Щербаль Сергей Стефанович
канд. полит. наук, старший преподаватель
Давиденко Дарья Евгеньевна
студентка
АНПОО «Кубанский институт профессионального образования»
г. Краснодар, Краснодарский край

ТЕХНОЛОГИЯ БОТИНГА КАК ИНСТРУМЕНТ ПОЛИТИЧЕСКОЙ КОММУНИКАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

***Аннотация**: в статье в контексте медиатизации и виртуализации публичной сферы рассматривается новый феномен политической коммуникации – социальный ботинг. Раскрывается понятие социального бота как автоматизированного алгоритма, имитирующего поведение реальных политических агентов, приводится их типология. Рассматриваются основные сферы применения политических ботов, их разновидности и функции. Выявляются особенности коммуникативных стратегий ботов в публичном пространстве как инструмента манипулирования общественным мнением. Дается обзор основных методов детектирования бот-технологий в российской и зарубежной практике.*

***Ключевые слова**: политическая коммуникация, социальные сети, политический бот, детектирование ботов, компьютерная пропаганда, манипулирование общественным мнением.*

Цифровая революция, произошедшая в конце прошлого столетия в развитых странах мира, запустила процесс конвергенции информатизации и телекоммуникации, что, в свою очередь, привело к возрастанию роли глобального информационного пространства. Эти процессы дали мощный импульс трансформации социальной архитектоники современного общества: из массового оно стало превращаться в сетевое. Возникла новая реальность, о которой еще в 1990-е годы писали голландский социолог Ян ван Дейк в работе «Сетевое общество» (*De Netwerkmaatschappij*) (1991) и его испанский коллега Мануэль Кастельс в фундаментальной монографии «Зарождение сетевого общества» (*The*

Rise of the Network Society) (1996), первая часть его трилогии «Информационная эпоха: экономика, общество и культура».

Ян ван Дейк определил сетевое общество как форму общества, все более и более организующего свои отношения в медиасетях, постепенно заменяющих или дополняющих социальные сети коммуникации, осуществляемые лицом к лицу [27].

Развивая концепцию сетевого общества М. Кастельс отмечает, что опосредованная компьютерными сетями социальная коммуникация порождает бесконечное множество виртуальных сообществ, дифференцирующихся относительно друг друга в зависимости от персональных вкусов и настроений их членов..(…) Сетевая виртуальность и социальная реальность смешиваются под воздействием постмодернистского релятивизма, порождая бесчисленное множество аттракторов, к которым тяготеет активность сетевого общества. Дискурс индивидуализации стимулирует отказ социальных субъектов от реальных контактов в пользу виртуального общения. Такова культура «реальной виртуальности», где виртуальный мир оказывается подчас более реальным, чем действительность [20].

Современная публичная политика характеризуется процессами виртуализации и медиатизации, в результате чего социально-политическая реальность для населения большинства стран становится результатом восприятия виртуальных представлений и образов, порой не имеющих ничего общего с объективной действительностью. Такая виртуальная медиатизированная социально-политическая реальность оказывается сотканной из бесконечного числа политических мифов, стереотипов, симулякров и брендов, которые можно объединить в одну группу виртуальных моделей, наполняющих коммуникационное пространство, в котором функционирует современное общество.

Современная политическая практика позволяет сформулировать аксиому: создание привлекательного *образа*, как ничто другое обеспечивает успех в борьбе за власть. *Мы живем в эпоху политики образов и образов политики.* Симуляция базовых компонент политических практик Модерна – идеологии,

реформ, организации, общественного мнения – ведет к виртуализации институтов массовой демократии – выборов, государства, партий. И эта виртуализация допускает и провоцирует превращение глобальной компьютерной сети Internet в средство/среду политической деятельности [7].

Сегодня уже можно говорить и о публичной политике в сети. Технологии сети Интернет способны изменить уровень и качество политического участия, которое способствует формированию конструктивной и дееспособной конкуренции внутри сетевого информационного пространства между различными социально-политическими акторами [15].

Особенностью функционирования современной публичной политики является повышение роли сетевых структур, в частности роли социальных сетей и блогосферы как новых акторов публичной политики. Под социальными сетями в данном случае понимается технологическая платформа, созданная в online-пространстве, служащая для вертикального и горизонтального взаимодействия пользователей [13, с. 203].

Сетевые сообщества становятся формой публичной политики, в рамках которой происходит обмен информацией между пользователями социальных сетей и блогосферы, способствующей формированию общественного мнения и принятию решений в сфере политики. Сетевые сообщества представляют собой интерактивную среду, способствующую не только формированию принципиально новых информационных возможностей для политических дискуссий и диалога, но и конструированию новых групп и контргрупп политической сетевой общественности [13, с. 207].

Социальные сети приобретают все большее значение в современном мире, и исследования, соответственно, сосредоточились на описании и анализе их структуры и динамики. Хотя эффективное влияние на результаты выборов все еще обсуждается, как и на общественное мнение по ключевым политическим темам, тем не менее нельзя отрицать, что новые средства массовой коммуникации представляют собой важный инструмент для формирования стратегии политического дискурса. По этой причине крайне важно исследовать возможные

искусственные манипуляции данными и поведением пользователей. В последние годы было выявлено вредоносное поведение, такое как использование автоматических учетных записей для усиления эффектов, таких как эхо-камеры, продвижение некоторых тенденциозных аргументов или искусственное повышение доверия пользователей [14].

Новые технологические возможности породили феномен социальных ботов – это автоматизированное программное обеспечение, связанное с платформой, через которую боты взаимодействуют с реальными пользователями [25].

В научный оборот вошел специальный термин «политический бот», под которым понимают аккаунт пользователя, оснащенный функциями или программным обеспечением для автоматизированного взаимодействия с другими учетными записями пользователей на темы, связанные с политикой [25].

Их активное применение в практике политической коммуникации дало основание ряду исследователей говорить о появлении нового феномена – компьютерной пропаганды (*Computational propaganda*) [28], цифровой пропаганды (*Digital Propaganda*) [21], киберпропаганды [26]. Несмотря на некоторые различия в интерпретации термина, речь идет об одном и том же явлении – новых формах и методах социального воздействия на сознание и поведение широких масс людей [2].

Бот совершает действия, которые должен осуществлять человек в социальной сети (отвечать, отправлять сообщения, комментировать чужие сообщения и т. д.). При этом бот не является аккаунтом – это программа управления аккаунтом (хотя в сложившейся традиции ботом обычно называют именно аккаунты, управляемые этими программами) [8, с. 253]. Такие программы создали миллионы аккаунтов пользователей, маскирующихся под реальных людей в социальных сетях Facebook, Twitter, Instagram, ВКонтакте и др. Внимание к проблеме было привлечено на фоне сообщений о влиянии ботов на выборы в Германии [19], референдум о выходе Великобритании из ЕС и обвинений в адрес России в инициировании вмешательства в выборы президента США в 2016 [18].

Многообразие ботов нашло отражение в классификациях, предложенных различными исследователями. В качестве референтной в настоящей работе мы используем типологию, предложенную Робертом Горва (*Robert Gorwa*) и Дугласом Гильбо (*Douglas Guilbeault*). Они выделяют следующие виды ботов:

− веб-роботы (краулеры и скреперы);

− чат-боты (диалоговые системы «человек-компьютер», использующие естественный язык посредством текста или речи);

− спам-боты;

− социальные боты (различные системы автоматизации, работающие на платформах социальных сетей);

− «sockpuppets» и тролли (поддельные личности, используемые для взаимодействия с обычными пользователями в социальных сетях);

− киборги и гибридные аккаунты (боты, управляемые человеком) [23].

Наиболее распространенным является разделение социальных ботов на полезных (доброкачественных) и злонамеренных (вредоносных) [22]. Такой типологический подход был предложен американским исследователем в области IT-технологий и коммуникаций Эмилио Феррара.

Доброкачественные боты генерируют контент, автоматически реагируют на сообщения, выполняют полезные услуги (новостные боты, информация о погоде, спортивные и траффик-боты и др.).

Вредоносных ботов разрабатывают для осуществления злонамеренных действий (спам, кража личных данных, распространение дезинформации и информационного шума во время политических дебатов, распространение вредоносного программного обеспечения и др.).

Классификация социальных ботов в контексте политической коммуникации основана преимущественно на параметрах их использования (цели, функции, способы), что связано с задачами стоящих за ними политических агентов. Обобщая российские и зарубежные исследования по данной тематике, можно выделить несколько основных направлений функционирования ботов в политической коммуникации. Они являются коммуникационным инструментом для:

ведения «мягких информационных войн» в рамках информационного противостояния; пропаганды проправительственной точки зрения; астротурфинга (продуцирования и поддержания искусственного общественного мнения путем наполнения информационного пространства сообщениями определенного содержания); изменения общественного мнения путем конструирования агентов влияния или ложных лидеров общественного мнения; делигитимации властных структур, поддержки оппозиционных сил и структур гражданского общества; формирования повестки дня, ведения политических дискуссий [1].

Исследования способов проведения бот-кампаний в выборах разного уровня в разных странах позволяют выделить три основные реализуемые с их помощью коммуникативные стратегии: 1) привлечение потенциальных сторонников кандидата на сторону пропагандиста; 2) конструирование позитивного политического имиджа политика; 3) деконструкция имиджа (дискредитация) политического конкурента. Тактики этих базовых стратегий разнятся в зависимости от конкретной электоральной ситуации [1].

Основной функцией ботов является массовое распространение информации для решения самых разнообразных задач. И боты-программы, и боты-люди (киборги) используются в условиях растущего доминирования технологии Веб 2.0, предполагающей интерактивность и модель коммуникации «многие – многим». Однако в последние годы все отчетливее просматривается тенденция, когда на смену традиционным СМК, где мнение формируется коммуникатором, пришли новые медиа, где столь же большое значение стала играть аудитория. И в новых условиях и механизированные боты, и киборги стали технологией, позволяющей влиять на общественное мнение не «сверху», а «снизу».

Важно подчеркнуть, что программные боты, как правило, не способны продолжительно и эффективно вести диалоговое общение: их алгоритмы стандартизированы, а потому не вызывают доверия и эмоционального включения собеседника. Ботов легко идентифицируют администраторы и пользователи сетей, поэтому в лучшем случае они способны выполнять роль «обманки» для

других ботов, например программ, которые индексируют данные в сети Интернет, а также случайных посетителей сайта.

Новым шагом в развитии технологии ботинга стало использование людей в качестве операторов коммуникации для более продуктивного выполнения функций роботов. В профессиональной среде эти человеко-боты получили название «киборгов» или «сетевиков». Далее в тексте статьи мы будем использовать эту метафору для обозначения рассматриваемых сетевых операторов. Сетевик – это поверхностный специалист, но во многих областях, быстро осваивающий любую сферу деятельности, при этом не погружающийся детально в каждую из них, способный к обучению и быстрому переформатированию. Архетипом такого сетевика является журналист [9]. Именно сетевик представляется носителем того, что в сетевых войнах называется сетевым кодом. Сетевой код – это некая мировоззренческая прадигма, с помощью которой человек может фильтровать информацию, вычленяя из её нескончаемого потока нужный ему элемент, используя только то, что необходимо ему в данный момент для реализации той или иной операции, действия. Такое явление позволило исследователям говорить о признаках специализации в политической пропаганде в условия медиатизации публичной сферы и формировании в ее поле отдельного высокотехнологичного направления – компьютерной пропаганды [2].

Публичные заявления петербургского предпринимателя (владельца ЧВК «Вагнер») Е. В. Пригожана, который на вопрос *Der Spiegel* и группы журналистов других западных изданий прямо заявил: «Я никогда не был просто финансистом «Агентства интернет-исследований». Я его придумал, я его создал, я им управлял длительное время», – высветили теневую сторону компьютерной пропаганды в России [4].

«Агентство интернет-исследований» было создано в 2013 году в Санкт-Петербурге. По сообщениям СМИ, сотрудники этой информационной структуры, более известной как «фабрика троллей», использовали фейковые аккаунты в социальных сетях для влияния на общественное мнение. С помощью массированного распространения на популярных интернет-площадках контента тен-

денциозного содержания сетевики Агентства продвигали пропагандистские месседжи, работая таким образом в интересах определенных заказчиков. В феврале 2018 года Министерство юстиции США обвинило Е.В. Пригожина и 12 сотрудников Агентства во вмешательстве в выборы президента в 2016 году и начало расследование. В том же году американский суд выдал ордер на арест предпринимателя после вынесения обвинения. В марте 2020 года суд Вашингтона закрыл дело против Е.В. Пригожина. Это было связано с тем, что его компания не работает на территории США, а значит, не понесет действенного наказания в случае обвинения [16].

В ходе информационных операций с использованием ботов их исполнители нередко реализуют сложные коммуникативные стратегии. Некоторые боты используются для повышения уровня доверия к реальным пользователям сети, которые сознательно или бессознательно публикуют контент в интересах заказчиков операции. Другие боты применяются для деконструкции имиджа целевого объекта атаки, например, для создания непрерывного потока (постинга) негативных комментариев в профилях активистов оппозиции. Нередко боты просто генерируют информационный шум с целью хаотизации дискурса в медиапространстве.

Самые эффективные сети ботов, манипулирующие дискуссиями в социальных сетях, используют для этого как автоматизированные учётные записи, так и киборгов (сетевиков).

В арсенале сетевых ботов имеется несколько различных взаимодополняющих тактик. Виртуалы (сетевики или киборги), к примеру, способны завязывать разговор с реальными пользователями, распространять новые идеи (месседжи) и инициировать дискуссии в онлайн-сообществах. Эти идеи затем тиражируются в виде репостов (автоматизированной рассылки) несколькими десятками тысяч учётных записей (фейковых аккаунтов), которые мы называем «ботами-усилителями».

Еще одна группа, именуемая «ботами одобрения», создает тенденциозные тексты постов или комментариев, используя при этом маркеры одобрения

(«лайки»), пересылку контента (репост) или стандартизированный ответ на реплики. Такой алгоритм призван создать эффект активной коммуникации и эмоционального общения пользователей.

Если речь идёт о дискуссионной тематике, в которой может присутствовать несколько точек зрения на предмет обсуждения, ботов нередко используют для формирования смысловой доминанты (нужной точки зрения). Для этого организуют массированную атаку на оппонента (-ов) с применением приемов троллинга или других средств эмоционально-психологического давления. Нередко такие атаки заканчиваются деморализацией объекта агрессии и нейтрализацией его коммуникативной активности.

На первый взгляд алгоритмы политических ботов очень напоминают действия и реакции обычных пользователей социальных сетей. Именно эта технологическая мимикрия ботов способна дезориентировать многих реальных пользователей, которые нередко становятся жертвами такой кибермистификации.

Еще одна распространенная стратегия использования ботов – формирование информационной повестки дня в медиапространстве. В современной политической науке концепт повестки дня является устоявшимся и широко используемым. Данное понятие вошло в научный оборот в XX в., когда исследователи выявили существование в информационном пространстве определённого круга актуальных проблем, так или иначе затрагивающих интересы целевой аудитории [11].

Верифицируемым критерием эффективности «фабрики ботов» является выведение сообщения о событии в верхнюю десятку (на журналистском сленге – в топ) новостной ленты информационных агрегаторов, а также «оккупация» первых страниц поисковиков и каталогов по определенным запросам ссылками на продвигаемые ботами информационные ресурсы.

Зачастую деятельность ботов в меньшей степени направлена на трансформацию политического сознания интернет-пользователей, а в большей – на символическое доминирование, которое, однако, может выступать триггером возможной трансформации.

«Фабрики ботов» оказывают существенное косвенное влияние на формирование политического ландшафта в сети Интернет. Это явление в нынешних условиях получило достаточно широкое распространение и демонстрирует тенденцию к расширению сферы деятельности в публичном пространстве. Для многих современных политиков в настоящее время бот-сети становятся частью коммуникационного инструментария для проведения избирательных кампаний [12].

Анализ практик использования ботов в ходе политических кампаний в публичной сфере показывает, что ангажированные недобросовестными акторами они становятся инструментом манипулирования общественным мнением и даже более того – распространения дезинформации. Этот феномен, безусловно, требует разработки новых методов анализа и способов выявления (детектирования) политических ботов.

В настоящее время в открытых источникам немного информации о программных средствах, способных распознать бот-активность в социальных сетях. К наиболее популярным можно отнести системы *Akismet, Vkontakte, Antispam* и «Исследовательский вес рунета».

Для детектирования ботов исследователи используют небольшой набор методов. У различных научных групп особенность подхода к решению задачи определяется комбинацией этих методов.

Наиболее плодотворным методом выявления ботов является технология интеллектуального анализа данных. Рассмотрим степень эффективности применения методов машинного обучения – нейронных сетей, дерева решений и логистической регрессии. Все три метода показывают высокую точность детектирования при решении задач классификации [3].

Для машинного обучения требуется набор признаков ботов, которые станут набором маркеров в процессе выявления автоматизированных алгоритмов, распространяющих целевую информацию. Выделяют две группы признаков (маркеров): статические и поведенческие [6].

Статическая информация включает в себя следующие параметры:

− наличие аватара (фото пользователя);

− корректное написание имени владельца аккаунта;

− степень открытости пользователя (количество заполненных личных данных);

− корреляция данных пользователя в аккаунте;

− количество подписчиков;

− степень обновления контента;

− наличие иллюстративного материала (фото, видео, картинки).

Поведенческие маркеры включают следующий набор:

− количество «друзей» и тематических сообществ в подписке;

− количество публикаций на «стене» аккаунта;

− активность с одного IP-адреса за небольшой промежуток времени;

− скорость комментирования;

− участие в массированном распространении информации и др.

На основании вектора входных признаков, характеризующих распределение значений параметров пользователя, решается задача классификации определенного пользователя социальной сети [5].

Нейронные сети с учетом всех вышеперечисленных параметров (принадлежности входного образа) разделяют анализируемый массив аккаунтов на две группы – «бот» / «не бот» (рис. 2).

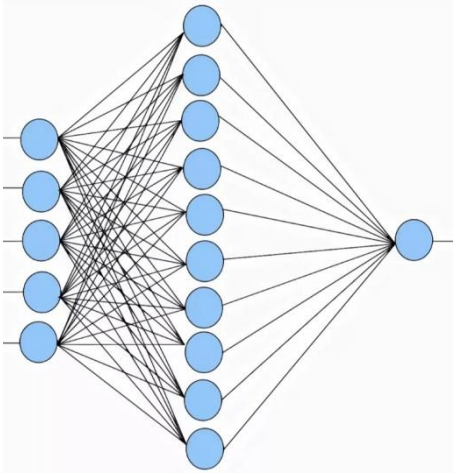

Рис. 2. Модель нейронной сети

Деревья решений – это способ представления правил в иерархической, последовательной структуре, где каждому объекту соответствует единственный узел, дающий решение (рис. 3). С помощью деревьев решений, учитывая при-

надлежности входного образа, разрабатываются способы идентификации ботов [8, с. 252–256].

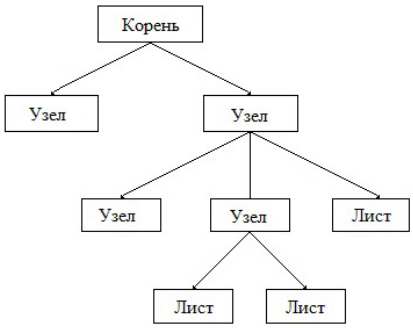

Рис. 3. Модель дерева решений

Деревья решений позволяют классифицировать новые, поступающие извне данные, и создавать достаточно экономичные конструкции.

При помощи логистической регрессии вычисляют вероятность определенных событий, в случае с линейной регрессией – можно предсказать значение переменной (рис. 4).

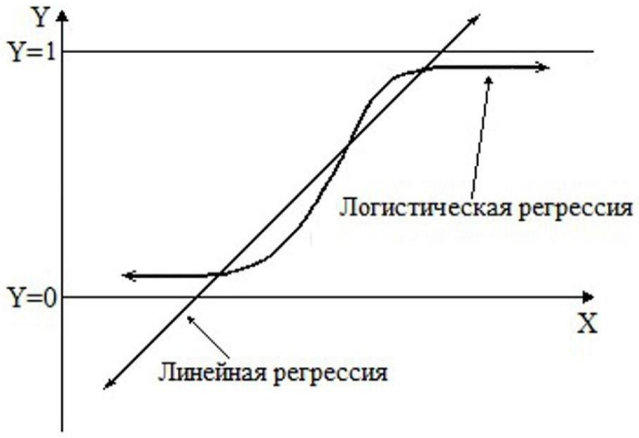

Рис. 4. Логистическая и линейная регрессии

Первый тип регрессии предсказывает номинальные значения, второй – любое численное значение.

Тестирование приведенных выше моделей показало, что наиболее эффективной из них является нейросетевая модель, точность ее показателей весьма высока [5].

Кроме машинного обучения для выявления ботов исследователи используют анализ распространяемого контента, частотный анализ сообщений и метод автоматизированного обнаружения ботов (*Botometer*). Остальные методы сводятся к анализу данных, указанных в методе машинного обучения.

В период референдума в Великобритании по вопросу о выходе из состава Евросоюза исследователи Ф. Ховард и Б. Коллани смогли обнаружить политических ботов в *Twitter*. Основываясь на трёх типах хэштегов («#за выход из ЕС», «#против выхода из ЕС» и нейтральных хэштегах, относящихся к референдуму), исследователи обнаружили 1,5 миллиона публикаций от 313382 аккаунтов. Метод частотного анализа сообщений позволил установить, что около 3 тысяч аккаунтов сгенерировали около 450 тысяч сообщений [24].

Российские исследователи ботинга А.М. Коновалова, А.В. Шорова и И.В. Котенко рассматривали не единичные бот-аккаунты, а сеть с большим количеством автоматизированных алгоритмов. В их исследовании использованы алгоритмы моделирования бот-сетей, основанные на генерации модельного трафика со статистическими параметрами, подобным параметрам трафика реальной сети. В процессе работы они провели эксперименты по созданию архитектуры среды моделирования, предназначенной для анализа бот-сетей [10].

Развитие информационных технологий привело к эволюции ботинга, что усложнило детектирование автоматизированных алгоритмов. Если на данный момент для их выявления достаточно иметь набор статических и поведенческих признаки ботов, то уже в ближайшем будущем потребуются новые, более совершенные методы, способные сочетать анализ контента, фоновых стратегий и распространяемых сообщений.

Использование программных средств детектирования бот-программ, имитирующих поведение людей, позволит уменьшить массовые хищения персональных данных, уровень недоверия в социальных сетях, количество информационных вбросов и дезинформации.

В созданной в 2010 году в России исследовательской и технологической компания «Крибрум» (Н.И. Касперская, И.С. Ашманов) разработан собственный

программно-аппаратный комплекс сбора, мониторинга и анализа данных социальных медиа в режиме реального времени (100–150 млн сообщений в сутки), который позволяет достаточно эффективно выявлять технологии ботинга [17].

Вместе с тем существует и другой подход к проблеме. Американский исследователь Самуэль Вулли (*Woolley S.C.*) и его британский коллега Филип Ховард (*Howard P.N.*) полагают, что продуктивнее не бороться с ботингом как явлением, а ввести компьютерную пропаганду в юридическое поле путем регламентации этого вида деятельности. Эти ученые считают, что применение бот-технологий в политических коммуникациях и не только достаточно сложно контролировать. С. Вулли и Ф. Ховард также отмечают, что в современных условиях медиатизации публичной сферы и виртуализации политического пространства очевиден запрос на новую междисциплинарную социальную науку, предметом исследования которой стало бы применение IT-технологий в сфере политики и не только [28].

Таким образом, рассмотренные инструменты детектирования ботов и выявления бот-сетей позволяют пролить свет на сложную экосистему современных медиа. Тем не менее многие вопросы по-прежнему остаются открытыми. Например, никто точно не знает, сколько социальных ботов присутствуют в соцсетях, или какую долю контента они генерируют – оценки исследователей сильно разнятся. Алгоритмы поведения ботов уже достаточно сложны: они способны создавать реалистичные профили и вызывающий доверие пользователей контент. Можно предположить, что по мере совершенствования систем их обнаружения будет модернизироваться и технология ботинга. Соревнование продолжится. Как долго? Покажет будущее.

Выводы.

1. Современная публичная политика характеризуется процессами виртуализации и медиатизации, в результате чего социально-политическая реальность для населения большинства стран становится результатом восприятия виртуальных представлений и образов, порой не имеющих ничего общего с объективной действительностью.

2. Особенностью функционирования современной публичной политики является повышение роли сетевых структур, в частности роли социальных сетей и блогосферы как новых акторов публичной политики.

3. Новые технологические возможности породили феномен социальных ботов. Их активное применение в практике политической коммуникации дало основание говорить о появлении нового феномена – компьютерной пропаганды.

4. Новым шагом в развитии технологии ботинга стало использование людей, получивших название «киборгов» или «сетевиков» в качестве операторов коммуникации для более продуктивного выполнения функций роботов.

5. Анализ практик использования ботов в ходе политических кампаний в публичной сфере показывает, что ангажированные недобросовестными акторами они становятся инструментом манипулирования общественным мнением и даже более того – распространения дезинформации. Этот требует разработки новых методов анализа и способов выявления (детектирования) политических ботов.

6. Для детектирования ботов исследователи используют небольшой набор методов. У различных научных групп особенность подхода к решению задачи определяется комбинацией этих методов. Наиболее плодотворным методом выявления ботов является технология интеллектуального анализа данных.

Список литературы

1. Василькова В.В. Социальные боты в политической коммуникации / В.В. Василькова, Н.И. Легостаева // Вестник РУДН. Социология. – 2019. – №1 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/sotsialnye-boty-v-politicheskoy-kommunikatsii (дата обращения: 05.03.2024). DOI 10.22363/2313-2272-2019-19-1-121-133. EDN VUHAGU

2. Василькова В.В. Компьютерная пропаганда: структурные характеристики и векторы исследования / В.В. Василькова, П.А. Трекин // Вестник Санкт-Петербургского университета. Социология. – 2020. – №1 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kompyuternaya-

propaganda-strukturnye-harakteristiki-i-vektory-issledovaniya (дата обращения: 02.03.2024). DOI 10.21638/spbu12.2020.105. EDN XSKRXR

3. Гончаров Н.О. Современные угрозы бот-сетей / Н.О. Гончаров // Молодежный научно-технический вестник. – 2014. – №10 [Электронный ресурс]. – Режим доступа: http://ainsnt.ru/doc/734776.html (дата обращения: 28.02.2024). EDN TBAVPN

4. Евгений Пригожин признал создание «фабрики троллей» // Коммерсантъ. – 2023. – 14 февраля [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/5826246 (дата обращения: 07.03.2024).

5. Евсеева А.О. Идентификация ботов в социальных сетях на базе технологий интеллектуального анализа данных / А.О. Евсеева, Р.И. Гумерова, А.С. Катасёв [и др.] // Вестник технологического университета. –2017. – №5. – С. 87–88. EDN YHEHJX

6. Зегжда Д.П. Оценка эффективности использования средств защиты для нейтрализации и устранения бот-сетей / Д.П. Зегжда, Т.В. Степанова // Проблемы информационной безопасности. Компьютерные системы. – 2012. – №2. – С. 21–27. EDN PAZTDH

7. Иванов Д.В. Виртуализация общества. Версия 2.0 / Д.В. Иванов. – СПб.: Петербургское востоковедение, 2002. – С. 108. EDN RQMXUB

8. Катасёв А.С. Нейросетевая модель идентификации ботов в социальных сетях / А.С. Катасёв, Д.В. Катасёва, А.П. Кирпичников [и др.] // Вестник Казанского технологического университета. – 2015. – №16. – С. 252–256.

9. Коровин В.М. Третья мировая сетевая война / В.М. Коровин. – СПб.: Питер, 2014. – С. 79.

10. Котенко И.В. Агентно-ориентированное моделирование бот-сетей и механизмов защиты от них / И.В. Котенко, А.М. Коновалов, А.В. Шоров // Вопросы защиты информации. – СПб.: СПИИРАН, 2011. – С. 24.

11. Лушанкин С.С. Категория «повестка дня» в структуре политического процесса: понятие «политической повестки дня» и модели её формирования / С.С. Лушанкин // Вестник Удмуртского университета. Социология. Политоло-

гия. Международные отношения. – 2017. – №4 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kategoriya-povestka-dnya-v-strukture-politicheskogo-protsessa-ponyatie-politicheskoy-povestki-dnya-i-modeli-eyo-formirovaniya (дата обращения: 10.03.2024). EDN KXGGHR

12. Мартьянов Д.С. Политический бот как профессия / Д.С. Мартьянов // ПОЛИТЭКС. – 2016. – №1 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/politicheskiy-bot-kak-professiya (дата обращения: 25.02.2024). EDN WKBFPB

13. Мирошниченко И.В. Организация сетевого online пространства публичной политики / И.В. Мирошниченко // Сетевой анализ публичной политики. – М.: РГ-Пресс, 2013. – С. 203–207.

14. Павлютенкова М.Ю. Роль и место социальных сетей в публичной политике / М.Ю. Павлютенкова // Вестник РУДН. Политология. – 2015. – №3 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/rol-i-mesto-sotsialnyh-setey-v-publichnoy-politike (дата обращения: 26.02.2024). EDN UDCUDL

15. Рябченко Н.А. Институционализация публичной политики в online-пространстве современной России / Н.А. Рябченко, И.В. Мирошниченко. – Краснодар: Просвещение-Юг, 2012. – С. 54. EDN RCIMGJ

16. ФБР пообещало $250 тыс. за информацию о Пригожине // Коммерсантъ. – 2021. – 26 февраля [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/4710119 (дата обращения: 04.03.2024).

17. АО «Крибрум»: официальный сайт [Электронный ресурс]. – Режим доступа: https://www.kribrum.ru/company/ (дата обращения: 01.03.2024).

18. Bessi A., Ferrara E. Social Bots Distort the 2016 US Presidential Election Online Discussion // First Monday. – 2016. – Vol. 21. №11. – P. 7 [Electronic resource]. – Access mode: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2982233 (дата обращения: 26.02.2024).

19. Brachten F., Stieglitz S., Hofeditz L., Kloppenborg K., Reimann A. Strategies and Influence of Social Bots in a 2017 German State Election: A Case Study on

Twitter [Electronic resource]. – Access mode: https://arxiv.org/abs/1710.07562 (дата обращения: 29.02.2024).

20. Castells M. The Rise of the Network Society // The Information Age: Economy, Society and Culture. – Cambridge MA, Oxford UK: Blackwell Publishers, 1996. – 556 p.

21. Corneliu B. The Ethics of Countering Digital Propaganda // Carnegie Council for Ethics in International Affairs. – 2018. – Vol. 32, iss. 3. – P. 305–315 [Electronic resource]. – Access mode: https://www.cambridge.org/core/journals/ethics-andinternational-affairs/article/ethics-of-countering-digitalpropaganda/DF393C0793F31EE0940E9208E24CB6A8 (дата обращения: 25.02.2024).

22. Ferrara E., Varol O., Davis C., Menczer F., Flammini A. The rise of social bots. Communications of the ACM [Electronic resource]. – Access mode: https://arxiv.org/abs/1407.5225 (дата обращения: 29.02.2024).

23. Gorwa R., Guilbeault D. Unpacking the Social Media Bot: A Typology to Guide Research and Policy [Electronic resource]. – Access mode: https://arxiv.org/abs/1801.06863 (дата обращения: 04.03.2024).

24. Howard P.N., Kollanyi B. Bots, #Strongerin, and #Brexit: Computational propaganda during the UK-EU referendum // Project on Computational Propaganda [Electronic resource]. – Access mode: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798311 (дата обращения: 04.03.2024).

25. Howard P.N., Woolley S., Calo R. Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration // Journal of Information Technology & Politics. – 2018. – №15. – P. 85.

26. Ncube L. Digital Media, Fake News and Pro-Movement for Democratic Change (MDC) Alliance Cyber-Propaganda during the 2018 Zimbabwe Election // African Journalism Studies. – 2019. – Vol. 40 [Electronic resource]. – Access mode: https://www.tandfonline.com/doi/figure/10.1080/23743670.2019.1670225?scroll=top&needAccess=true (дата обращения: 07.03.2024).

27. Van Dijk, Jan. The Network Society. – London: Sage Publications, 1999. – P. 69 [Electronic resource]. – Access mode: https://www.researchgate.net/publication/298428268_Jan_Van_Dijk_The_Network_Society_London_Sage_Publications_2012 (дата обращения: 01.03.2024).

28. Woolley S.C., Howard P.N. Computational propaganda: political parties, politicians, and political manipulation on social media // Oxford University Press, 2018. – P. 263.

29. Woolley S.C., Howard P.N. Automation, algorithms, and politics/political communication, computational propaganda, and autonomous agent – introduction // International Journal of Communication. – 2016. – №10 [Electronic resource]. – Access mode: https://ijoc.org/index.php/ijoc/article/view/6298 (дата обращения: 10.03.2024).