DOI: 10.55648/1998-6920-2024-18-3-3-13 УДК 004.5; 004.8:004.9

Описательная модель социального бота, учитывающая его потенциал нарушителя информационно-психологической безопасности *

А. О. Логинова

Московский государственный лингвистический университет (ФГБОУ ВО МГЛУ)

Аннотация: Цель настоящего исследования заключается в создании описательной модели социального бота, учитывающей его потенциал нарушителя информационно-психологической безопасности. Исследование проводилось на примере американского политического дискурса. В основу модели легли результаты комплексного анализа неразмеченного корпуса текстов постов социальных ботов в Twitter. Исследуемый корпус текстов представляет собой совокупность текстов постов на английском языке аккаунтов в социальной сети, которые ранее были определены исследователями как социальные бот-аккаунты, задействованные в предвыборной кампании кандидатов в президенты. Исследование мотивировано отсутствием исчерпывающего определения понятия «социальный бот». Разработанная модель бота формирует новый подход к раскрытию сути данного понятия. В настоящей статье социальный бот рассматривается как нарушитель информационно-психологической безопасности пользователя интернет-средств массовой коммуникации.

Ключевые слова: социальный бот, модель нарушителя, информационно-психологическая безопасность, интернет-средства массовой коммуникации, социальные сети.

Для цитирования: Логинова А. О. Описательная модель социального бота, учитывающая его потенциал нарушителя информационно-психологической безопасности // Вестник СибГУТИ. 2024. Т. 18, № 3. С. 3–13. https://doi.org/10.55648/1998-6920-2024-18-3-3-13.

Статья поступила в редакцию 22.01.2024;
переработанный вариант – 25.02.2024;
принята к публикации 27.02.2024.

1. Введение

Сегодня, когда доступ к различного рода медиаконтенту есть у всех интернет-пользователей, а их число ежегодно растет [1], практика информационного воздействия обретает совершенно иные масштабы. Методы информационного воздействия в равной мере используются как для достижения целей маркетинга, так и для ведения боевых действий, которые, как отмечают эксперты, всё чаще ведутся в киберпространстве.

Одним из современных инструментов информационного воздействия, бесспорно, является социальный бот (далее – бот, социальный бот, бот-аккаунт, автоматизированный социальный актор) [2, 3]. В литературе существует большое разнообразие определений понятия со-

* Статья подготовлена при поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (научный проект № 14/23-К).

циального бота, но они дают лишь частичное понимание того, что на самом деле скрывается за ним.

Цель настоящего исследования заключается в создании модели социального бота на примере американского политического дискурса.

В работе применяется метод описательного моделирования социального бота как нарушителя информационно-психологической безопасности пользователей интернет-средств массовой коммуникации (социальные сети, блоги, форумы и др.) (далее – интернет-СМК).

Материалом исследования послужил неразмеченный корпус текстов коротких электронных сообщений пользователей социальной сети Twitter на английском языке, собранный из веб-архива, которые были заблокированы модераторами Twitter как аккаунты социальных ботов, задействованные в предвыборной кампании кандидатов в президенты США в 2015–2016 годах.

Такой выбор материала для исследования был обусловлен рядом аргументов:

– в ходе избирательной кампании в качестве основного канала связи с электоратом впервые была использована социальная сеть [4, 5], поэтому в архиве Интернета [6] на сегодняшний день хранится достаточно большой объём текстовой информации, в частности, содержание постов главных кандидатов в президенты, которые могут быть использованы для анализа;

– доказано, что при реализации политической пропаганды использовались социальные боты [4, 7];

– коллективы исследователей, занимающиеся вопросом обнаружения социальных ботов, сформировали определения понятия «социальный бот», отличающиеся в части описания природы происхождения автоматизированного социального актора [8 – 10]. Этот факт поспособствовал формированию гипотезы о том, что социальные боты имеют не только различную природу происхождения, но и разный потенциал нарушителя информационно-психологической безопасности. До сих пор данное предположение не подвергалось проверке.

2. Используемые определения понятия «социальный бот»

Действующие нормативные правовые акты не дают определения понятия «социальный бот», вместе с тем различные исследовательские коллективы приводили свои определения [8 – 10]. В совокупности они формируют следующее представление о социальном боте в целом: это в первую очередь аккаунт в социальной сети, который управляется с помощью специального программного обеспечения и контролируется человеком. Результатом работы такого аккаунта является создание и распространение заданного контента среди участников некоторого интернет-сообщества в социальной сети.

Действия таких ботов подвергают угрозам информационно-психологическую безопасность (далее – ИПБ) реальных пользователей интернет-СМК. Отсутствие возможности у пользователя достоверно идентифицировать коммуниканта – причина реализации угроз ИПБ [11].

Результаты проведённого нами исследования текстов опубликованных сообщений, постов, ботов в социальной сети Twitter идут вразрез с содержанием устоявшегося определения в части, касающейся способа управления бот-аккаунтом и генерации текстов.

3. Систематизация наблюдений

Значения относительной частоты употребления конкретных единиц языка в исследуемых корпусах текста, авторства людей и социальных ботов, полученные в результате предшествующих этапов исследования на материале американского политического дискурса, относящегося к президентской гонке 2015 – 2016 годов в США [12], демонстрируют незначительные отличия текстовых сообщений социальных ботов (в сложившемся понимании) от сообщений людей.

При этом рассмотрение сообщений ботов в индивидуальном порядке позволяет выделить некоторые синтаксические особенности постов, опубликованных несколькими аккаунтами, определённых исследователями как социальные боты. Выявленные особенности обнаруживают несоответствие действительности устоявшихся определений понятия «социальный бот».

Так, например, при создании текстов постов, отражённых в табл. 1, использовались приёмы суггестии [13]. Данные приёмы не могли быть реализованы только лишь посредством программного обеспечения, генерирующего текстовые сообщения для социального бота, включая возможности ChatGPT, без редакторской правки человеком. Это может свидетельствовать о том, что тексты, публикуемые вышеуказанными аккаунтами, составлены человеком или группой людей, имеющими обширные знания в области социальной психологии и социальной инженерии. Отметим также, что чат-бот ChatGPT был анонсирован только в 2020 году, т.е. гораздо позже президентской гонки между Х. Клинтон и Д. Трампом.

Некоторая доля постов бот-аккаунтов, например, @Marycar08639249, @PatDollard и @u_edilberto, состоит из репостов текстов других аккаунтов, принадлежащих действительным пользователями социальной сети или также являющихся ботами.

Таблица 1. Примеры использования приёмов суггестии в сообщениях социальных ботов

№ п/п	Пример поста социального бота (сохранены авторские орфография и пунктуация)	Перевод выделенных фрагментов	Приём суггестии
1.	«*@63df8aabe784aebc5674b36a34c14dae77bfaa89e1d9bafa5a485ed32f6e2834* If Hillary becomes president I'm moving to Benghazi, that way I'll know she will leave me alone! **#Hillary4Prison** #TrumpForPresident»	#ХиллариВтюрьму	навешивание ярлыков: #Hillary4Prison
2.	«*@Marycar08639249* RT @AlwaysActions: Powerful response to obama's "insult" speech by Donald Trump supporting @USArmy @AdBell45 **#VoteTrump2016 #Trump2016** htt ...» [7]	#ГолосуйЗаТрампа2016 #Трамп2016	повтор информации
3.	«*@natespuewell* #NeverTrump **Those fake, nonsense polls are actually real, good polls, Trump's spokesman insists — Campaign of lies** `https://t.co/Mvja0PPeaH`» [7]	«Эти фальшивые, бессмысленные результаты голосований на самом деле настоящие, правильные результаты, настаивает пресс-секретарь Трампа – Кампания лжи»	утверждение
4.	«*@jeannemccarthy0 RT* @realDonaldTrump: **The best thing to die in 2016?** Political correctness.We have been set free from the intolerant left. Let's thank ` https://t.co/cO9gm7aAcZ_`» [7]	«Лучшее, за что можно умереть в 2016?»	постановка риторических вопросов
5.	*@pavegecko01* **#Hillary can't walk down the stairs by herself** `https://t.co/8DOZSwaHNm`	«Хиллари не может спуститься по лестнице самостоятельно»	создание послеобраза

Информация о репосте сообщается подписчикам любого аккаунта в Twitter посредством следующего набора символов: «RT @nickname:», где RT сообщает о том, что имеет место репост, а @nickname – указание наименования аккаунта, с которого был сделан репост, после символа «:» записан текст оригинального поста, например:

– @Marycar08639249: RT @AlwaysActions: Powerful response to Obama's "insult" speech […];
– @PatDollard: RT @DesertRiver: Oh Goody... […];
– @u_edilberto: RT @WeNeedHillary: Polls Are All Over t... […].

Однотипные операции репоста могли выполняться человеком, выполняющим простые повторяющиеся операции, или путём автоматизации работы такого аккаунта посредством программного обеспечения.

Некоторые сообщения исследуемого корпуса, опубликованные разными пользователями, идентифицированные исследователями как боты, в точности повторяют друг друга без указания информации о репосте, как если бы имело место легитимное копирование поста другого автора. Например:

– @CloudBeDelusion: Fox’s Shepard Smith Call’s Bulls*t […];
– @ProletariatStriving: Fox’s Shepard Smith Call’s Bulls*t […];
– @FillingDCSwamp: Pattern Of Hacking Preceded Attendee Of Donald Trump’s Camp […];
– @ProletariatStriving: Pattern Of Hacking Preceded Attendee Of Donald Trump’s Camp […].

Такая особенность текстов постов может свидетельствовать о том, что данные аккаунты входят в состав бот-нета, владелец которого может являться как продвинутым специалистом, способным развернуть подобный бот-нет, так и организованной группой людей, в которой каждый участник – узел бот-нета или же усилия каждого участника направлены на то, чтобы развернуть свою сеть ботов в целях достижения общей цели, например, на политической арене.

Полученные результаты позволяют сделать вывод о том, что в некоторых случаях задача обнаружения социального бота может трансформироваться в задачу обнаружения аккаунта человека, действующего как бот. В этом случае обнаружение деятельности социального бота – поиск конкретной языковой личности по особенностям создаваемого текста.

Подчеркнём, что сообщения ChatGPT, способного генерировать ответы на запросы, относящиеся к различным сферам жизни, в режиме диалога сегодня не могут быть приравнены к сообщениям людей, поскольку восприятие текста человеком в целом зависит не только от корректности грамматических конструкций и соответствия ответа заданному вопросу. Текст, созданный человеком, – результат социальной рефлексии.

В настоящее время пользователями ChatGPT обнаружена возможность чат-бота имитировать эмпатию посредством языковых конструкций при генерации текстов. Данный факт был установлен эмпирическим путём. В своих экспериментах различные пользователи ChatGPT формулировали запрос к чат-боту как к психотерапевту с указанием желаемых характеристик тона излагаемых рекомендаций, характеристик предлагаемых действий для решения проблемы, ограничений и других параметров ответов ChatGPT. Пользователи отмечали, что, несмотря на спокойный тон сообщений и проявления внимательности посредством языковых конструкций, сообщения ChatGPT в значительной мере отличались от речи психотерапевта. Сравнению подвергается именно качество диалога, а не уровень включенности в диалог и применимости получаемых рекомендаций. При общем положительном впечатлении от диалога в нём читалась цепочка: проблема – решение – проблема. Данные ботом советы были обезличены и в большинстве случаев лишены конкретики, т.е. не разрешали частной проблемы обратившегося за консультацией человека. В ответах содержалась общая информация, представляющая собой хорошо структурированную компиляцию информации по некоторому заданному вопросу. Именно отсутствие передачи личного отношения к проблеме с использованием средств языка отличало тексты ChatGPT, генерирующего тексты достаточно высокого качества, от текстов, созданных человеком.

Таким образом, предположив существование чат-бота ChatGPT в 2015 году, отметим, что даже сегодняшний уровень развития данной технологии и предоставляемые на сегодняшний день возможности противоречат предположению о том, что тексты, сгенерированные с помощью ChatGPT, могут оказывать суггестивное воздействие на человека. Это связано с тем, что манипуляционное воздействие методом суггестии характеризуется воздействием на чувства человека, которые блокируют его способность критически оценивать ситуацию. В наблюдениях пользователей ChatGPT не отмечалось ощущения полного погружения коммуниканта, в роли которого выступал ChatGPT, использующий речевую модель психотерапевта, в проблему «пациента», вместо этого прослеживалось использование шаблонов в формулировках ответов. Это не позволяло пользователям ChatGPT избавиться от ощущения общения с ботом, что доказывает несостоятельность предположение об использовании методов суггестии при генерации текстов социальных ботов только с помощью ChatGPT без коррекции текста человеком, компетентным в сфере социальной психологии, в частности социальной инженерии.

4. Формирование модели социального бота

Опираясь на данные, полученные в ходе изучения корпуса текстов постов социальных ботов в американском политическом дискурсе, построим модель социального бота по принципу модели нарушителя информационной безопасности (рис. 1).

Модель, составленная на материале текстов ботов в политическом дискурсе, отражает основные общие характеристики бот-аккаунта в социальной сети, а именно:

1. Правомочие пользования аккаунтом в социальной сети: использование украденного аккаунта в социальной сети / использование вновь созданного аккаунта.

2. Способ управления контролируемым аккаунтом: аккаунт управляется с помощью программного обеспечения (далее – ПО) / аккаунт управляется человеком.

Отметим, что аккаунт, управляемый с помощью ПО, не может быть полностью автономным (в модели установленный факт обозначен зависимостью). Это утверждение справедливо по ряду причин. ПО, позволяющее автоматизировать работу аккаунта в социальной сети, не является предустановленным, решение об использовании или об отказе в использовании любого ПО для работы аккаунта принимается его владельцем.

Человек может выполнять функции автомата, реализовывать простые однотипные действия, например, делать репосты или копировать тексты постов в нарушение авторских прав.

В описанном случае человек может являться как владельцем процесса и устанавливать цели, которые реализуются путём массовой публикации контента определённого содержания, так и являться исполнителем. Человек может быть как владельцем бот-аккаунта и управлять им единолично, так и быть частью организованной группы людей.

3. Выполняемые с помощью управляемого аккаунта действия.

В наборах выполняемых действий наблюдается градация: сложность выполняемых действий увеличивается со сложностью организации нарушителя. Так, для аккаунта, управляемого с помощью ПО, и аккаунта, управляемого человеком, но с низким потенциалом нарушителя, набор действий прост и заключается в копировании постов, копировании текстов постов других аккаунтов, генерации и публикации новых текстов постов. При этом для аккаунта, управляемого человеком или группой лиц с высоким потенциалом нарушителя, указано создание бот-нета, генерирующего посты с использованием всех доступных инструментов. Бот-нет при этом может состоять как из аккаунтов, управляемых только с помощью ПО, так и из аккаунтов, управляемых людьми, или комбинации аккаунтов разной природы.

Рис. 1. Описательная модель социального бота

4. Потенциал нарушителя ИПБ: низкий, средний, высокий, – комплексный критерий оценки нарушителя с точки зрения ресурсов, которые он может использовать для реализации цели. В качестве ресурсов, определяющих потенциал нарушителя, в данной модели были приняты: вычислительная мощность, уровень финансового обеспечения, уровень знаний в информационных технологиях, уровень знаний в социальной психологии. Такой выбор обусловлен тем, что:

– количество генерируемых постов в единицу времени, количество поддерживаемых диалогов, масштабируемость бот-нета, т.е. допустимое число управляемых аккаунтов в бот-нете, зависят от производительности контролирующей системы;

– уровень знаний информационных технологий определяет тип действий владельца аккаунта: наверстывающий или опережающий. Высокий уровень знаний позволяет своевременно внедрять доступные инструменты в работу;

– уровень финансового обеспечения является определяющим фактором для увеличения производительности: будь то закупка дополнительного оборудования для увеличения вычислительной мощности оборудования или оплата труда людей, генерирующих и публикующих тексты постов;

– успех применения социальных ботов объясняется эффективностью методов социальной инженерии. Их использование в коммуникации в социальных сетях позволяет увеличить длину пути социального графа – увеличить число действительных пользователей, подвергающихся воздействию. Уровень знаний нарушителей в области социальной психологии, в частности в социальной инженерии, во многом определяет успешность реализуемой атаки.

5. Цели, преследуемые лицом, управляющим бот-аккаунтом, или владельцем бот-аккаунта, имеют прямо пропорциональную зависимость с потенциалом нарушителя. В модели представлены индивидуальные цели, или цели исполнителей (создание положительного имиджа заказчика в интернет-СМК), локальные (увеличение клиентской базы) и глобальные цели (дискредитация оппонентов, увеличение электората).

6. Вид нарушителя для каждого уровня потенциала нарушителя ИПБ.

Набор предположений о располагаемой вычислительной мощности нарушителя информационно-психологической безопасности, уровне финансового обеспечения, его уровне знаний в области информационных технологий и в области социальной психологии, сформированный на основе наблюдений, позволил составить общую характеристику нарушителей, предположить род их деятельности.

В модели представлены примеры нарушителей, которые могут работать как поодиночке, так и в составе организованных групп. Так, примерами лиц, управляющих аккаунтами с использованием или без использования специального ПО с низким потенциалом, являются человек, выполняющий низкоквалифицированную работу, или начинающий SMM-специалист, со средним потенциалом – продвинутый SMM-специалист, с высоким потенциалом – организованные группы лиц, а именно: конкурирующий внутригосударственный политический штаб или зарубежный политический штаб. В ряд нарушителей с высоким потенциалом при необходимости можно включить представителей разведывательных организаций.

На основе приведённой модели социального бота попытаемся сформулировать новое определение понятия «социальный бот»: это аккаунт в интернет-СМК, владельцем которого может являться как физическое лицо, так и организованная группа лиц, который управляется человеком с использованием специального ПО, позволяющего автоматизировать процедуры рассылки, копирования и генерации новых текстов сообщений и (или) постов. Аккаунт может быть автономным или являться частью бот-нета. Цель использования таких аккаунтов – создание и массовое распространение контента, оказывающего информационно-психологическое воздействие на участников сообщества в некотором интернет-СМК.

5. Перспективы исследования

Учитывая сформированную модель, можно определить общий вид нарушителя ИПБ, социального бота, на обнаружение которого направлены существующие исследования. В качестве примеров рассмотрим работы российских исследователей.

В работе Менщикова А. А. [14] используется методика, основанная на построении графа пользовательского поведения: производится анализ действий пользователей и их последовательности в социальных сетях. Разработанная Менщиковым А. А. методика направлена на обнаружение веб-роботов, т.е. аккаунтов со встроенным ПО, позволяющим выполнять заданные действия. Следовательно, рассматриваемая методика подходит для обнаружения аккаунтов, управляемых с помощью специального ПО, имеющих низкий потенциал нарушителя.

Чесноковым В. О. в целях обнаружения интернет-ботов было проведено исследование социальных графов, взаимосвязей пользователей социальных сетей друг с другом с последующим выделением сообществ в социальной сети [15]. В сформированной модели представлен ряд правил, по которым должна производиться фильтрация аккаунтов в социальной сети с целью выделения среди них бот-аккаунтов. С точки зрения представленной модели социального бота методика обнаружения ботов, предложенная Чесноковым В. О., направлена на обнаружение аккаунтов как управляемых с помощью специального ПО, так и управляемых человеком. Нарушители ИПБ при этом имеют низкий и средний потенциалы.

Обнаружение социальных ботов с высоким потенциалом нарушителя, представленных аккаунтами, управляемыми людьми, может рассматриваться как последовательная работа по обнаружению единичных узлов бот-нета и установлению взаимосвязей между ними.

Попытка разработки методики выявления бот-нета предпринята коллективом исследователей в составе Васильковой В. В. и Легостаевой Н. И [16]. Методика, предложенная исследователями, включает комплекс из анализа всплесков публикационной активности пользователей социальной сети, анализа постов, профайлингов бот-аккаунтов, статистического анализа текстовых данных, анализа топологии бот-нета и других компонентов.

Исследователи полагают, что предложенные ими методики одинаково эффективны для поиска ботов любой категории, поскольку не выделяли различий среди бот-аккаунтов и не учитывали их в работе. Перспективы дальнейшего исследования проблемы мы видим в детальном изучении выделенных категорий социальных ботов.

6. Заключение

Результаты проведённого исследования корпуса текста постов аккаунтов, признанных социальными ботами, меняют сложившееся понимание социального бота. Разработанная модель социального бота на примере американского политического дискурса представляет основу для новой типологии ботов, при которой боты изучаются не только с точки зрения вида деятельности и назначения, но ещё и с точки зрения природы их существования. Выделение такого критерия оценки ботов позволит проводить направленные исследования для обнаружения конкретного типа бота.

Суть полученных результатов заключается в том, что обнаружение социального бота не должно сводиться к поиску результатов работы ПО, которое работает по некоторому алгоритму и воспроизводит заданные речевые паттерны с использованием некоторого ПО, в том числе с использованием технологии машинного обучения, к примеру, применяя для генерации текстов постов возможности ChatGPT. Необходимо комплексно подходить к задаче обнаружения социального бота, одним из этапов решения которой является определение природы социального бота и способа управления им.

Результативность известных методик обнаружения социальных ботов может быть переоценена при тестировании их работы на корпусах текстов социальных ботов, которые пред-

ставляют различные категории нарушителей. Так, например, методика, эффективная для поиска веб-ботов, может показать более низкие показатели результативности в случае, если бот-аккаунтом управляет человек.

Литература

1. Интернет в России: что говорит статистика? [Электронный ресурс]. URL: https://rskrf.ru/tips/eksperty-obyasnyayut/internet-stats/ (дата обращения: 20.11.2023).
2. *Ibtisam A. A.* Social bots' role in online political communication: Evidence from German Federal Election 2021 // MAGKS Joint Discussion Paper Series in Economics. 2023. № 09.
3. *Keller F. B., Schoch D., Stier S., Yang J. H.* Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign // Political Communication. 2020. № 37:2. P. 256–280.
4. *Ветров И.* Интернет победил телевизор. Как интернет и соцсети помогли Трампу победить Клинтон [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2016/11/09/10318019/internetvstv.shtml (дата обращения: 26.03.2022).
5. *Почепцов Г.* Новая коммуникативная среда выборов и big data [Электронный ресурс]. URL: https://ms.detector.media/mediaanalitika/post/18419/2017-02-19-novaya-kommunykatyvnaya-sreda-vyborov-y-big-data/ (дата обращения: 26.03.2022).
6. Internet Archive [Электронный ресурс]. URL: https://web.archive.org/(дата обращения: 25.02.2022).
7. 3 times bots have impacted major world events [Электронный ресурс]. URL: https://www.netacea.com/blog/3-times-bots-have-impacted-major-world-events/?amp#2016_and_2020_The_US_presidential_elections_-_Did_bots_influence_the_result (дата обращения: 26.03.2022).
8. *Василькова В. В., Легостаева Н. И.* Социальные боты в политической коммуникации // Вестник Российского университета дружбы народов. Серия: Социология. 2019. Т. 19, № 1. С. 121–133.
9. *Василькова В. В., Легостаева Н. И., Радушевский В. Б.* Тематический ландшафт бот-пространства социальной сети «Вконтакте» // Журнал социологии и социальной антропологии. 2019. Т. 22, № 4. С. 202–245.
10. *Гудков А. С.* Анализ активности бот-аккаунтов в новостных сообществах социальной сети Вконтакте // Материалы 11-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD), Москва, 1–3 октября 2018 года. Том II. С. 512–514.
11. *Ненашев С. М.* Информационно-технологическая и информационно-психологическая безопасность пользователей социальных сетей // Вопросы кибербезопасности. 2016. № 5 (18). С. 65–72.
12. *Логинова А. О.* Обнаружение интернет-бота по структурно-вероятностной модели электронного сообщения // Вестник Воронежского института МВД России. 2022. № 3. С. 105–114.
13. *Логинова А. О., Алейникова Д. В.* Выявление демаскирующих признаков социального бота на синтаксическом уровне генерируемого сообщения // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2023. № 1. С. 139–147.
14. Менщиков А. А. Методы обнаружения и противодействия автоматизированному сбору информации с веб-ресурсов: дис. … канд. тех. наук. СПб. 2019. 264 с.
15. Чесноков В. О. Алгоритмическое и программное обеспечение анализа графов ближайшего окружения для выявления ботов и определения неуказанных атрибутов пользователей в онлайновых социальных сетях: автореф. дис. … канд. М. 2018. 19 с.
16. *Василькова В. В. Легостаева Н. И.* Детектирование тематического разнообразия ботне-

тов: подходы и методика // Материалы XXV Международной конференции памяти профессора Л. Н. Когана «Культура, личность, общество в условиях пандемии и постпандемии: методология, опыт эмпирического исследования», УГПУ, 2022. С. 239–24.

Логинова Алина Олеговна
ведущий специалист по защите информации отдела информационной безопасности Департамента цифрового развития, Московский государственный лингвистический университет (ФГБОУ ВО МГЛУ, 119034, Москва, ул. Остоженка, д. 38, стр. 1), e-mail: a.loginova@linguanet.ru, ORCID ID: 0000-0002-7806-0586.

Автор прочитал и одобрил окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

The Descriptive Model of Social Bot on the Base of American Political Discourse

Alina O. Loginova

Moscow State Linguistic University (MSLU)

Abstract: The purpose of this study is to create a descriptive model of a social bot that takes into account its potential as a violator of information and psychological security. The study was made on the base of American political discourse. The model is based on the results of a comprehensive analysis of the unmarked text corpus of social bot posts on Twitter. The corpus of texts is a collection of texts of posts in English of social network accounts that were previously identified by researchers as social bot accounts involved in the president election campaign. The study is motivated by the lack of an exhaustive definition of the concept of "social bot". This bot model forms a new approach to the disclosure of the essence of this concept. In this article, a social bot is considered as a violator of the information and psychological security of the user of the Internet mass media. The article was funded by the Ministry of Digital Development of the Russian Federation according to the research project No. № 14/23-К.

Keywords: social bots, methods of detecting bots, information-psychological security, Internet mass media.

For citation: Loginova A. O. The descriptive model of Social Bot on the base of American political discourse (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 3, pp. 3-13. https://doi.org/10.55648/1998-6920-2024-18-3-3-13.

The article was submitted: 22.01.2024;
revised version: 25.02.2022;
accepted for publication 27.02.2022.

References

1. *Internet v Rossii: chto govorit statistika?* [The Internet in Russia. What are the statistics about this?], available at: https://rskrf.ru/tips/eksperty-obyasnyayut/internet-stats/ (accessed 20.11.2023).
2. Ibtisam A. A. Social bots' role in online political communication: Evidence from German Federal Election 2021. *MAGKS Joint Discussion Paper Series in Economics*, 2023, no. 09.
3. Keller F. B., Schoch D., Stier S., Yang J. H. Political Astroturfing on Twitter: How to Coordinate a Dis-

information Campaign. *Political Communication*, 2020, no. 37:2. pp. 256-280.
4. Vetrov I. *Internet pobedil televizor. Kak internet i socseti pomogli Trampu pobedit' Klinton* [The Internet has won over the TV. How the Internet and social media helped Trump defeat Clinton], available at: https://www.gazeta.ru/tech/2016/11/09/10318019/internetvstv.shtml (accessed: 26.03.2022).
5. Pochepcov G. *Novaya kommunikativnaya sreda vyborov i big data* [The new communicative environment of elections and big data], available at: https://ms.detector.media/mediaanalitika/post/18419/2017-02-19-novaya-kommunykatyvnaya-sreda-vyborov-y-big-data/ (accessed: 26.03.2022).
6. *Internet Archive*, available at: https://web.archive.org/ (accessed: 25.02.2022).
7. *3 times bots have impacted major event*s, available at: https://www.netacea.com/blog/3-times-bots-have-impacted-major-world-events/?amp#2016_and_2020_The_US_presidential_elections_-_Did_bots_influence_the_result (accessed: 26.03.2022).
8. Vasil'kova V. V., Legostaeva N. I. Social'nye boty v politicheskoj kommunikacii [Social bots in political communication]. *Vestnik Rossijskogo universiteta druzhby narodov. Seriya: Sociologiya,* 2019, vol. 19, no. 1. pp. 121-133.
9. Vasil'kova V. V., Legostaeva N. I., Radushevskij V. B Tematicheskij landshaft bot-prostranstva social'noj seti «Vkontakte» [Thematic landscape of the bot-space of the social network “Vkontakte”]. *ZHurnal sociologii i social'noj antropologii,* 2019, vol 22, no. 4. pp. 202-245.
10. Gudkov A. S. Analiz aktivnosti bot-akkauntov v novostnyh soobshchestvah social'noj seti Vkontakte [The analysis of bot-accounts activity in news communities of the Vkontakte social network]. *Materialy odinnadcatoj mezhdunarodnoj konferencii,* vol. II, 2018, pp.512-514.
11. Nenashev S. M. Informacionno-tekhnologicheskaya i informacionno-psihologicheskaya bezopasnost' pol'zovatelej social'nyh setej [Information-technical and information-psychological security of social-network users]. *Voprosy kiberbezopasnosti,* 2016, no. 5 (18), pp. 65-72.
12. Loginova A. O. Obnaruzhenie internet-bota po strukturno-veroyatnostnoj modeli elektronnogo soobshcheniya [Detecting internet bot by a structural probabilistic model of its electronic message]. *Vestnik Voronezhskogo instituta MVD Rossii*, 2022, no. 3, pp. 105-114.
13. Loginova A. O., Alejnikova D. V. Vyyavlenie demaskiruyushchih priznakov social'nogo bota na sintaksicheskom urovne generiruemogo soobshcheniya [Detecting the unmasking features of a social bot at the syntax level of a generated message]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyj analiz i informacionnye tekhnologii*, 2023, no 1, pp. 139-147.
14. Menshchikov A. A. *Metody obnaruzheniya i protivodejstviya avtomatizirovannomu sboru informacii s veb-resursov* [Methods of detecting and withstanding automated collection of information from web resources]. Ph. D. thesis. Saint Petersburg, 2019. 264 p.
15. CHesnokov V. O. *Algoritmicheskoe i programmnoe obespechenie analiza grafov blizhajshego okruzheniya dlya vyyavleniya botov i opredeleniya neukazannyh atributov pol'zovatelej v onlajnovyh social'nyh setyah* [Detecting the thematic diversity of botnets: approaches and methods]. Ph. D. thesis. Moscow, 2018. 19 p.
16. Vasil'kova V. V. Legostaeva N. I. Detektirovanie tematicheskogo raznoobraziya botnetov: podhody i metodika [Detecting the thematic diversity of botnets: approaches and methods]. *Kul'tura, lichnost', obshchestvo v usloviyah pandemii i post-pandemii: metodologiya, opyt empiricheskogo issledovaniya. Materialy XHV Mezhdunarodnoj konferencii pamyati professora L. N. Kogana*, Ekaterinburg, Ural State Pedagogical Univercity, 2022, pp. 239-24.

Alina O. Loginova

Leading specialist of the Information Security Sector of the Department of Digital Development, Moscow State Linguistic University (MSLU, 119034, Moscow, Ostozhenka street, 38, build. 1), e-mail: a.loginova@linguanet.ru, ORCID ID: 0000-0002-7806-0586.