УДК 004.056.5:005.311.6

ОПТИМІЗАЦІЯ ПРОЦЕСУ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ РИЗИКАМИ КІБЕРБЕЗПЕКИ

Фролов Д.І.
e-mail: denys.frolov@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім.В.В. Поповського
м. Харків, Україна

The Security Operations Center provides round-the-clock protection against attacks, necessitating the automation of malware detection and classification. The use of deep learning models allows for high accuracy in solving such tasks. Budget constraints in the SOC affect its decisions regarding the choice of tools. Using an algorithm for solving a quasi-linear constrained optimization problem helps find the necessary balance, which is an important step in the process of automating cybersecurity risk management.

Вплив негативних факторів на управління ризиками кібербезпеки може бути зменшений за допомогою технологій штучного інтелекту (ШІ) [1]. Протягом останніх років відбувається активна інтеграція технологій ШІ з кібербезпекою. Вектор досліджень у галузі штучного інтелекту спрямований, в тому числі, на розробку методів формалізації, узагальнення, класифікації, представлення знань, а також, на розробку алгоритмів для навчання інтелектуальних систем [2].

Операційний центр безпеки (ОЦБ) є першою лінією захисту, забезпечуючи цілодобовий моніторинг, виявлення та реагування на атаки. Ефективне розпізнавання та класифікація шкідливого програмного забезпечення (ШПЗ) є важливим завданням для аналітиків та обумовлює потребу в автоматизації. Бінарна візуалізація, що є підходом до оцінювання та класифікації ШПЗ як його зображень у відтінках сірого, робить можливим використання нейромережевих архітектур комп'ютерного зору та моделей глибинного навчання (як складової ШІ) в рамках цієї задачі [3]. Разом з цим, існує велика кількість моделей, які забезпечують точність розпізнавання та класифікації зловмисного програмного забезпечення на рівні 90% та вище, що робить їх потенційно придатними для використання в реальному середовищі.

Хмарні сервіси вже є обов'язковою складовою інфраструктури багатьох компаній. В зв'язку з цим, розгортання обраних аналітиком ОЦБ моделей (їх тренування та перетренування) в робочому середовищі та на реальних наборах даних вимагають врахування вартості використання задіяних хмарних сервісів.

Одним з ключових факторів, що впливають на роботу ОЦБ та його зрілість є наявні обмеження бюджету (в тому числі, на дослідження та впровадження інструментів безпеки). Зазначений контекст формує потребу

в пошуку оптимального рішення, враховуючи не тільки критерії ефективності моделей (наприклад, за такими метриками, як точність та кількість епох), але й вартість потрібних обчислювальних можливостей в хмарі. Такі обмеження ускладнюють пошук оптимального рішення щодо остаточного вибору моделі для її подальшого впровадження в реальному середовищі з боку аналітика ОЦБ.

Система підтримки прийняття рішень, побудована з використанням алгоритмів оптимізації, повинна максимально спростити процес прийняття найбільш оптимального рішення в умовах наявних обмежень [4].

Для вирішення зазначеного питання багатокритеріальної оптимізації вибору доцільним методом є використання алгоритму розв'язання квазілінійної оптимізаційної задачі з обмеженнями [5] (де сідлова точка буде відображати оптимальний баланс між точністю, часом навчання та вартістю ресурсів). Аналіз квазілінійної оптимізаційної задачі показав, що допустима область розв'язків формується сідловими поверхнями та площинами, а цільова функція має властивості неперервності, диференційованості та монотонності. Максимальні або мінімальні значення цільової функції знаходяться на межі цієї області, що дозволяє використовувати метод симплексів для ефективного розв'язання задачі. Використання s-1-вимірної сідлової поверхні (рисунок 1) у задачах багатокритеріальної оптимізації є доцільним для аналізу та прийняття рішень щодо вибору моделі машинного навчання з урахуванням критеріїв ефективності такої моделі, пов’язаних витрат на хмарні обчислювальні ресурси на основних платформах (AWS, GCP, Azure), а також, обмеженого бюджету.

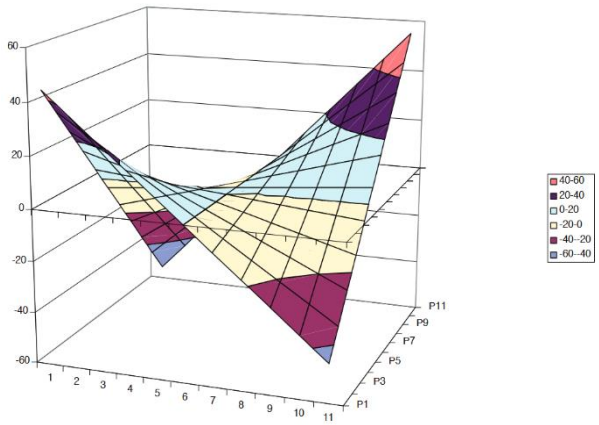

Рисунок 1 – s-1-вимірна сідлова поверхня [5]

Зазначений підхід до оптимізації процесу прийняття рішень (та обґрунтовування раціональності підсумкового рішення) щодо визначення найбільш оптимальної моделі машинного навчання для розпізнавання та класифікації ШПЗ може бути також адаптований до визначення найбільш

ефективного інструментарію ОЦБ для автоматизації управління ризиками кібербезпеки, в умовах обмеженості ресурсів.

Список використаних джерел:

1. Teliukov S., Frolov D., Dubniak M., Manzhai O., Haidarzhy A. Fundamentals of applying technology to support intelligence in decision-making systems // Revista Gestao & Tecnologia-Journal of Management and Technology. 2024. Т. 24, № 5. DOI: 10.20397/2177-6652/2024.V24I5.3119

2. Frolov D., Radziewicz W., Saienko V., Kuchuk N., Mozhaiev M., Gnusov Y., Onishchenko Y. Theoretical and technological aspects of intelligent systems: problems of artificial intelligence // International Journal of Computer Science and Network Security. 2021. Т. 21, № 5. С. 6. DOI: 10.22937/IJCSNS. 2021.21.5.6

3. Nataraj L., Karthikeyan S., Jacob G., Manjunath B.S. Malware images: Visualization and automatic classification // Proceedings of the 8th International Symposium on Visualization for Cyber Security. 2011. Стаття 4. ACM. DOI: 10.1145/2016904.2016908

4. Smyrnova I., Mazur O., Skliarenko I., Hannoshyna I., Fedorov D., Frolov D. Analysis of the navigation coordinate systems that I use will solve the problem of finding a unique route // International Journal of Computer Science and Network Security. 2022. Т. 22, № 4. С. 53. DOI: 10.22937/IJCSNS.2022.22.4.53

5. Arutiunian I., Dankevych N., Arutiunian Y., Saikov D., Poltavets M., Maranov A., Frolov D. Development of a mathematical model for selection and rationale for making optimal construction decisions // Advances in Mathematics: Scientific Journal. 2020. DOI: 10.37418/amsj.9.12.50