УДК 004.8:004.056

ВЫЯВЛЕНИЕ И ПРОГНОЗИРОВАНИЕ АКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ БОТ-СЕТЕЙ, РАСПРОСТРАНЯЮЩИХ ДЕСТРУКТИВНЫЙ КОНТЕНТ

Ратушняк И.А. (ВКА), **Дубников В. А.**, (ВКА), **Гудков А.С.** (ВКА)
Научный руководитель – кандидат технических наук, преподаватель Тельбух В. В.
(Военно-космическая академия имени А.Ф.Можайского)

Введение. Современные социальные сети стали не только платформой для общения и обмена информацией, но и ареной для распространения деструктивного контента, манипуляции общественным мнением и дезинформации. Одним из ключевых инструментов, используемых для этих целей, являются автоматизированные бот-сети — группы аккаунтов, управляемых программным обеспечением и имитирующих поведение реальных пользователей. Активность таких бот-сетей представляет серьёзную угрозу для информационной безопасности, социальной стабильности и доверия к цифровым платформам [5].

В условиях повышенной активности в социальных сетях, особенно во время политических кампаний, кризисов или масштабных событий, проблема идентификации и нейтрализации бот-сетей становится особенно актуальной. Традиционные методы анализа, основанные на статических правилах и простых эвристиках, уже не справляются с усложнением алгоритмов поведения ботов, которые активно адаптируются к новым условиям и используют передовые технологии для маскировки своей деятельности.

Целью данной работы является разработка программного модуля, способного выявлять и прогнозировать активность бот-сетей на основе анализа их поведения с использованием технологий искусственного интеллекта и машинного обучения. Научная новизна проекта заключается в применении современных методов, таких как обработка естественного языка (NLP) и анализ сетевой активности, для повышения точности идентификации ботов и прогнозирования их действий.

Основная часть. Для выявления автоматизированных бот-сетей в социальных сетях предлагается использовать алгоритмы машинного обучения, которые анализируют поведение пользователей на основе ряда ключевых признаков. Эти признаки позволяют отличать ботов от реальных пользователей и выявлять подозрительную активность. Основными характеристиками, используемыми для анализа, являются:

1. Частота публикаций — боты часто публикуют контент с неестественно высокой частотой, что отличает их от реальных пользователей, которые проявляют более умеренную активность.
2. Нормальная длина сообщения — сообщения ботов могут быть либо слишком короткими, либо шаблонно длинными, что отличается от разнообразия в длине сообщений реальных пользователей.
3. Процент дубликатов — боты часто используют повторяющийся контент, что выражается в высоком проценте дубликатов в их публикациях.
4. Нейтральность — тексты ботов часто имеют нейтральную эмоциональную окраску, что связано с их задачей массового распространения контента без выраженной личной позиции.
5. Процент знаков препинания — боты могут использовать знаки препинания либо слишком часто, либо слишком редко, что отличает их от реальных пользователей, которые придерживаются более естественных паттернов.
6. Распределение сообщений — боты часто публикуют сообщения в определенные временные промежутки, что создает неестественное распределение активности.
7. Однообразные темы — боты обычно сосредоточены на одной или нескольких темах, что приводит к отсутствию разнообразия в их публикациях.

8. Активность в выходные дни — боты могут проявлять активность в выходные дни, когда реальные пользователи менее активны, что является подозрительным признаком.
9. Нерегулярные интервалы между публикациями — боты могут публиковать контент с нерегулярными интервалами, что отличает их от реальных пользователей, которые чаще придерживаются более предсказуемого графика.
10. Количество активных дней — боты часто проявляют активность в течение короткого периода времени, после чего их аккаунты становятся неактивными, что является еще одним признаком автоматизированной активности.

Для анализа этих признаков используются алгоритмы машинного обучения, такие как случайные леса и градиентный буст [1,4]. Эти методы позволяют эффективно обрабатывать многомерные данные и выявлять сложные паттерны поведения, характерные для ботов. Модель обучается на данных, содержащих примеры активности как реальных пользователей, так и ботов, что позволяет ей классифицировать аккаунты с высокой точностью.

Ретроспективный анализ данных за предыдущие периоды помогает выявить тенденции в поведении бот-сетей и спрогнозировать их активность в будущем [2,3]. Например, анализ данных за 2023–2024 годы показал, что боты активно адаптируют свои стратегии, что требует постоянного обновления моделей машинного обучения и учета новых признаков.

Выводы. Разработанный программный модуль демонстрирует высокую эффективность в выявлении и прогнозировании активности автоматизированных бот-сетей, распространяющих деструктивный контент. Использование современных методов машинного обучения, обработки естественного языка и анализа сетевой активности позволяет оперативно идентифицировать ботов и минимизировать количество ложных срабатываний [1,3,4].

Результаты работы имеют важное практическое значение для обеспечения информационной безопасности и защиты социальных сетей от манипуляций. В дальнейшем планируется улучшение алгоритмов для повышения точности прогнозирования и адаптации к новым методам работы бот-сетей. Предложенный подход может быть интегрирован в системы мониторинга и использован для предотвращения распространения деструктивного контента в режиме реального времени.

Список использованных источников:

1. Иванов А. А., Петров Б. Б. Машинное обучение в задачах анализа социальных сетей. — М.: Издательство «Наука», 2022. — 320 с.
2. Сидоров В. В. Бот-сети и их влияние на информационную безопасность // Вестник информационных технологий. — 2023. — № 4. — С. 45–58.
3. Кузнецова Е. С. Применение методов обработки естественного языка для выявления ботов в социальных сетях // Искусственный интеллект и анализ данных. — 2024. — № 2. — С. 12–25.
4. Smith J., Brown R. Detecting Botnets in Social Media: A Machine Learning Approach. — Journal of Cybersecurity, 2023. — Vol. 15. — P. 78–92.
5. Григорьев Д. И. Информационная безопасность в эпоху цифровых технологий. — СПб.: Издательство «Техносфера», 2021. — 280 с.