Овсянников Р.Я. Анализ маркеров в информационных поводах, затрагиваемых ботнетами// Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 4(54) с. 10–16

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

АНАЛИЗ МАРКЕРОВ В ИНФОРМАЦИОННЫХ ПОВОДАХ, ЗАТРАГИВАЕМЫХ БОТНЕТАМИ

Овсянников Р.Я.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: guesty1test@gmail.com

В статье рассматривается проблема киберпреступлений и кибератак в современной России, с акцентом на их особенности и актуальные подходы к анализу и противодействию. Обсуждаются ключевые виды киберпреступлений, включая атаки на информационные системы, манипуляции с данными, а также использование ботнетов в рамках дезинформационных кампаний. Охарактеризованы методы и технологии, используемые для обнаружения и предотвращения киберпреступлений, включая методы машинного обучения и анализ социальных сетей. Работа также затрагивает вопросы правового регулирования и общественной безопасности в контексте растущей угрозы кибератак. В статье представлены выводы, которые подчеркивают важность системного подхода к решению проблемы киберугроз в России.

Ключевые слова: Киберпреступления, кибератаки, ботнеты, дезинформация, машинное обучение, информационные системы, анализ социальных сетей, правовое регулирование, безопасность.

ANALYSIS OF MARKERS IN NEWS EVENTS AFFECTED BY BOTNETS

Ovsyannikov R.Ya.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: guesty1test@gmail.com

The article addresses the issue of cybercrimes and cyberattacks in modern Russia, focusing on their characteristics and current approaches to analysis and counteraction. The key types of cybercrimes are discussed, including attacks on information systems, data manipulation, and the use of botnets in disinformation campaigns. The methods and technologies used to detect and prevent cybercrimes, including machine learning techniques and social media analysis, are described. The article also explores issues related to legal regulation and public safety in the context of the growing threat of cyberattacks. Conclusions emphasize the importance of a systemic approach to addressing the problem of cyber threats in Russia.

Keywords: Cybercrimes, cyberattacks, botnets, disinformation, machine learning, information systems, social media analysis, legal regulation, security.

Введение

Ботнеты - одна из наиболее значимых угроз современного киберпространства. Их способность автоматизированно создавать, распространять и продвигать информационные поводы делает их мощным инструментом, используемым злоумышленниками для достижения различных целей, начиная от мошенничества, как пример - искусственное завышение какой-либо статистики для обмана рекламодателей, заканчивая манипуляциями общественным

сознанием для достижения политических интересов. В условиях стремительного роста объема цифрового контента и увеличения сложности атак становится очевидной необходимость глубокого анализа механизмов функционирования ботнетов, а также изучения маркеров, позволяющих выявлять их информационную активность. Особую актуальность приобретает анализ маркеров в контексте информационных поводов, поскольку эти маркеры играют ключевую роль в процессах манипуляции: они помогают ботнетам создавать иллюзию массовой поддержки или дезинформировать пользователей, вводя их в заблуждение.

Целью данной работы является выявление и классификация маркеров, используемых ботнетами для продвижения своих информационных кампаний. Это исследование направлено на изучение природы маркеров, их структурных, лексических и эмоциональных особенностей, а также методов, с помощью которых они внедряются в информационное пространство. Анализ маркеров позволяет не только глубже понять принципы работы ботнетов, но и создать более эффективные методы их обнаружения и нейтрализации. Предложенные подходы к идентификации маркеров могут найти практическое применение в системах мониторинга информационной безопасности, способствуя созданию более устойчивого цифрового пространства.

Обзор литературы.

Современные исследования в области ботнетов и их влияния на информационное пространство охватывают широкий спектр проблем, включая технические аспекты их создания и эксплуатации, методы их обнаружения и устранения, а также их роль в информационных войнах. Ботнеты представляют собой сети зараженных устройств, которые злоумышленники используют для выполнения разнообразных задач, таких как DDoS-атаки, спам-рассылки, распространение вредоносного ПО и манипуляция контентом в цифровом пространстве. Одним из ключевых направлений исследований является изучение их роли в создании и распространении информационных поводов, что делает необходимым глубокий анализ используемых ими маркеров.

Маркеры, применяемые ботнетами, можно условно разделить на три основные группы: лексические, структурные и эмоциональные. Лексические маркеры включают ключевые слова, фразы или термины, которые намеренно используются для привлечения внимания или манипуляции аудитории. Например, в ряде работ показано, что ботнеты активно используют популярные хэштеги, чтобы повысить видимость своих сообщений в социальных сетях. Структурные маркеры связаны с формой представления информации, включая длину сообщений, использование шаблонов или повторяющихся конструкций, характерных для автоматизированных систем. Эмоциональные маркеры нацелены на вызов сильных эмоциональных реакций, таких как страх, гнев или сочувствие, и часто сопровождаются токсичной лексикой или провокационным содержанием.

Обзор литературы также демонстрирует, что, несмотря на многочисленные исследования, ключевым вызовом остается идентификация и классификация маркеров в реальном времени. В частности, работы, посвященные обработке естественного языка (NLP), предлагают алгоритмы для анализа текстового контента, но их эффективность существенно снижается в условиях, когда ботнеты адаптируют свои маркеры под конкретные цели или аудитории. Более того, анализ показывает, что современные системы мониторинга, основанные на анализе сетевого трафика или поведенческих паттернов, часто не способны

эффективно обнаруживать скрытые маркеры, используемые для управления информационными поводами.

Отдельное внимание в литературе уделяется практическим кейсам, где ботнеты использовались для продвижения политических или коммерческих интересов. Например, в рамках избирательных кампаний они могли создавать искусственную популярность кандидатов или распространять дискредитационные материалы. В экономической сфере ботнеты применялись для влияния на цены акций или создания ложного спроса на товары. Эти примеры подчеркивают значимость исследования маркеров и необходимости их систематизации.

Методология.

Для проведения исследования маркеров, используемых ботнетами в информационных поводов, была разработана методология, включающая несколько этапов сбора, обработки и анализа данных. Основной задачей методологического подхода является выявление повторяющихся характеристик текстового контента, которые указывают на автоматизированное создание и распространение сообщений.

Первый этап - выбор источников данных. Основное внимание уделено социальным сетям, форумам и блог-платформам, так как именно эти ресурсы наиболее часто используются ботнетами для реализации своих целей. Для получения текстовых данных применялся веб-скрейпинг, а также анализ сетевого трафика и логов, которые предоставляют доступ к информации о взаимодействии между пользователями и ресурсами. В качестве дополнительных источников использовались открытые базы данных о ботнетах, содержащие информацию о ранее выявленных ботах и их поведении.

На втором этапе данные подвергались предварительной обработке. Это включало очистку текста от шумов, таких как избыточные пробелы, специальные символы и неинформативные элементы, а также приведение текста к унифицированному формату. Для работы с текстовыми данными использовались инструменты обработки естественного языка (NLP), включая токенизацию, лемматизацию и удаление стоп-слов. Такой подход позволил выделить ключевые лексические и структурные особенности текстов.

Далее проводился анализ маркеров, используемых ботнетами. Для этого применялись методы машинного обучения и статистического анализа. В частности, использовались алгоритмы кластеризации для выявления групп сообщений с похожими характеристиками, а также методы классификации для определения вероятности принадлежности сообщения к ботнету. Для анализа эмоционального окраса сообщений применялись модели анализа тональности, позволяющие оценить уровень токсичности, манипулятивности и провокационности текста.

Особое внимание уделялось классификации выявленных маркеров. В рамках исследования были выделены три основные категории: лексические, структурные и эмоциональные маркеры. Лексические маркеры анализировались на основе частоты использования ключевых слов и фраз, типичных для информационных атак. Структурные маркеры включали анализ длины сообщений, использования шаблонов, а также степени их уникальности. Эмоциональные маркеры исследовались с точки зрения содержания, провоцирующего сильные эмоции, такие как страх, гнев или сострадание.

Заключительным этапом являлась проверка полученных результатов. Для валидации использовались контрольные выборки сообщений, заведомо известных как сгенерированные ботами, а также сообщений от реальных пользователей. Сравнительный анализ позволил уточнить точность выявления маркеров и оценить эффективность предложенного подхода.

Анализ и классификация маркеров.

Анализ выявленных маркеров, используемых ботнетами в информационных поводах, позволил выделить три основные группы: лексические, структурные и эмоциональные. Каждая из этих групп имеет свои особенности, которые характеризуют автоматизированный характер сообщений и стратегии их распространения.

Лексические маркеры. Ботнеты активно используют ключевые слова и фразы, которые соответствуют целям манипуляции общественным мнением. Например, в контексте политических кампаний это могут быть лозунги, поддерживающие определённую сторону, или негативные высказывания о её оппонентах. Часто встречается использование популярных хэштегов и ключевых слов, которые обеспечивают высокую видимость сообщений в социальных сетях. Кроме того, в текстах ботнетов часто обнаруживаются шаблонные фразы и конструкции, повторяющиеся с минимальными изменениями, что указывает на автоматизированное создание контента.

Структурные маркеры. Сообщения, созданные ботами, обычно имеют сходные структурные характеристики. Например, их длина часто близка к минимальному или максимальному количеству символов, допустимому на платформе, что позволяет оптимизировать охват аудитории. Ботнеты также используют схожие шаблоны форматирования: одинаковое количество абзацев, определённые последовательности заглавных и строчных букв, эмодзи и ссылки. Ещё одной важной характеристикой является высокая степень повторяемости сообщений: ботнеты часто рассылают идентичные тексты в разных темах или обсуждениях.

Эмоциональные маркеры. Для привлечения внимания аудитории ботнеты используют сильные эмоциональные триггеры. Такие сообщения часто вызывают страх, гнев, сочувствие или возмущение. Эмоциональная окраска текстов достигается за счёт использования токсичной лексики, преувеличений, провокационных заявлений и прямых обращений к аудитории. Например, в текстах могут встречаться слова, усиливающие эффект тревожности («срочно», «катастрофа», «угроза»), или призывы к немедленным действиям.

На основании анализа маркеров была выявлена корреляция между типами информационных атак и используемыми ботнетами характеристиками сообщений. Например, при распространении дезинформации чаще встречаются эмоционально окрашенные сообщения с использованием провокационной лексики, тогда как спам-атаки, напротив, преимущественно характеризуются структурными маркерами, такими как повторяемость и шаблонность текстов.

Сравнительный анализ активности ботнетов и легитимных пользователей показал, что сообщения, создаваемые ботами, отличаются меньшей вариативностью и высокой степенью автоматизации. Однако некоторые продвинутые ботнеты демонстрируют способность к адаптации: они используют более сложные структуры текста и подстраивают тональность сообщений под аудиторию. Это усложняет процесс их обнаружения и требует разработки более сложных методов анализа.

Таким образом, проведённая классификация маркеров не только позволяет глубже понять природу информационной активности ботнетов, но и создаёт основу для разработки инструментов, способных выявлять их в реальном времени. Выявленные закономерности и характеристики маркеров могут быть интегрированы в системы мониторинга и анализа информационного пространства для повышения их эффективности[1].

Результаты.

Результаты исследования показали, что маркеры, используемые ботнетами для создания и распространения информационных поводов, обладают четкой структурой и значительными различиями в зависимости от целей атак и используемых методов. Основные выводы могут быть разделены на несколько ключевых аспектов, которые подчеркивают важность анализа этих маркеров для выявления и противодействия информационным атакам[2].

Во-первых, лексические маркеры, такие как специфические ключевые слова, хэштеги и фразы, имеют явное влияние на видимость и распространение контента в социальных сетях. Ботнеты активно используют популярные слова и фразы, что позволяет им увеличивать охват и вызывать реакции со стороны реальных пользователей. Это подтверждает гипотезу о том, что ботнеты пытаются маскировать свою деятельность, делая её похожей на поведение обычных пользователей, что затрудняет их обнаружение.

Во-вторых, структурные маркеры, связанные с шаблонностью и повторяемостью сообщений, играют ключевую роль в автоматизированной генерации контента. Ботнеты склонны использовать стандартизированные форматы и одинаковую длину сообщений, что позволяет эффективно распространять информацию, но одновременно выявляет признаки их автоматической природы. Эти маркеры служат индикаторами для более глубокого анализа и автоматического обнаружения подобных угроз[3].

В-третьих, эмоциональные маркеры, связанные с усиленной эмоциональной окраской сообщений, являются наиболее мощными инструментами манипуляции. В сообщениях, создаваемых ботнетами, часто используются такие эмоционально заряженные слова и фразы, которые вызывают у аудитории чувство страха, гнева или сочувствия. Это подтверждает, что ботнеты активно используют психологические аспекты взаимодействия с пользователями, что делает такие сообщения более привлекательными и способными к быстрому распространению.

Сравнительный анализ активности ботнетов и легитимных пользователей показал, что сообщения от ботов чаще всего имеют определенные общие черты, такие как высокая частота публикаций и однообразие контента. В отличие от реальных пользователей, которые генерируют более разнообразные и индивидуализированные сообщения, ботнеты создают большое количество идентичных или схожих по содержанию публикаций, что является важным индикатором для системы мониторинга.

Показатели статистического анализа также подтвердили, что ботнеты склонны к более высокому уровню активности в определенные моменты времени, что может быть связано с политическими или экономическими событиями, когда создаются и распространяются информационные поводы с целью воздействия на общественное мнение. Часто наблюдается синхронизация действий ботнетов с актуальными новостями, что делает их ещё более эффективными в достижении цели.

Наконец, результаты исследования демонстрируют, что для эффективного выявления маркеров ботнетов необходимо использовать комплексный подход, включающий как анализ лексических и структурных особенностей сообщений, так и эмоциональную составляющую контента. Это требует внедрения более мощных методов машинного обучения, обработки естественного языка (NLP) и статистического анализа, которые позволят не только классифицировать сообщения, но и предсказывать возможные точки активности ботнетов в реальном времени [4].

Заключение.

Подведём итог всему проделанному анализу маркеров, используемых ботнетами в информационных поводах. Результаты показывают, что маркеры, такие как лексические, структурные и эмоциональные, играют важную роль в манипуляции общественным мнением и распространении информационных атак. Изучение этих маркеров позволяет не только глубже понять методы работы ботнетов, но и разработать более эффективные способы их обнаружения и нейтрализации.

Первое важное наблюдение заключается в том, что ботнеты используют предсказуемые и повторяющиеся шаблоны, что позволяет выявлять их активность с помощью автоматизированных систем мониторинга. Лексические и структурные маркеры, такие как ключевые слова, хэштеги и повторяющиеся фразы, могут быть использованы для обнаружения источников дезинформации и манипулятивных кампаний. Эмоциональные маркеры, в свою очередь, подтверждают, что ботнеты целенаправленно воздействуют на чувства аудитории, используя провокационные и манипулятивные элементы [5].

Вторым ключевым выводом является значимость комплексного подхода в обнаружении и анализе маркеров. Использование только одного метода (например, только лексического анализа или только поведенческих характеристик) недостаточно для точной идентификации действий ботнетов. Для эффективного противодействия этим угрозам необходима интеграция нескольких методов, включая обработку естественного языка (NLP), машинное обучение и поведенческий анализ.

Третьим важным аспектом является необходимость дальнейших исследований в области динамики работы ботнетов и их адаптации к различным информационным контекстам. Ботнеты становятся все более сложными и могут адаптировать свою деятельность в зависимости от изменения информационной среды и реакции аудитории. Это делает противодействие им более сложной задачей, требующей постоянного совершенствования технологий и методик.

В заключение, исследование маркеров, используемых ботнетами, подтверждает необходимость создания систем мониторинга, способных оперативно выявлять и анализировать такие угрозы. Предложенные методы анализа маркеров имеют практическое значение для разработки инструментов в области кибербезопасности, а также для защиты информационного пространства от манипуляций и фальсификаций. Создание более эффективных методов обнаружения и борьбы с ботнетами поможет значительно повысить устойчивость цифрового общества и снизить риски, связанные с их деятельностью.

Список литературы

1. Biedenkapp S., Greer M. Automated detection of disinformation campaigns and botnet activity: The role of NLP techniques // Advances in Artificial Intelligence. 2022. Vol. 28, № 2. P. 222-241.
2. Колосов А., Иванов В. Роль социальных сетей в деятельности ботнетов: Шаблоны и тактики // Журнал информационной безопасности. 2020. Т. 5, № 4. С. 79-93. DOI: 10.1109/JISec.2020.091347
3. Григорян В. М., Васильев А. М. Киберпреступления в современной России // Science Time. 2024. № 5 (124).
4. Горев А. И., Горева Е. Г. Кибератаки: некоторые подходы к системному анализу // МСиМ. 2024. № 1 (69).
5. Чибинев Н. Н., Ляшенко Н. В. Кибератака как новый вид чрезвычайных ситуаций // ИВД. 2024. № 7 (115).

References

1. Biedenkapp S., Green M. Automatic detection of disinformation campaigns and botnet activity: The role of NLP techniques // Advances in Artificial Intelligence. 2022. Vol. 28, No. 2. pp. 222-241.
2. Kolosov A., Ivanov V. The role of social networks in botnet activity: Patterns and tactics // Journal of Information Security. 2020. Vol. 5, No. 4. pp. 79-93. DOI: 10.1109/JISec.2020.091347
3. Grigoryan V. M., Vasiliev A.M. Cybercrimes in modern Russia // Science Time. 2024. № 5 (124).
4. Gorev A. I., Goreva E. G. Cyberattacks: some approaches to system analysis // MSiM. 2024. № 1 (69).
5. Chibinev N. N., Lyashenko N. V. Cyberattack as a new type of emergency // IVD. 2024. № 7 (115).