Фещенко Д.І., магістрант,
Науковий керівник – Сугоняк І.І., к.т.н., доц.,
Житомирський державний технологічний університет

ВИКОРИСТАННЯ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ РОЗПІЗНАВАННЯ РЕКЛАМИ

Забезпечення інформаційної безпеки, до якої відноситься фільтрація спаму та розпізнавання рекламних повідомлень досить часто є складним та вимогливим до ресурсів.

Є велика різниця між тим, як аналізує контент людина і машина. Людина використовує для аналізу власний досвід, знання про різноманітні рекламні та інформаційні ресурси, може робити певні висновки та навчатися в процесі роботи. Людське мислення не слідує єдиному шаблону, не зводиться до простого статистичного аналізу та не опирається на припущення.

На даний момент було проведено вже багато досліджень в галузі аналізу текстового контенту, зокрема, доведено ефективність використання теореми Байєса.

Нехай $H_1, H_2, \ldots$ - повна група подій, а A – деяка подія з позитивною ймовірністю. Тоді, умовна ймовірність того, що мала місце подія H_k, враховуючи, що в результаті експерименту спостерігалась подія A можна вирахувати за формулою

$$P(H_k\ A\ = \frac{P(H_k)\times P(A|H_k)}{\sum_{i=1}^{\infty} P(H_i)\times P(A|H_i)}$$

При цьому, даний алгоритм працює лише з текстовою інформацією, що унеможливлює його застосування для аналізу різноманітних зображень, рукописних текстів, тощо. Також, оскільки даний метод базується на припущенні, що одні слова частіше зустрічаються в спамі, а інші – в звичайних повідомленнях, то він стає неефективним, якщо дане припущення не виконується.

За допомогою методу Баєсовського отруєння можна додати багато надлишкового тексту в повідомлення, яке в наслідку цього не буде якісно проаналізоване та відфільтроване.

Метод використання нейронних мереж для фільтрації спаму базується на тому, щоб наділити машину відповідними рисами, які в деякій мірі присутні людському мисленню, зокрема, це здатність навчатися та аналізувати контекст, використовувати певну систему переваг та виключень, які використовуються під час прийняття рішення. Це дозволить автоматизувати рутинні операції, звільнити людські ресурси та підвищити якість роботи систем для забезпечення інформаційної безпеки. Розроблена нейронна мережа повинна не лише видаляти всю рекламу та спам контент, а також мати можливість залишати певну корисну інформацію виходячи з контексту повідомлення.

Мережа повинна аналізувати контент за різними ознаками, починаючи з кількості слів, що викликають підозру на спам в повідомленні, а також включаючи аналіз контексту повідомлення – аналіз орфографії та морфології тексту, семантичні ознаки, визначати загальну тематику повідомлення, тощо.

Даний метод є схожим на фільтрацію за допомогою класифікатора Баєса, але замість ваг слів використовуються відповідні зв’язки між нейронами мережі, що можуть змінюватися в процесі навчання мережі та підвищувати якість розпізнавання нового контенту.

Варто зауважити, що наявність орфографічних та синтаксичних помилок в повідомленнях можуть значно зменшити ефективність роботи та якість отриманого результату. Тому, дані помилки потрібно попередньо знайти та виправити.

Для того, щоб розпізнавати повідомлення з динамічно сформованими рекламними або спам зображеннями, можна використати методи OCR – оптичного розпізнавання символів. Дані методи дозволяють виділити та розпізнати текст на зображенні, після чого він може бути проаналізований за допомогою інших методів фільтрації спаму. На даний момент оптичне розпізнавання символів ще розвивається. Зараз поширені інтелектуальні методи для розпізнаванні символів, що можуть розпізнавати не лише друковані літери, а й в певній мірі рукописні друковані символи, тощо.

Нажаль, розпізнавання рукописних не друкованих символів є не вирішеною задачею, досягти високої точності для звичайного рукописного тексту досі не вдалося. Можна зменшити ефективність алгоритму використовуючи методи для додавання шумів та спотворення зображення. Також, можна додати складну анімацію, на перших кадрах якої не буде відповідного тексту, що також дозволить успішно пройти перевірку.

Все це відкриває можливості для дослідження та застосування нових прогресивних методів для вирішення такої класичної задачі як фільтрація та розпізнавання спаму. Використовуючи такі новітні розробки, як глибинні нейронні мережі, оптичне розпізнавання символів, аналіз зображень, анімацій та відео контенту за допомогою певних сигнатур, тощо, можна значно поліпшити роботу класичних алгоритмів.