УДК 004.056.52

П'ятак Р. О.
Войтович О. П.

Система пошуку та аналізу небезпечного контенту інформаційних ресурсів

Анотація

Робота присвячена покращенню методів та засобів пошуку та аналізу небезпечного контенту на інформаційних ресурсах різних систем

Ключові слова: *небезпечний контент, інформаційні ресурси, система, веб-додаток, пошук, аналіз.*

Abstract

The work is devoted to the improvement of methods and tools for searching and analyzing dangerous content on the information resources of various systems.

Keywords: *dangerous content, information resources, system, web application, search, analysis*.

Вступ

В сучасному цифровому світі, насиченому інформацією, проблема небезпечного контенту на інтернет-ресурсах стає все більш актуальною та загостреною. Швидкий розвиток технологій та широкий доступ до мережі створюють потребу в ефективних системах пошуку та аналізу небезпечного контенту.

Цифрова епоха, в яку ми ввійшли, несе із собою не тільки безмежні можливості доступу до інформації, але й виклики, пов'язані з поширенням небезпечного контенту в інтернеті [1]. Небажані вмістові елементи, такі як фейкові новини, образливий контент чи шкідливі дезінформації, заклики до тероризму, шкідливе програмне забезпечення, стають все більшими загрозами громадській безпеці та стабільності. В цьому контексті актуальною стає проблема розробки систем, які не лише виявляють такий контент, але й забезпечують аналіз його впливу та поширення серед користувачів [2].

Задача розробки системи пошуку та аналізу небезпечного контенту інформаційних ресурсів ставить перед собою важливі завдання в контексті сучасного інтернет-простору. Спроби забезпечити безпеку користувачів та визначити ступінь небезпеки інформаційного вмісту на різних платформах вимагають новаторських підходів та технологій[3].

Проект спрямований на створення інтегрованої системи, яка здатна виявляти різноманітний небезпечний контент, враховуючи його різні форми та вирази, а також реагувати на нові тенденції у сфері кібербезпеки. Використання методів штучного інтелекту та машинного навчання має допомогти у покращенні точності виявлення та класифікації небезпечного контенту, а також у вивченні їхнього впливу на користувачів та суспільство.

Результати дослідження

Для реалізації програмного застосунку потрібно розглянути два методи його реалізації та вибрати саме той, який буде найбільш ефективним.

Перший метод реалізації такого застосунку, є створення веб-сайту, методів та функції аналізу постів/зображень. Створення таблиці систематизації інформації для її класифікації на наявність ознак небезпечного контенту.

Система може працювати в двох режимах :

- Перевірка конкретного джерела – користувач відправляє посилання на сайт, що потребує перевірки на вміст небезпечного контенту, система перевіряє сайт за посиланням та користувач отримує повідомлення з коротким звітом аналізу.
- Онлайн моніторинг – користувач вмикає функцію моніторингу і система онлайн перевіряє сайти та посилання, які відвідує користувач. У випадку виявлення небезпечного контенту система його аналізує та сигналізує про це користувача.

Крім того, система працює з базою даних та записує весь проаналізований небезпечний контент.

Серед переваг даного метода є кросплатформеність, тому що веб-сайт, який виступає графічним інтерфейсом системи може бути відкритим у будь-якому браузері на будь-якій операційній системі.

До недоліків можна віднести те, що потрібен постійно працюючий сервер для бази даних, а також для роботи веб-сайту.

Другий метод полягає у створенні веб-розширення для браузера Google Chrome з аналогічним першому методу вмістом методів та функцій для пошуку та аналізу небезпечного контенту, з подальшим завантаженням в магазин розширень[4].

Серед переваг даного метода є його легкість в реалізації, оскільки відпадає потреба у створені GUI-інтерфейсу та серверу для клієнтської частини системи.

Із недоліків можна віднести те, що отримати доступ до системи можна лише через браузер Google Chrome.

Аналіз показав, що для реалізації програмного застосунку було б доцільніше використовувати перший метод.

Структура запропонованого засобу показана на рис.1

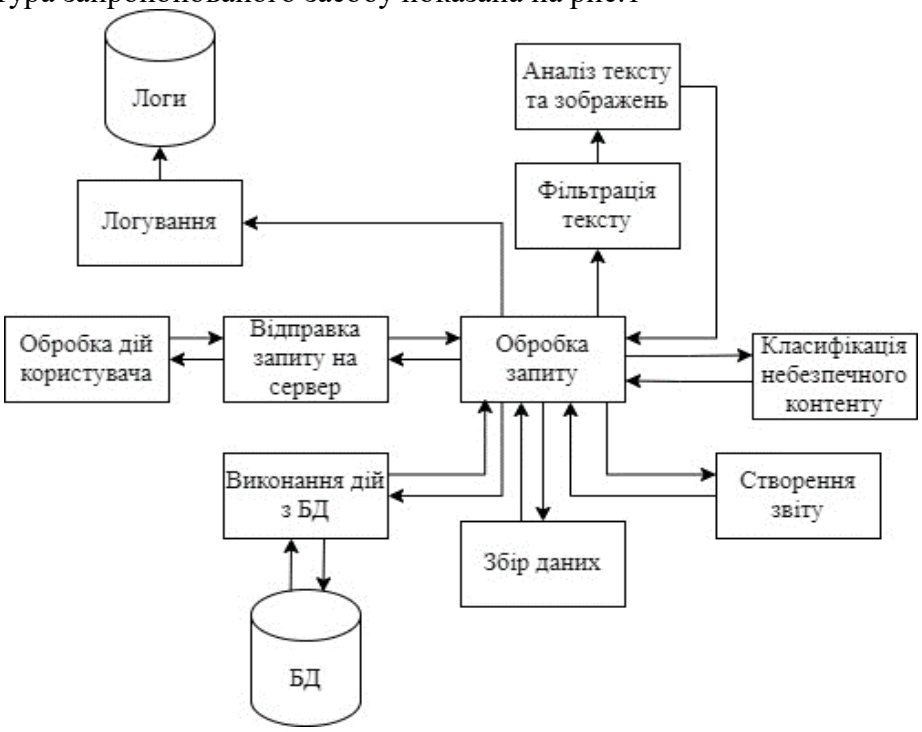

Рисунок 1 – Структурна схема засобу для аналізу телеграм-каналів

Система складається з таких модулів: модуль взаємодії з користувачем; модуль збору даних; модуль фільтрації; модуль аналізу тексту та зображень; модуль класифікації; модуль звітування .

Висновки

Описано причини виробництва та розповсюдження інформаційних вкидів, поняття інформаційних вкидів та інформаційних війн, оцінено переваги використання телеграм-каналів для поширення інформаційних вкидів в інтернеті. Проведено аналіз методів, які можна застосувати для вирішення задачі, оцінено їх переваги та недоліки та обрано оптимальний.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Щіпак Д. и др. Протидії маніпулятивному впливу інформаційних фейків у соціальних мережах. – 2021. С. 23-27.

2. Захарченко А. П. Кількісне оцінювання потенціалу впливу пошукової видачі Google на репутацію публічної особи //Вісник Харківського національного університету імені ВН Каразіна. Серія «Соціальні комунікації». – 2018. – №. 14. – С. 54-60.

3. Молодецька-Гринчук К. В. Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками //Радіоелектроніка, інформатика, управління. – 2017. – №. 2. – С. 117-126..

4.Qin Z. et al. Bootstrapping recommendations at chrome web store //Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. – 2021. – С. 3483-3491.

П'ятак Руслан Олегович - студент Кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: 20012006ruslan@gmail.com

Войтович Олеся Петрівна - к.т.н., доцент, професор кафедри захисту інформації. Вінницький національний технічний університет, м. Вінниця, email: voytovych.op@gmail.com.

Piatak Bohdan Olegovich - student of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: 20012006ruslan@gmail.com

Voytovych Olesya Petrivna - Ph.D., Associate professor of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: voytovych.op@gmail.com