Пулеко І. В., к.т.н., доц.,
доцент кафедри комп'ютерної інженерії та кібербезпеки
Погребніченко П. К., магістрант, гр. КБм-22-1,
Державний університет «Житомирська політехніка»

ОЦІНКА ЯКОСТІ ВИЯВЛЕННЯ КІБЕРАТАК РОЗРОБЛЕНИМ ПРОГРАМНИМ ДОДАТКОМ ДЕТЕКТОРУ АТАК НА ОСНОВІ PYTHON ТА KDD DATASET

Результатом більшості задач машинного навчання є метрики, котрі використовуються для розуміння точності роботи, прогнозування та в цілому поведінки машини. Ці метрики можуть бути різними для різних типів задач, проте у всіх є обов'язковий набір показників, котрі й відображають усю ефективність роботи машини. Серед цих метрик існують такі:

Точність (Accuracy). Під точністю класифікації ми, зазвичай, маємо на увазі термін відношення кількості правильних прогнозів до загальної кількості вхідних вибірок

Влучність (Precision). Влучність має на меті відповідати на питання «Яка кількість позитивних відповідей є дійсно коректною?»

Влучність допомагає, коли існує велика вартість хибно-позитивних результатів.

Наприклад, проблема пов'язана з несправним біометричним валідатором. Коли у моделі низька влучність, то багатьом буде дозволено доступ, хоча так бути не повинно, і такий результат буде мати багато помилкових рішень. Це може призвести до великих втрат та несанкціонованого доступу до різного класу приміщень.

Повнота (Recall). Повнота ж відповідає на питання «Яка кількість позитивних відповідей була коректно визначена?».

Дана метрика буде у нагоді, коли існує велика кількість хибно-негативних результатів. Наприклад, якщо потрібно розпізнати надходячу ракету, хибно-негативний результат призведе до руйнівних наслідків. Коли в моделі велика кількість хибно-негативних результатів – це головне, чого треба позбутись.

F1 Оцінка (F1 Score). Оцінка F1 – це загальна величина двох попередніх показників: влучності та повноти.

Хороший результат Оцінки F1 означає, що у моделі низький рівень помилково-позитивних та помилково-негативних рішень, тобто, вона правильно визначає реальні загрози та не сповіщає за хибними.

Матриця неточностей. Матриця порівнює фактичні цільові значення із передбаченими моделлю машин-ного навчання.

Це дає цілісне уявлення про те, наскільки добре працює модель класифікації і яких помилок вона допускає.

AUC-ROC крива. ROC (Reciever Operator Characteristic) крива є метрикою оцінки для задач бінарної класифікації. Це крива ймовірностей, котра співставляє істино-позитивні відповіді з хибно-позитивними на різних порогових значеннях, та відокремлює «сигнал» від «шуму».

AUC (Area Under the Curve) – це міра здатності класифікатора розрізняти класи, вона використовується як підсумок до кривої ROC.

Ентропія (Entropy). Ентропія визначається як випадковість або міра безладу в наборі інформації, що обробляє машина. Іншими словами, ентропія – це показник машинного навчання, який вимірює непередбачуваність або сторонні додатки у системі.

Список використаних джерел

1. Archna Oberoi. Back to Basics: 5 Crucial Components of Machine Learning, 2020. URL: https://insights.daffodilsw.com/blog/back-to-basics-5-crucial-components-of-machine-learning
2. Amanda Iglesias Moreno. Data normalization with Pandas and Scikit-Learn, 2020. URL: https://towardsdatascience.com/data-normalization-with-pandas-and-scikit-learn-7c1cc6ed6475
3. Samarth Agrawal. Understanding the Confusion Matrix from Scikit learn, 2021. URL: https://towardsdatascience.com/understanding-the-confusion-matrix-from-scikit-learn-c51d88929c79
4. Andrew Long. Understanding Data Science Classification Metrics in Scikit-Learn in Python, 2018. URL: https://towardsdatascience.com/understanding-data-science-classification-metrics-in-scikit-learn-in-python-3bc336865019

Evaluation Metrics With Python Codes, 2022. URL: https://www.analyticsvidhya.com/blog/2022/01/evaluation-metrics-with-python-codes/