УДК 004.8, 519.7

О.О. ЛЕТИЧЕВСЬКИЙ
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *oleksandr.letychevskyi@litsoft.com.ua*.

КОГНІТИВНІ МЕРЕЖІ, ЇХНІ ВЛАСТИВОСТІ ТА ЗАСТОСУВАННЯ У СИСТЕМАХ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАКАМ

Анотація. Розглянуто методи виявлення кібератак у реальному часі, що ґрунтуються на алгебраїчному підході. Застосовано метод алгебраїчного зіставлення, в основу якого покладено методи розв'язання поведінкових рівнянь та алгебраїчного моделювання. Водночас для підвищення ефективності виявлення та запобігання запропоновано використовувати композицію нейронної мережі для класифікації атак та методу алгебраїчного зіставлення. Цю конструкцію називають когнітивною мережею, поняття якої вперше було сформульовано у 2005 р. Розглянуто такі властивості когнітивної мережі, як подвійна класифікація та самонавчання. Представлено технологічну лінію для виявлення кібератак з використанням когнітивних мереж.

Ключові слова: штучний інтелект, нейронна мережа, глибоке машинне навчання, алгебра поведінок, нейросимвольний підхід, алгебраїчне моделювання, інсерційне моделювання.

ВСТУП. ПРОБЛЕМИ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ У ВИЯВЛЕННІ КІБЕРАТАК

Методи штучного інтелекту сьогодні досить активно застосовують у різних предметних галузях. Зокрема технологію нейронних мереж використовують у таких задачах класифікації, як розпізнання образів, розуміння мови, у галузі кібербезпеки, медицини та у багатьох інших. Із моделями класифікації співіснують і так звані генеративні мережі, що створюють такі об'єкти, як зображення, мовні конструкції тощо, згідно з навчанням нейронної мережі. Зокрема, в галузі кібербезпеки генеративні системи використовують для створення наборів даних з певними властивостями, на яких навчають нейронну мережу.

Застосування технології штучного інтелекту для виявлення у реальному часі атак на мережеве або комп'ютерне середовище є однією із нагальних задач кібербезпеки, з якою пов'язані численні розробки, як інженерні, так і наукові. Задача полягає як у виявленні ознак вторгнення, так і в нейтралізації атаки у межах комп'ютерних ресурсів. Для захисту від цих зловмисних дій аналізують як дані протоколів інтернету, так і поведінку системи, та у разі виявлення активують захисні дії для запобігання атаці.

У сучасній індустрії кібербезпеки використовують системи виявлення вторгнень, які є удосконаленням попередніх функцій захисту, як-от: мережеві екрани, віртуальні приватні мережі та інші засоби. Для швидкого виявлення атаки застосовують нейронні мережі глибокого навчання DNN (Deep Neuron Networks), які можуть класифікувати поведінку мережевого протоколу під час вторгнення як ненормальну. Більш розвинені нейронні мережі визначають тип атаки відповідно до її класифікаційної моделі.

Нейронні мережі будують шляхом навчання на певних наборах даних, зібраних під час спостереження за поведінкою мережевих протоколів. Щоб у найпростіший і найшвидший спосіб виявити атаки в режимі реального часу, потрібно детектувати аномальну поведінку, яка не відповідає звичайним діям протоколу. Але водночас можуть виникнути помилкові виявлення, оскільки відхилення від нормальної поведінки можуть бути спричинені не тільки вторгненням у систему, а й неправильним використанням ресурсів, помилками користувача або програмами, що працюють у середовищі. З іншого боку, досить важко