Секція 1

ЗАСТОСУВАННЯ АЛГОРИТМІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Луханін Б. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Землянко Г.А.

Актуальність. В останні роки йде зростання потреби на мережеві системи. Програмне забезпечення стає більш складним, що призвело до ускладнення виявлення помилок та вразливих місць. Зловмисники стають все більш витонченими. Через це системи потребують більш ефективного захисту. Механізми виявлення вторгнень повинні мати більш якісні алгоритми аналізу даних для того, щоб покращити свою результативність. Тож чи є алгоритм, що здатний відповідати всім потребам.

Метою даної роботи є: розглянути алгоритми інтелектуального аналізу даних та зробити висновки щодо проблематики їх використання.

Основні положення.

Зробимо порівняльний аналіз переваг та недоліків 4 алгоритмів інтелектуального аналізу даних у системах виявлення вторгнення. Це метод опорних векторів, метод k-найближчих сусідів, дерево прийняття рішень та нейронна мережа.

1. Метод опорних векторів (SupportVectorMachine, SVM) — набір подібних алгоритмів навчання з учителем, застосовуваних у задачах класифікації та регресійного аналізу.Як переваги SVM можна відзначити здатність до узагальнення, високу точність і низьку обчислювальну складність прийняття рішення. Недоліком методу є відносно велика обчислювальна складність побудови моделі, що класифікує [2].

2. Метод k-найближчих сусідів (k-nearestneighbors, k-NN) — метричний алгоритм автоматичної класифікації об'єктів чи регресії. Об'єкт, що класифікується, відноситься до того класу, якому належать найближчі до нього об'єкти навчальної вибірки [3]. Метод k-NN є одним із найпростіших методів ІАД. Результати застосування методу легко піддаються інтерпретації. Недолік методу – його чутливість до локальної структури даних [2].

3. Дерево прийняття рішень - засіб підтримки прийняття рішень, що використовується в статистиці та аналіз даних для прогнозних моделей [4].Перевагами дерев прийняття рішень є простий принцип їх побудови та хороша інтерпретованість результатів, недоліком – невисока точність класифікації [2].

4. Нейронна мережа (або штучна нейронна мережа) — математична модель, а також її програмне або апаратне втілення, побудована за принципом організації та функціонування біологічних нейронних мереж — мереж нервових клітин живого організму. Нейронні мережі не програмуються у звичному значенні цього слова, вони навчаються. Навчання мережі відбувається шляхом коригування значень ваги нейронів для мінімізації помилки класифікації [5]. Переваги нейронних мереж виражаються в їх здатності автоматично набувати знань під час навчання, а також здатності до узагальнення, основний недолік полягає у чутливості до шуму у вхідних даних [2]. Отже високу точність мають лише нейронні мережі та метод опорних векторів, який також має високу масштабованість разом із деревом прийняття рішень. Окрім високої масштабованості, вони також мають високу трудомісткість. У той же час метод k-найближчих сусідів має дуже низьку масштабованість, нейтральну трудомісткість та дуже низьку швидкість. А метод опорних векторів та дерево прийняття рішень мають високу швидкість та високу популярність

Висновки. Після порівняння їх переваг та недоліків стає зрозуміло, що кожен алгоритм має свої сильні та слабкі сторони. Але жоден з них немає можливості вирішити весь спектр задач, які потребує інтелектуальний аналіз даних.

Список літератури

1. Nefedov A. SupportVectorMachines: A SimpleTutorial. *Svmtutorial*. URL: https://svmtutorial.online/ (дата звернення: 27.10.2021);
2. Шарабыров И. В. Система обнаружения атак в локальных беспроводных вычислительных сетях на основе технологий интеллектуального анализа данных : дис. канд. тех. наук. Уфа, 2016. 144 с;
3. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning: guide book. Springer, 2001, 745 p;
4. Microsoft DecisionTreesAlgorithm. *Microsoft.* URL: https://docs.microsoft.com/en-us/sql/analysis-services/data-mining/micro-soft-decision-trees-algorithm (дата звернення: 12.11.2021)
5. Philip D. Wasserman Neural Computing: Theory and Practice: guide book. Van Nostrand Reinhold, 1989, 230 p.

Відомості про авторів

Луханін Богдан Юрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 096-875-81-12, b.lukhanin@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@khai.edu