УДК 004.9
Зуєв Б.В.[1], Зайко Т.А.[2]
[1] студ. гр. КНТ-139 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

МЕТОДИ ВИЗНАЧЕННЯ БОТІВ СЕРЕД КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ

На сьогоднішній день соціальні мережі відіграють величезну роль у світосприйнятті людей. Щодня користувачі відвідують такі відомі соціальні мережі, як Instagram, Facebook, YouTube, Twitter, TikTok та інші. Так,

наприклад, платформу YouTube використовує 96% відвідувачів мережі «Інтернет», проводячи при цьому на ній в середньому 40 хвилин на день [1]. Проводячи таку кількість часу, кожен користувач піддається інформаційному впливу. Як правило, маніпулювання відбувається через соціальних ботів, що мають на меті нав'язування іншим учасникам соціальної мережі деяких ідей або посилів шляхом активного розповсюдження великої кількості одноманітних повідомлень, постів, тощо.

Соціальний бот – спеціальна програма (агент), що створена для імітації поведінки людей у соц. мережах, або реальна людина під вигаданим ім'ям, що виконує завдання інформаційного впливу та формування суспільної думки.

Для того, щоб боротися з ботами, спершу їх необхідно ідентифікувати серед інших користувачів соц. мереж. Існує ціла низка параметрів, на які слід орієнтуватися, перш ніж блокувати недобросовісного користувача, або обмежувати його можливості. Перш за все, необхідно звернути увагу на такі параметри підозрілої сторінки:

- фотографія - якщо аватар користувача – зображення з мережі «Інтернет», чи стандартного фотостоку, це перша підозра. Важливим також є те, коли були додані фотографії і відповідність пори року фотографії до поточного часу.

- список друзів - сторінка вважається підозрілою, якщо її власник має замалу, або ж навпаки, завелику кількість друзів.

- зміст публікацій - типовий бот, зазвичай, виконує репости з інших підозрілих сторінок, використовує завелику кількість посилань на інші матеріали.

- швидкість відповіді - звичайна людина, перечитуючи коментар, формулює свою думку й надсилає відповідь, витрачаючи на це більшу кількість часу, аніж бот, адже соціальний бот може мати купу готових провокативних відповідей та запитань.

- схожість з іншими користувачами соц. мережі. Один з критеріїв виявлення бота є порівняння поточного підозрілого аканту з іншими. Трапляється, під однією темою дискусії або постом, можна побачити відразу декілька схожих акаунтів, з однаковою, закономірною поведінкою, тезами, аргументами та іншим провокативним змістом, як правило, інформаційно-психологічного характеру.

Найпростіший спосіб виявлення бота – повідомлення про знаходження підозрілого акаунту звичайним користувачем. Більшість соціальних мереж надають відвідувачам можливість поскаржитися на певну публікацію чи цілий обліковий запис, при цьому, якщо система зафіксує перевищення ліміту таких скарг, акаунт буде розглянуто адміністрацією й перевірено на відповідність поведінки до правил сервісу.

Деякі веб-ресурси, такі як дошки об'яв чи маркетплейси, користуються репутаційними системами, це означає, що недобросовісні користувачі, чи спеціалізовані програми будуть гірше просуватися на таких платформах, а іноді, навіть, блокуватися. Хоча репутаційні системи використовуються, найчастіше, для захисту від шахраїв, вони також можуть бути одним з інструментів для боротьби з ботами, а значить, їх вплив на інших користувачів суттєво зменшуватиметься.

Найскладнішим та найсучаснішим способом виявлення ботів є спеціалізовані програми, як правило, створені розробниками соціальної мережі, яку необхідно захистити. Метод полягає у збиранні статистичних даних підозрілих акаунтів, визначенні можливих шаблонів поведінки ботів, обчисленні певних статистичних показників та визначенні коефіцієнтів кореляції між підозрілими обліковими записами. Наприклад, 3 березня 2021 року, компанія Facebook повідомила, що було виявлено та видалено 530 російських акаунтів Instagram, пов'язаних із протестними акціями в РФ у січні та лютому [2]. Безумовно, такі величезні соціальні мережі не в змозі контролювати усі скарги власноруч, тому, не є виключенням, що Facebook використовує автоматизовані методи виявлення та знешкодження ботів. Вочевидь, усі заблоковані сторінки мали велику кореляцію подібності, дуже схожі шаблони поведінки, використовувані провокативні репліки, що й допомогло відрізнити їх від реальних користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1 За рік кількість українців у соцмережах зросла на 7 мільйонів – дослідження [Електрон. ресурс]. – Режим доступу : https://www.epravda.com.ua/rus/news/2021/03/17/672023/.

2 February 2021 Coordinated Inauthentic Behavior Report [Electronic resource]. – Access mode : https://about.fb.com/news/2021/03/february-2021-coordinated-inauthentic-behavior-report/.

3 Соціальний бот, Вікіпедія [Електрон. ресурс]. – Режим доступу : uk.wikipedia.org/wiki/Соціальний_бот.