Пулеко І. В., канд. тех. наук, доцент,
доцент кафедри КІ та КБ,
Свінцицька О. М., канд. екон. наук, доцент кафедри КН
Державний університет «Житомирська політехніка»,
Поліщук Ю. Я., аспірант
Національний авіаційний університет

ЗГОРТКОВИЙ ПІДХІД ДО ОЦІНКИ ЯКОСТІ АЛГОРИТМІВ КЛАСИФІКАЦІЇ МАШИННОГО НАВЧАННЯ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ

Серед методів машинного навчання, що застосовуються в задачах кібербезпеки, на сьогоднішній день найбільшої популярності набули методи класифікації які відносяться до контрольованого типу навчання або навчання з учителем (supervised learning). Завдання класифікації – це завдання, в якому множину об'єктів (ситуацій), необхідно розділити на класи, причому існують і розмічені дані з визначеними класами на яких алгоритм класифікації навчається. Досить часто в задачах кібербезпеки вирішується і обернена задача – пошук аномалій.

Алгоритми, що вирішують завдання класифікації відомі досить давно і у математичній статистиці їх також називають завданнями дискримінантного аналізу. Тому на сьогодні відома достатньо велика кількість алгоритмів класифікації, наприклад «наївного» Баєса, дерево рішень, k-найближчих сусідів, метод опорних векторів (SVM), логістична регресія та інші. Також існує і велика кількість модифікацій класичних алгоритмів. Різноманітність пропозицій алгоритмів класифікації породжує проблему вибору. Який з алгоритмів краще обрати для виконання того чи іншого завдання? Відповідь на це питання далеко не однозначна, адже існуючі метрики для оцінки якості класифікації не надають однозначного результату. Особливо складно здійснити такий вибір початківцям.

Основні метрики для порівняння алгоритмів базуються на матриці помилок класифікації. Це матриця, яка візуалізує кількість фактичних екземплярів класу в порівнянні з прогнозованими екземплярами класу. Таке подання дозволяє швидко побачити кількість правильних і неправильних прогнозів для кожної категорії. Неважко помітити, що з позиції кібербезпеки, ці помилки нерівноцінні по зв'язаних з ними наслідками. У разі "помилкової тривоги" втрати складуть тільки марно потрачений час та ресурси на протидію неіснуючій загрозі. У разі "пропуску цілі" можна втратити набагато більше (інформацію, роботу мережі та інше, це залежить від виду атаки). Тому системі захисту важливіше не допустити "пропуск цілі", ніж "помилкову тривогу". Оскільки з точки зору логіки завдання виявлення аномалій нам важливіше правильно розпізнати аномалію (атаку) з міткою y = 1, ніж помилитися в розпізнаванні нормальної роботи мережі, будемо називати відповідний результат класифікації позитивним (аномалія чи атака виявлені вірно), а протилежний - негативним (аномалії чи атаки немає y = 0). Тоді можливі наступні чотири результати класифікації: True Positive (TP) – наявність атаки класифікована як наявна атака, тобто позитивний клас розпізнано як позитивний; True Negative (TN) – нормальна робота мережі класифікована як нормальна робота без аномалій, тобто негативний клас розпізнано як негативний; False Positive (FP) – нормальна робота мережі класифікована як аномальна, тобто мала місце помилка, в результаті якої негативний клас був розпізнаний як позитивний (помилка I роду); False Negative (FN) – атака чи аномальна робота мережі розпізнана як нормальна, тобто мала місце помилка, в результаті якої позитивний клас був розпізнаний як негативний (помилка II роду).

На основі матриці помилок, розглядаються і інші показники: акуратність (англ. accuracy) - пропорція точних прогнозів по відношенню до загальної кількості прогнозів; точність (англ. Precision) - частка правильних відповідей моделі в межах класу; повнота (англ. recall) - це частка істинно позитивних класифікацій; F-міра (англ. F-score), що є гармонійним середнім між точністю і повнотою; ROC-крива, що показує частку хибно позитивних прикладів в порівнянні з часткою істинно позитивних прикладів, та інші.

Щоб полегшити нефахівцю правильність вибору алгоритму, авторами запропоновано застосувати згортання відповідних критеріїв за нелінійною схемою компромісів професора Вороніна А.М.

Переваги методу нелінійної схеми компромісів полягають у тому, що, по-перше, даний метод є досить простим по обчислювальних витратах і при цьому дозволяє одержати розв'язання з множини Парето з урахуванням обмежень за принципом "якомога далі від обмежень". По-друге, скалярна згортка при опуклості частинних критеріїв має властивість унімодальності. Також нелінійна схема компромісів має властивість безупинної адаптації до різних ситуацій, у яких потрібно прийняти багатокритеріальний розв'язок. У напружених ситуаціях (коли один або декілька частинних критеріїв знаходяться в небезпечній близькості від обмежень) вона діє еквівалентно мінімаксній моделі, у досить спокійних ситуаціях згортка діє еквівалентно моделі інтегральної оптимальності. У проміжку між обома полюсами нелінійна згортка дає різні ступені вирівнювання частинних критеріїв.