ВИКОРИСТАННЯ МЕТОДІВ ГЛИБОКОГО НАВЧАННЯ ДЛЯ ВІЗУАЛІЗАЦІЇ ТА ВИЯВЛЕННЯ MALWARE

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

В останні роки атаки за допомогою зловмисного програмного забезпечення стали серйозною загрозою безпеці та продовжують завдавати величезних збитків бізнесу. Через швидке зростання кількості варіантів шкідливих програм, їх миттєва й точна класифікація має вирішальне значення для кібербезпеки.

Оскільки традиційні методи, засновані на машинному навчанні, обмежені в швидкості обробки величезної кількісті зловмисного програмного забезпечення, класифікація зловмисного програмного забезпечення на основі зображень [1] - візуалізації вихідного коду malware - та глибокого навчання може стати ефективним рішенням цього завдання.

Згорточні нейронні мережі швидко стали найсучаснішими фреймворками для різноманітних додатків, які використовуються в класифікації зображень [2, 3]. На відміну від більш традиційних методів машинного навчання, класифікатори глибокого навчання навчаються за допомогою вивчення характеристик, а не за допомогою алгоритмів для конкретних завдань. Це означає, що машина вивчатиме шаблони в зображеннях, які їй представлені, замість того, щоб вимагати від людини-оператора визначати шаблони, які машина повинна шукати на зображенні.

Тож методи глибокого навчання можуть застосовуватися до згенерованих зображень, щоб класифікувати їх як зловмисне або ж безпечне програмне забезпечення.

Метою доповіді є дослідження методів глибокого навчання та отримання результатів щодо їх ефективності при виявленні шкідливого програмного забезпечення у вигляді метрик. В доповіді також надається аналіз результатів роботи отриманих моделей.

Список літератури

1. G. Sun and Q. Qian, “Deep Learning and Visualization for Identifying Malware Families,” IEEE Trans. Dependable Secur. Comput., vol. 18, no. 1, pp. 283–295, 2021, doi: 10.1109/TDSC.2018.2884928.

2. A. Patil and M. Rane, “Convolutional Neural Networks: An Overview and Its Applications in Pattern Recognition,” Smart Innov. Syst. Tech-nol., vol. 195, pp. 21–30, 2021, doi: 10.1007/978-981-15-7078-0_3.

3. Федюшин О. І., Хижняк К. М. Методи виявлення та блокування Ransomware загроз / Матеріали Дванадцятої міжнародної науково-технічної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», м. Харків, 27-28 квітня 2022р. – С. 152.