УДК 004.896

ПОДХОД К СОЗДАНИЮ ПРОГРАММНОГО КОМПЛЕКСА ОБНАРУЖЕНИЯ И РЕАЛИЗАЦИИ ПРОТИВОДЕЙСТВИЯ СООБЩЕНИЯМ В СЕТИ, ДИСКРЕДИТИРУЮЩИМ РОССИЙСКУЮ ФЕДЕРАЦИЮ

Баев В.В. (ВКА)**, Ткаченко С.Ф.** (ВКА)**, Дудкин А.С.** (ВКА)
Научный руководитель – кандидат технических наук, доцент Дудкин А.С.
(Военно-космическая академия имени А.Ф.Можайского)

Введение. В современных условиях информационного противостояния особую значимость приобретает вопрос нейтрализации пропагандистских атак, целенаправленно дискредитирующих Российскую Федерацию, ее политический курс, деятельность Министерства обороны и значимость проведения специальной военной операции. Данные кампании, координируемые структурами так называемой «пятой колонны» и враждебно настроенными агентами украинского режима и государств НАТО, преследуют цель искажения общественного сознания и манипуляции мнением граждан. Основным каналом распространения дезинформации чаще всего становятся известные цифровые платформы и социальные сети.

Источники антигосударственной пропаганды в инфотелекоммуникационной сети «Интернет» становятся все более разнообразными и труднодоступными для отслеживания [1]. Данные ресурсы часто меняют адреса и названия, иногда маскируясь под сайты с неполитической тематикой, что в свою очередь затрудняет их обнаружение и мониторинг. Ситуация осложняется тем, что распространение антигосударственных материалов достигло масштабов, при которых негативный контент создается автоматически и распространяется в форме «спама» [2]. Зачастую источником таких публикаций выступают не настоящие пользователи, а автоматизированные бот-сети, искусственно генерирующие активность в цифровом пространстве [3]. Подобная технология маскировки создаёт серьёзные препятствия для выявления конкретных организаторов и первоисточников деструктивного контента, скрывая следы их происхождения за анонимностью алгоритмических инструментов.

На этой основе, с целью противостояния дезинформации предлагается применение программного комплекса, осуществляющего поиск дискредитирующего контента в различных социальных сетях и мессенджерах, его анализ и генерацию аргументированной критики, что в свою очередь позволит оперативно выявлять и нейтрализовать враждебные информационные атаки, формировать контраргументы и доносить их до целевой аудитории, создавая пространство для объективного обсуждения и защиты национальных интересов в информационном поле [4].

Основная часть. Исследование посвящено разработке программного комплекса, состоящего из стека современных технологий, отобранных в соответствии с актуальными стандартами, соответствующими требованиям 2025 года. Разрабатываемое решение обязано предусматривать:

– интуитивно понятный интерфейс, который позволит оператору грамотно управлять и анализировать полученную информацию;

– сенсоры, позволяющие добывать информацию из сети;

– интеллектуальный решатель, способный определять степень негатива, направленного в сторону Российской Федерации;

– генератор, формирующий текст в качестве аргументов с противоположным мнением.

Концепция предполагает создание системы из нескольких взаимосвязанных программных компонентов, которые реализованы в виде микросервисов с дальнейшим разделением на две группы сервисов, где первая группа, назовем ее «добывающей», будет включать в себя независимые сервисы, каждый из которых будет отвечать за получение данных из одной конкретной целевой социальной сети, мессенджера или видеохостинга. В

свою очередь, вторая группа сервисов будет предоставлять услуги обработки полученных данных при помощи некоторого набора нейронных сетей, каждая из которых будет максимально эффективно выполнять поставленную перед ней задачу, будь то определение антироссийской позиции автора некоторого сообщения или генерация ответа, опровергающего антироссийский тезис, основанный на фальсифицированных фактах.

Выводы. Реализация предложенной концепции, основанной на модульном подходе к решению различных задач, позволяет разработать единый программный комплекс, целью которого будет оперативное реагирование на дискредитирующий контент с последующим решением взаимосвязанных задач в автоматизированном режиме.

Список использованных источников:

1. Смирнов Д.А. Маскировка деструктивного контента в сети Интернет // Современные технологии в киберпространстве. – 2023. – № 2. – С. 19-24.

2. Романов П.В. Автоматизированное распространение фейковой информации // Журнал цифровых коммуникаций. – 2022. – № 5. – С. 77-82.

3. Захаров Л.М. Бот-сети как инструмент манипуляции общественным мнением // Вестник кибербезопасности. – 2022. – № 3. – С. 88-94.

4. Воронов А.Н. Технологии противодействия кибератакам. – Екатеринбург: Уральский университет, 2023. – 198 с.

Баев В.В. (автор) Подпись

Ткаченко С.Ф. (автор) Подпись

Дудкин А.С. (автор) Подпись