відсутні. Модель самостійно вивчає структуру даних та виявляє аномалії шляхом розпізнання відхилень від типових патернів [2]. Натомість метод глибокого навчання використовує нейронні мережі з багатьма шарами для автоматичного вивчення високорівневих представлень даних. Цей метод використовується для розв'язання складних завдань, як-от розпізнавання образів, розпізнавання мови, аналіз текстів тощо. Одна з ключових особливостей методу глибокого навчання полягає в тому, що він дає змогу моделі автоматично вивчати ієрархічні або складні функції представлення даних за допомогою використання багатьох шарів обробки інформації [3].

Застосування методів машинного навчання має переваги – автоматизацію виявлення аномалій та реакцію на кіберзагрози в реальному часі. Однак існують і недоліки – складність налаштування та обробки великих обсягів даних. Результати попередніх досліджень показують успішні випадки використання цих методів у кібербезпеці, що свідчить про їх ефективність.

Але є деякі недоліки, що включають можливість хибнопозитивних або хибнонегативних результатів, особливо під час роботи з великими обсягами даних або в умовах невідомих типів аномалій. До того ж ці методи можуть бути вразливими до атак, спрямованих на обман або обхід систем виявлення аномалій.

Статистичні методи виявлення аномалій базуються на аналізі статистичних властивостей даних для виявлення відхилень або аномальних патернів, що можуть вказувати на потенційні загрози безпеці. Ці методи використовують різноманітні статистичні моделі та техніки, як-от засоби контролю за рівнем довіри, методи кластеризації, збіжність даних та відступи від середнього значення, для виявлення аномалій.

Один із видів статистичних методів виявлення аномалій полягає в застосуванні методу кластеризації, який використовує алгоритми для групування даних у визначені кластери – як аномальні, так і нормальні дані. До того ж існують методи, які базуються на аналізі даних із використанням статистичних метрик, як-от середнє значення, дисперсія та коефіцієнти кореляції, для виявлення відхилень від типової поведінки. Також використовуються методи статистичного тестування, які дають змогу перевіряти гіпотези щодо розподілу даних та визначати аномалії [4].

Однією з основних переваг статистичних методів є їх широке застосування та здатність робити припущення про характерні властивості даних без необхідності великих обсягів навчальних даних. Вони можуть бути ефективними для виявлення широкого спектру аномалій у реальному часі.

Однак серед недоліків може бути обмежена здатність до виявлення складних аномалій, що можуть мати складну структуру або бути змішаними з нормальними даними. До того ж статистичні методи можуть бути вразливими до хитрощів та вимагати ретельного налаштування параметрів для досягнення оптимальної продуктивності.

У майбутньому статистичні методи можуть стати більш ефективними завдяки поєднанню з іншими методами машинного навчання, як-от нейронні мережі або глибокі моделі навчання для того, щоб створювати більш точні моделі, які зможуть ефективно виявляти складні аномалії та атаки. Одним з основних викликів буде забезпечення ефективності та точності методів в умовах швидкої зміни кіберпростору та розвитку нових типів загроз. До того ж статистичні методи можуть стикатися з обмеженнями в обробці великих обсягів даних та недостатньою здатністю до автоматичного виявлення складних аномалій без додаткового навчання [5].

Для покращення методів інтелектуального аналізу для виявлення аномалій у майбутньому необхідно приділяти увагу деяким питанням. По-перше, важливо забезпечити постійне оновлення моделей та алгоритмів з урахуванням нових кіберзагроз та технологічних досягнень. Також необхідно розвивати методи захисту від атак, спрямованих на самі системи виявлення аномалій, включно з заходами безпеки даних та архітектурними заходами. До того ж важливо вдосконалювати методи взаємодії між людьми та автоматизованими системами виявлення аномалій для більш ефективного виявлення та управління кіберзагрозами [6].

Інтелектуальний аналіз даних відкриває нові можливості для ефективного виявлення, прогнозування та запобігання кіберзагрозам. Виявлено широкий спектр застосувань статистичних методів, машинного навчання та інших технік штучного інтелекту, що дасть змогу створювати розумні системи, які постійно вдосконалюються і адаптуються до змін у кіберпросторі. Розглянуто перелік недоліків та майбутніх викликів інтелектуального аналізу.

Список використаних джерел

1. Yaniv Harel, Irad Ben Gal, Yuval Elovici. Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. ACM Transactions on Intelligent Systems and Technology. 2017. Vol. 8, iss. 4. Art. № 49. P. 1–12. DOI: 10.1145/3057729.

2. The Benefits of Integrating Intelligence and Investigative Analysis. URL: https://www.securitymagazine.com/articles/88618-the-benefits-of-integrating-intelligence-and-investigative-analysis (дата звернення: 16.02.2024).

3. Anomaly Detection Based on Deep Learning: Insights and Opportunities / H. Zhang, R. Xie, K. Li, W. Huang, C. Yang , J. Liu. *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom).* 2023. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10195601&isnumber=10195273 (дата звернення: 16.02.2024).

4. Netspot: A Simple Intrusion Detection System with Statistical Learning / P. Siffer, A. Fouque, A. Termier, C. Largouet. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).* 2020. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9343018&isnumber=9342964 (дата звернення: 17.02.2024).

5. Intrusion Detection Systems: A Comprehensive Review / H.-J. Liao, Ch.-H. R. Lin, Y.-Ch. Lin, K.-Y. Tung. *Journal of Network and Computer Applications.* Vol. 36, iss. 1, January, 2013. P. 16–24. URL: https://link.springer.com/article/10.1007/s10586-022-03776-z (дата звернення: 17.02.2023).

6. Sarker I. H. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science.* Vol. 10. P. 1473–1498. 2023. DOI: 10.1007/s40745-022-00444-2.

Анотація. У роботі проведено огляд перспектив застосування інтелектуального аналізу даних у сфері кібербезпеки.

Ключові слова: штучний інтелект, кіберпростір, інтелектуальний аналіз.

УДК 004.775:004.451.7]:659.4:334.72

Палецька Альона Олегівна
(наук. керівник – канд. пед. наук, доцент Карпенко О. О.)
Державний університет інформаційно-комунікаційних технологій, м. Київ

СУЧАСНИЙ СТАН ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У PR-ДІЯЛЬНОСТІ ПІДПРИЄМСТВ

Постановка проблеми. У сучасному світі, коли швидкість і доступність інформації стали ключовими факторами успіху, використання інформаційно-комунікаційних технологій (ІКТ) у діяльності підприємств виявляється не лише необ-