УДК 004.056.5:004.738.5(045)

Бондаренко І.О
Порицька В.В

ВПЛИВ БОТІВ У СОЦІАЛЬНИХ МЕРЕЖАХ ТА ЇХ НЕБЕЗПЕКА

Вінницький національний технічний університет

Анотація

Доповідь присвячена огляду впливу ботів на користувачів у соціальних мережах та їх небезпеці. Досліджено вплив та ризики, які несуть боти для суспільства та інформаційної безпеки.

Ключові слова: соціальні боти, веб-сканери, чат-боти, інформаційна безпека, дезінформація, маніпулювання.

Abstract

The report is devoted to an overview of the impact of bots on users in social networks and their danger. The impact and risks posed by bots to society and information security are analyzed.

Keywords: social bots, web crawlers, chatbots, information security, disinformation, manipulation.

Вступ

У цифрову еру інформаційних технологій соціальні мережі стають не лише платформами для спілкування, але й аренами, де відбувається активна боротьба за увагу та вплив. Серед інструментів, що використовуються в цій боротьбі, особливе місце займають соціальні боти. Ці автоматизовані програми здатні оперативно створювати, поширювати та підсилювати певні повідомлення чи думки в мережі, впливаючи на громадську думку та поведінку користувачів [1].

Завдяки великій аудиторії в соціальних мережах, будь-яка новина може легко зібрати мільйони переглядів, але перевірити правдивість новин дуже важко, що сприяє поширенню дезінформації і дозволяє маніпулювати людською свідомістю за допомогою ботів та інших технологій.

Результати дослідження

Наведемо визначення поняття «бот». Ботами називають повністю або частково автоматизовані системи, які виконують поставлені завдання [1]. Відповідно до їх призначення розрізняють багато видів ботів, серед яких найпоширенішими є [2]:

– веб-сканери, що періодично переглядають мережу для індексації сторінок;

– чат-боти, за допомогою штучного інтелекту імітують персональну розмову, відомим прикладом є ChatGPT та боти, які автоматизують обслуговування клієнтів на веб-сайтах;

– соціальні боти, облікові записи призначені для одно- або багатостороннього спілкування та імітації поведінки людини у соціальних мережах. Соціальні боти є керованими програмним забезпеченням обліковими записами соціальних мереж, які імітують людей зі зловмисними намірами.

Соціальні боти отримали широке розповсюдження, адже допомагають автоматизувати багато проблем бізнесу, а саме, пришвидшити клієнтське обслуговування, забезпечити персоналізацію контенту, що покращує користувацький досвід з певним сервісом. Але також використовуються і для розповсюдження спаму, дезінформації та різноманітних маніпуляцій.

До типових форм шкідливої діяльності ботів відносяться:

– поширення дезінформації;
– маніпуляція громадською думкою;
– спам;
– фішинг та кібершахрайство;
– створення ботнетів.

Боти можуть автоматично створювати та поширювати фальшиві новини, пропагандистську інформацію з метою впливу на громадську думку, можуть автоматично розміщувати коментарі або повідомлення, тим самим перешкоджаючі спілкуванню користувачів у соцмережах, можуть намагатися

отримати конфіденційну інформацію від користувачів. Дані форми діяльності ботів можуть мати серйозні наслідки для користувачів соціальних мереж та суспільства в цілому, тому важливо бути обережними при взаємодії з вмістом у мережі.

Багато фейкових акаунтів створюються з метою впливу на користувачів у хибний спосіб для своїх рекламних кампаній чи підтримки певних політичних партій. З кожним роком кількість фейкових акаунтів постійно зростає, хоча немає загальноприйнятого стандарту, як саме визначати ботів серед користувачів і результати можуть відрізнятися від методу, але ще у 2015 році кількість ботів у мережі Twitter (нині X) становила від 9% до 15% усіх користувачів [3].

Яскравим прикладом дезінформації та маніпулювання за участю ботів є президентські вибори США у 2016 році. Дослідження дослідників Columbia SIPA, які досліджували вплив російських інтернет-«тролів» на ринки онлайн-букмекерів, свідчить про те, що діяльність тролів вплинула на президентські вибори в бік Дональда Трампа [4].

Через активне залучення соціальних ботів у політичне життя багатьох країн у грудні 2018 року Європейська комісія (2018 : 4) оприлюднила свій План дій проти дезінформації [5]. У якому соціальні боти розглядаються як техніка «поширення та посилення суперечливого контенту та дебатів у соціальних мережах», які можна використовувати для поширення дезінформації. Були прийняті заходи регулювання, які вимагають маркування облікових записів ботів.

Розуміючи реальну загрозу були проведені дослідження, які дозволяють порівнювати наявні методи для виявлення фейкових акаунтів, зокрема дослідження «Bot, or not? Comparing three methods for detecting social bots in five political discourses» [5], де порівнювалися три різних методи виявлення ботів. Однак, як зазначають автори, будь-які дослідження на дану тему стикаються щонайменше з двома проблемами:

– проблема фактичної правди, дослідники не можуть з упевненістю говорити, що даний аккаунт є фейковим;

– швидке старіння даних, адже соціальні мережі динамічні структури. Це призводить до того, що аналіз залежить від часу.

Перш ніж проводити дослідження, автори домовилися позначати ботами облікові записи які у результаті отримали 0,75 балів і вище. Адже у результаті кожен обліковий запис отримував від 0 до 1, де 1 – це дуже підозріла поведінка.

Проаналізувавши за допомогою методів важкої автоматизації, Tweetbotornot та Botometer у соціальній мережі Twitter різних політичних дискусів, дослідники дійшли висновку, що методами важкої автоматизації та Tweetbotornot було отримано схожі результати, тоді як Botometer виявив значно меншу кількість ботів. Загалом було перевірено 122 884 унікальних облікових записів та виявлено, які були активні у політичних дискусіях 2018 року та виявлено 27 363 облікових записів, що були сильно автоматизовані, тобто 22% від усіх перевірених облікових записів.

Висновок

Отже, небезпека діяльності шкідливих ботів у соціальних мережах з часом буде лише зростати, тому вирішенню даної проблеми присвячено багато статей та досліджень, адже це має значний вплив на наше реальне життя. Тому вкрай важливим є розробка передових методів автоматичного виявлення соціальних ботів.

Загалом, лише спільні зусилля та комплексний підхід можуть принести значимі результати у боротьбі із впливом ботів у соціальних мережах та забезпечити безпеку та довіру у цифровому середовищі. Важливо надавати користувачам достатню освіту та інформацію про розпізнавання та уникнення впливу ботів, фейкових новин та дезінформації. А компанії-розробники соціальних мереж повинні продовжувати розвивати технології виявлення та блокування ботів, використовувати штучний інтелект та машинне навчання для виявлення шкідливої активності.

В цілому, шкідлива діяльність ботів може мати серйозні наслідки як для звичайних користувачів, так і для суспільства в цілому, тому важливо приділяти увагу цьому проблемному явищу та розвивати стратегії протидії його поширенню.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Assenmacher, D., Clever, L., Frischlich, L., Quandt, T., Trautmann, H., & Grimme, C. (2020). Demystifying Social Bots: On the Intelligence of Automated Social Media Actors. Social Media + Society, 6(3). URL: https://doi.org/10.1177/2056305120939264 (дата звернення: 10.02.2024).

2. Зацепін О. А. Фільтрація Твіттер-стрічки у режимі реального часу за допомогою машинного навчання. Репозитарій КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/server/api/core/bitstreams/aff42c0f-1d86-4401-b9f8-750eca0ec3db/content (дата звернення: 12.02.2024).

3. Detection of Bots in Social Media: A Systematic Review. *ScienceDirect*. URL: https://www.science-direct.com/science/article/abs/pii/S0306457319313937 (дата звернення: 15.02.2024).

4. Study Confirms Influence of Russian Internet “Trolls” on 2016 Election. URL: https://www.sipa.columbia.edu/news/study-confirms-influence-russian-internet-trolls-2016-election (дата звернення: 15.02.2024).

5. Bot, or not? Comparing three methods for detecting social bots in five political discourses. SageJournals. URL: https://doi.org/10.1177/20539517211033566 (дата звернення: 20.02.2024).

Порицька Вероніка Володимирівна – студентка групи КІТС-21б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: porickaveronika@gmail.com

Бондаренко Ірина Олексіївна – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Porytska Veronika V. – student of CSITS-21b group, Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia**,** e-mail: porickaveronika@gmail.com

Bondarenko Iryna O. – assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua