УДК 004.738.5, 6

А.О. Логинова
Московский государственный лингвистический университет, Москва

АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К КЛАССИФИКАЦИИ И ТИПОЛОГИИ БОТОВ

В данной статье представлен обзор существующих подходов к классификации и типологии ботов. Распределение ботов по классам было осуществлено на основе существенных свойств ботов, описанных в литературе по релевантной теме.

Ключевые слова: боты, классификация ботов, типология ботов, информационная безопасность.

A.O. Loginova
Moscow State Linguistic University, Moscow

THE ANALYSIS OF EXISTING APPROACHES TO BOTS CLASSIFICATION AND TYPOLOGY

This article provides an overview of existing approaches to the classification and typology of bots. The division of bots into classes was based on essential specifications of bots described in the literature on the relevant topic.

Keywords: bots, bots classification, bots typology, information security.

В 2016 году обложки профессиональных изданий сообщали о скорой замене приложений ботами [1]. Несмотря на то, что данный инструмент не был новинкой – первый бот был создан в Массачусетском технологическом институте в 1966 году на основе теории машинного интеллекта А. Тьюринга (1947 года) – интерес к нему возрос из-за перспектив использования в онлайн-сервисах посредством различных интерфейсов. Предположение о грядущей замене приложений ботами не подтвердилось, но, тем не менее, боты прижились в интернет-пространстве.

В 2009 году боты были “авторами” порядка 24% всех сообщений в Twitter, по данным маркетологов около 54% рекламы в Интернете приходилось на ботов [2]. Согласно результатам исследования, опубликованным в 2019 году компанией GlobalDots, 37,9% интернет-трафика в 2018 году создавали боты [3].

В последние годы наблюдается стабильный рост числа ботов в Интернете. Социальные сети стали питательной средой для ботов, представляя широкие возможности для распространения различного рода информации или, наоборот, её сбора из открытых источников. На сегодняшний день остро стоит проблема идентификации и фильтрации ботов. В литературе по релевантной теме множество ботов часто делят на подмножества “плохих” (вредоносных) и “хороших” (полезных) [2, 3, 4]. Отсюда следует, что одна из целей менеджеров информационной безопасности – это блокировка одних и поддержание работоспособности других. Однако, используя один алгоритм работы, “плохие”

боты маскируются под “хороших”, усложняя задачу фильтрации [4]. К тому же, есть люди готовые за небольшое вознаграждение выполнять однотипные операции ботов, как те, что позволяют увеличить количество лайков под постом в Instagram, или же группы ботов, управляемые операторами-людьми. Поведение таких ботов практически невозможно отличить от поведения человека в сети [5]. В связи с этим становится актуальной задача типологии ботов, решение которой позволит блокировать нежелательных ботов.

Не только компании заинтересованы в использовании ботов для автоматизации некоторых несложных однотипных задач, например, консультация клиентов интернет-магазина о товаре в целях экономии трудозатрат и временного ресурса. Многие интернет-пользователи прибегают к услугам ботов. К примеру, с развитием монетизации в социальных сетях появился спрос на “накрутку” лайков и просмотров постов. Если опубликованный в YouTube или Instagram материал набирает большое количество просмотров, лайков, комментариев, то материал имеет все шансы попасть в рекомендуемые к просмотру. Автор поста при этом увеличивает охват своей аудитории за счёт новых подписчиков, заинтересовавшихся его профилем/каналом, таким образом, следующий пост увидит ещё большее количество пользователей социальной сети. Такой механизм распространения информации применяется в достижении различных целей: от удовлетворении желания стать известным и зарабатывать деньги за счёт своих постов с размещением рекламных продуктов до продвижения политических кампаний. Искусственное поднятие рейтинга просмотров – лишь один из вариантов применения ботов.

Существует несколько подходов к классификации ботов:

1) упомянутое выше разделение на “плохих” и “хороших”;
2) классификация по роду деятельности [6]:

a) боты, предназначенные для сбора информации (поисковые боты/web crawlers; спам-боты, собирающие контактные данные и др.);

b) боты для создания контента (боты-редакторы; спам-боты, распространяющие рекламу; боты, генерирующие отзывы; AdSense-боты (контекстная реклама) и др.);

c) боты-эмуляторы поведения человека (торговые боты; чат-боты; астротурфинг-боты; социальные боты и др.);

d) боты, выполняющие операции (боты-цензоры; боты-модераторы; боты аукционных площадок; боты высокочастотного трейдинга (алгоритмическая торговля на финансовых рынках)/биржевой бот и др.);

3) классификация по назначению:

a) боты-посредники, предназначенные для осуществления коммуникации, например, между клиентом и компанией (чат-боты; поисковые боты/web crawlers и др.);

b) функциональные боты, заменяющие работу приложений, осуществляющие подбор продукта по заданным характеристикам (боты для поиска выгодных предложений покупки авиа- и ж/д-билетов; торговые боты; новостные боты и др.);

4) разделение ботов на социальных и не относящихся к ним. Социальными ботами называют автоматизированное программное обеспечение, способное работать с реальными пользователями через интерфейсы социальных сетей. “При этом бот не является аккаунтом – это программа управления аккаунтом (хотя в сложившейся традиции ботом обычно называют именно аккаунты, управляемые ботами)” [7]. Некоторые источники дают более узкое определение социальному боту, говоря о том, что это программа, использующая социальные сети, имитирующая общение и взаимодействие людей [8]. Социальные боты в свою очередь делятся на подклассы:

a) спам-боты ;

b) технические боты, выполняющие однообразные рутинные действия («накрутка» просмотров и рейтинга и др.);

c) боевые боты, способные заблокировать аккаунт, получить доступ к персональным данным пользователя и др.;

d) боты-тролли, размещающие оскорбительные комментарии, а также посты с информацией, способствующей разжиганию ненависти и др.;

e) астротурфинг-боты используются как механизм управления общественным мнением. Астротурфинг-боты работают через посты, отзывы и комментарии, создают впечатление у читающего о том, что большое количество людей поддерживает или выступает против чего-то конкретного, искусственно формируя общественное мнение;

5) классификация по способу управления:

a) автоматические боты, не требующие контроля человека при работе;

b) управляемые боты, нуждающиеся в контроле человека-оператора;

6) классификация по формам взаимодействия с пользователем:

a) работающие посредством заложенных команд/кнопок;

b) использующие технологию распознавания речи;

c) inline-боты, не требующие запуска самого бота, при этом бот должен быть добавлен в используемые. В чате Telegram такой бот вызывается с помощью указания его имени в строке набора сообщения, например, @ya_*запрос*, так вызывается бот поисковика Yandex. Результатом его работы будет предоставление пользователю информации по заданному запросу по разным ссылкам. Пользователь может выбрать ссылку с информацией наиболее соответствующей его запросу и направить её собеседнику.

Множество ботов можно классифицировать сразу по нескольким существенным свойствам. Так, например, в статье, опубликованной по результатам исследования, проведенного специалистами из Оксфордского Института Интернета совместно со специалистами Института имени А. Тьюринга, «Even good bots fight: The case of Wikipedia» была предложена типология, основанная на пересечении классов ботов, сформированных по типу намерений (пункт 1) и роду деятельности (пункт 2) ботов [6]. Такой способ представления множества ботов в упорядоченной форме возник в результате изучения исследователями вопроса взаимодействия ботов друг с другом.

В статье «Do Social Bots Dream of Electric Sheep? A categorisation of Social Media Bot Accounts» авторы представляют перекрёстную типологию ботов, объединив классификацию по типу намерений (пункт 1) и по уровню имитации ими поведения человека [8]. Рассматривая класс социальных ботов (пункт 4), авторы пришли к выводу о том, что представители данного класса различаются по типу намерений и степени имитации человеческого поведения. Под «социальными ботами» авторы подразумевают аккаунты в социальных сетях, контролируемые ботами, такие боты в значительной мере имитируют поведение пользователей в сети: создают и рассылают сообщения, отправляют «заявки в друзья», копируют посты и делятся ими с «друзьями». Отмечается, что работа социальных ботов оказывает большое влияние на участников интернет-коммуникации.

Таким образом, в зависимости от условий задачи фильтрации, используя разные комбинации подходов к классификации ботов, можно создать адаптивную типологию ботов. Использование такой типологии позволит с наибольшей точностью идентифицировать бота.

Список литературы

1. Chatbots were the next big thing: what happened? // The startup. Build something awesome URL: https://medium.com/swlh/chatbots-were-the-next-big-thing-what-happened-5fc49dd6fa61 (дата обращения: 19.12.2020).
2. О чём хорошие боты спорят в Википедии // Хабр URL: https://habr.com/ru/post/373207/ (дата обращения: 15.12.2020).
3. Industry Report: Bad Bot Landscape 2019 // GlobalDots. We Make IT Faster URL: https://www.globaldots.com/bad-bot-report-2019#form (дата обращения: 15.12.2020).
4. Белые начинают: так ли уж хороши “хорошие” боты? // Хабр URL: https://habr.com/ru/company/variti/blog/527348/ (дата обращения: 16.12.2020).
5. Чесноков В.О. Алгоритмическое и программное обеспечение анализа графов ближайшего окружения для выявления ботов и определения неуказанных атрибутов пользователей в онлайновых социальных сетях: дис. канд. тех. наук: 05.13.11 - Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей. - М., 2018.
6. Tsvetkova M, García-Gavilanes R, Floridi L, Yasseri T (2017) Even good bots fight: The case of Wikipedia. PLoS ONE 12(2): e0171774. https://doi.org/10.1371/journal.pone.0171774
7. Василькова В.В., Легостаева Н.И. Социальные боты в политической коммуникации // Вестник РУДН. Серия: СОЦИОЛОГИЯ. - 2019. - Том 19, № 1 (2019). - С. 121-133.
8. Stieglitz, Stefan; Brachten, Florian; Ross, Björn; and Jung, Anna, "Do Social Bots Dream of Electric Sheep? A Categorisation of Social Media Bot Accounts" (2017). ACIS 2017 Proceedings. 89 https://aisel.aisnet.org/acis2017/89.

Сведения об авторах

Логинова Алина Олеговна – аспирант кафедры международной информационной безопасности Института информационных наук, эксперт отдела научного менеджмента и наукометрии, Московский государственный лингвистический университет, Москва, email: loginova@linguanet.ru

About the authors

Loginova Alina Olegovna – post-graduate student of International Information Security Department of the Information Sciences Institute, expert of the Scientific Management and Scientometrics Department, Moscow State Linguistic University, Moscow, e-mail: loginova@linguanet.ru