CNN ТА ЇХ ВИКОРИСТАННЯ ДЛЯ КЛАСИФІКАЦІЇ MALWARE

Федюшин О.І., Хижняк К.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Зловмисне програмне забезпечення – це широка категорія програмного забезпечення, яка включає віруси, трояни, програми-вимагачі та інші malware, призначені для нанесення шкоди або проникнення в комп'ютерні системи [1]. Його динамічний характер, який виражається незліченною кількістю нових варіантів, що з'являються щодня, створює серйозну проблему для традиційних антивірусних систем і систем виявлення вторгнень.

Протистояння між професіоналами з кібербезпеки та авторами шкідливих програм призводить до безперервної еволюції методів їх виявлення. Одним із багатообіцяючих підходів, який набув популярності в останні роки, є використання глибокого навчання, зокрема згорткових нейронних мереж (CNN), для класифікації та ідентифікації штамів шкідливих програм [2]. CNN, як тип глибокої нейронної мережі, були особливо успішними в розпізнаванні зображень. Фундаментальна ідея CNN полягає в тому, що вони можуть автоматично вивчати та отримувати релевантні функції з вихідних даних. Дослідники визнали потенціал застосування цих концепцій до проблеми класифікації шкідливих програм.

Критичним кроком у класифікації шкідливих програм є виділення ознак. На відміну від традиційних графічних даних або тексту, зловмисне програмне забезпечення часто представляється у вигляді двійкових файлів [3]. CNN можуть навчитися представляти ці двійкові файли як послідовності даних і витягувати значущі шаблони та ознаки для класифікації.

Метою доповіді є дослідження моделей нейронних мереж та отримання результатів щодо їх ефективності у ролі класифікатора шкідливого програмного забезпечення на основі таких метрик, як precision, recall, F1-Score та інші [4]. В доповіді також надається аналіз результатів роботи навчаних з нуля моделей.

Список літератури

1. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. (2017). Аналіз сучасних методів атак на електронні ресурси органів управління. *Системи озброєння і військова техніка*, (1), 65-68.

2. Makandar, Aziz, and Anita Patrot. "Overview of malware analysis and detection." International Journal of Computer Applications 975 (2015): 8887.

3. Федюшин О. І., Хижняк К. М. Використання методів глибокого навчання для візуалізації та виявлення malware / Матеріали Тринадцятої міжнародної науково-технічної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», м. Харків, 26-27 квітня 2023р. – С. 84.

4. Anandhi, V., Vinod, P., Menon, V.G. et al. Performance evaluation of deep neural network on malware detection: visual feature approach. Cluster Comput 25, 4601–4615 (2022).