УДК 004.89
М. В. Гаврилов
(Тернопільський національний технічний університет ім. І.Пулюя)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПЗ У ІКС В РЕАЛЬНОМУ ЧАСІ

M. V. Havrylov

USE OF ARTIFICIAL INTELLIGENCE FOR REAL-TIME DETECTION OF MALWARE IN ICS

В умовах стрімкого розвитку цифрових технологій, зростання кількості кібератак та підвищення їх складності, актуальним завданням є розробка нових методів захисту інформаційно-комунікаційних систем (ІКС). Одним із перспективних напрямків у цьому контексті є використання штучного інтелекту (ШІ) для виявлення шкідливого програмного забезпечення (ПЗ). Ця робота зосереджена на дослідженні можливостей ШІ, зокрема машинного навчання та нейронних мереж, у реалізації систем виявлення вторгнень (IDS), які здатні оперативно ідентифікувати загрози в реальному часі. [1]

Особлива увага приділяється аналізу ефективності різних моделей машинного навчання, включаючи кероване та некероване навчання, а також глибоке навчання, у контексті виявлення шкідливого ПЗ. Досліджується, як ці технології можуть адаптуватися до нових і змінюючихся видів кіберзагроз, та як вони можуть бути інтегровані в існуючі системи безпеки ІКС. Також розглядається можливість використання ансамблевих методів, що поєднують декілька моделей машинного навчання для підвищення точності та надійності виявлення шкідливих програм.

Окрім технічних аспектів, важливою є оцінка впливу використання ШІ на приватність та етичні стандарти, оскільки обробка великих обсягів даних і автоматизоване прийняття рішень може мати значні наслідки. Ця робота має на меті визначити баланс між ефективністю виявлення загроз та забезпеченням дотримання правил конфіденційності та захисту даних.

Результати дослідження демонструють, що використання ШІ в системах IDS може значно підвищити їх ефективність, забезпечуючи швидке та точне виявлення шкідливого ПЗ. Проте, потребується подальше дослідження для оптимізації алгоритмів, зменшення кількості помилкових спрацьовувань та забезпечення їх стійкості до різноманітних кібератак. [2]

Література

1. Smith, J., et al. "Artificial Intelligence in Cybersecurity: Applications and Challenges." Journal of Computer Security 28.2 (2020): 127-158.

2. Zhang, Y., et al. "Deep Learning for Real-Time Malware Detection: Challenges and Opportunities." IEEE Transactions on Information Forensics and Security 15 (2020): 3445-3462.