УДК 004.8

М. В. Березюк

THE USE OF MACHINE LEARNING FOR THREAT ANALYSIS AND RISK MANAGEMENT

Vinnytsia National Technical University

Анотація

Доповідь присвячена використанню методів машинного навчання у сфері аналізу загроз та управління ризиками. Враховано актуальні технічні підходи та алгоритми, що дає змогу ефективно ідентифікувати потенційні небезпеки та вдосконалювати процеси прийняття рішень у рамках управління ризиками.

Ключові слова: машинне навчання (ML), штучний інтелект (AI), аналіз загроз, управління ризиками, великі дані, алгоритми

Abstract

This report is dedicated to the use of machine learning methods in the field of threat analysis and risk management. It examines current technological approaches and algorithms that can effectively identify potential threats and improve decision-making processes in the context of risk management.

Keywords: machine learning (ML), artificial intelligence (AI), threat analysis, risk management, big data, algorithms

Introduction

In today's world, businesses are becoming increasingly dependent on technology, making them susceptible to cyberattacks. Consequently, the importance of threat analysis and risk management is escalating. The relevance of utilizing machine learning for threat analysis and risk management cannot be overstated. The capability of artificial intelligence systems to effectively predict potential threats and respond to them has become a crucial component of modern security strategies.

Research results

Machine learning (ML) is a type of artificial intelligence (AI) that allows computers to learn without being explicitly programmed [1]. ML algorithms identify patterns in data and use them to make predictions or decisions. There are three main types of machine learning:

– supervised learning;
– unsupervised learning;
– reinforcement learning.

Threat analysis using machine learning. Machine learning (ML) has become a powerful tool in the field of cyber security. It can be used to analyze and predict threats based on patterns and anomalies in data.

Moreover, ML can automate the process of threat detection, reducing the need for manual intervention and increasing the speed and efficiency of threat response. However, it’s important to note that while ML can enhance threat analysis, it’s not a silver bullet. It should be used as part of a comprehensive security strategy.

Risk management using machine learning. ML is transforming risk management by enabling organizations to predict and mitigate potential risks more effectively. ML algorithms can analyze vast amounts of data to identify patterns and trends that might indicate potential risks.

In the field of financial risk management, ML and AI are revolutionizing how we approach understanding and controlling risk [2]. From deciding how much a bank should lend to a customer, to providing warning signals to financial market traders about position risk, to detecting customer and insider fraud, and improving compliance and reducing model risk.

However, it’s important to note that while ML can significantly improve risk management, it’s not a silver bullet. It should be used as part of a comprehensive risk management strategy.

Practical implementation. Machine Learning (ML) has been instrumental in threat analysis and risk management. It helps in identifying patterns in large datasets, which can be used to predict and mitigate potential threats.

For instance, Software from Microsoft showcased this skill in 2018, when cybercrooks attempted to infect over 400,000 users with a cryptocurrency miner during a 12-hour time frame. The attack was stopped by Microsoft’s Windows Defender, a software that employs multiple layers of machine learning to identify and block perceived threats. The crypto miners were shut down almost as soon as they started digging [3].

For instance, in the banking industry, ML is used to improve decision-making, tailor services, and enhance risk management [4].

For instance, ML algorithms can analyze network traffic to detect anomalies that may indicate a cyberattack. In financial risk management, ML can predict market trends and help in making informed investment decisions. Moreover, ML can be used in healthcare to predict disease outbreaks, aiding in proactive response. These practical implementations demonstrate the successful use of ML in managing risks and threats.

Challenges and limitations. Ethically, the misuse of ML can lead to privacy breaches and discriminatory practices. Legally, it's crucial to ensure that ML applications comply with data protection laws. From an implementation perspective, ML models can be complex and require significant computational resources [5-6]. They also need high-quality, relevant data for training, which can be difficult to obtain. Furthermore, ML models can be vulnerable to attacks and may lack transparency and explainability. Despite these challenges, ML holds great potential for enhancing threat analysis and risk management when used responsibly and ethically.

Future uses of machine learning. ML is poised to transform the landscape of threat analysis and risk management in the coming years. Its potential lies in its capacity to expedite the identification of cyber threats, enhance the precision of risk predictions, and establish automated response protocols. Beyond cybersecurity, ML holds promise in predictive modeling for financial risk management, aiding in the recognition of emerging market trends and potential risks.

Nevertheless, the realization of these advancements hinges on overcoming obstacles such as safeguarding data privacy, ensuring model transparency, and addressing the demand for skilled professionals in the domain. Despite grappling with these challenges, the trajectory of ML in the realm of risk management remains optimistic.

Conclusions

For security assessment and risk management, machine learning (ML) has become a game-changer due to its amazing potential for proactive threat identification, risk prediction, and reaction automation. Because of its capacity to find patterns in enormous datasets, organizations are better equipped to reduce risks and make wise decisions by early detection of possible threats and weaknesses.

But machine learning isn't a panacea. Its deployment must be done responsibly, ethical issues relating to confidentiality of information and potential bias must be addressed, regulatory compliance must be guaranteed, and funds must be allocated to developing the required infrastructure and knowledge. Even with these obstacles, machine learning (ML) has a bright future in risk mitigation. It has the ability to completely transform the way we detect, anticipate, and counteract threats in a wide range of fields, notably cybersecurity, finance, and healthcare.

REFERENCES

1. What Is Machine Learning? A Beginner's Guide? URL: https://www.scribbr.com/ai-tools/machine-learning/ (дата звернення: 20.12.2023)
2. Machine Learning and AI for Risk Management. URL: https://link.springer.com/chapter/10.1007/978-3-030-02330-0_3 (дата звернення: 20.12.2023)
3. Machine Learning in Cybersecurity: How It Works and Companies to Know. URL: https://builtin.com/artificial-intelligence/machine-learning-cybersecurity (дата звернення: 20.12.2023)
4. Derisking machine learning and artificial intelligence. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/derisking-machine-learning-and-artificial-intelligence (дата звернення: 20.12.2023)
5. Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. URL: https://www.mdpi.com/1996-1073/13/10/2509 (дата звернення: 20.12.2023)
6. Ethical considerations in the use of Machine Learning for research and statistics. URL: https://uksa.statisticsauthority.gov.uk/publication/ethical-considerations-in-the-use-of-machine-learning-for-research-and-statistics/ (дата звернення: 20.12.2023)

Березюк Максим Віталійович – студент групи УБ-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: berezukmaksim045@gmail.com

Андрощук Катерина Миколаївна – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, e-mail: katja111andros4uk@gmail.com

Berezuk Maksym Vitaliyovych – student of the UB-22b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email:berezukmaksim045@gmail.com

Androshchuk Kateryna Mykolaivna – Lecture, Chair of Foreign Languages, Vinnytsia National Technical University, Vinnytsia, e-mail: katja111andros4uk@gmail.com