Cyber defense challenge 2025

Кафедра кибербезопасность и криптология

Задание 2: Разработка моделей для выявления киберэкстремизма в социальных сетях и мессенджерах

Описание задачи:

С развитием интернета и социальных медиа экстремистские группы находят новые способы пропаганды и рекрутинга. Это включает в себя использование веб-сайтов, форумов, чатов, социальных сетей и стриминговых платформ для распространения радикальной пропаганды. Модели машинного обучения могут помочь выявлять и блокировать подобный контент, и они могут быстро адаптироваться к изменяющимся условиям и обнаруживать новые формы экстремистского контента. Выявление экстремистского контента и предотвращение его распространения в сети способствует защите пользователей от индоктринирования и рекрутинга в экстремистские группы. Это особенно важно для предотвращения радикализации молодежи и защиты уязвимых групп.

Цель: Разработка новых моделей для выявления киберэкстремизма в социальных сетях и мессенджерах

Поставленные задачи:

1. Разработка мультиклассификационных моделей на основе машинного обучения, определяющих *идеологическую направленность* (пропаганда, вербовка, радикализация) экстремистского содержания в аудио-и видеопубликах социальных сетей и мессенджеров

Ожидаемый результат: Модель мультиклассификации на основе машинного обучения, определяющая идеологическую направленность экстремистского содержания в аудио-видео публикациях социальных сетей и мессенджеров

2. Разработка модели мультиклассификации на основе машинного обучения, определяющей экстремистское (*религиозный экстремизм, политический экстремизм, ксенофобия*) содержание в текстовых, аудио, видео публикациях социальных сетей и мессенджеров.

Ожидаемый результат: Модель мультиклассификации на основе машинного обучения, определяющая экстремистское (религиозный экстремизм, политический экстремизм, ксенофобия) содержание в текстовых, аудио, видео публикациях социальных сетей и мессенджеров

3. Разработка гибридной модели обнаружения наиболее активных киберпропаганд в социальных сетях и мессенджерах

Ожидаемый результат: Гибридная модель обнаружения наиболее активных киберпропаганд в социальных сетях и мессенджерах.

4. Разработка программного обеспечения, реализующего разработанные методы и модели.

Ожидаемый результат: Программное обеспечение для внедрения моделей, методов и алгоритмов, разработанных в рамках сайбер дефенса. Тестирование и отладка программы для обеспечения ее корректной работы и соответствия требованиям.

Формат решения:

Программное обеспечение с анализом различных показателей.

Требования к участникам:

Навыки программирования на выбранном языке (предпочтительно Go, Python, Java, Scala или любой другой язык, обучаемый в университетах).

Понимание процесса классификации текстовых, аудио, видео сообщений в социальных сетях и мессенджерах и ключевых компетенций в IT индустрии.

Готовность к совместной работе в команде и выполнению задач в рамках Cyber defense challenge. В данном задании вы можете выбрать одну из задачи 1-3 как основу. Демонстрация нескольких задач также приветствуется.

Желаем удачи в разработке!

По всем вопросам обращаться: Bolatbek.milana@gmail.com