УДК 004.056

В. М. Островська
О. П. Войтович

ТРОЛІНГ ЯК ЗАСІБ ІНФОРМАЦІЙНОЇ ВІЙНИ

Вінницький національний технічний університет

Анотація

В роботі досліджено явище тролінгу, як виду інформаційно-психологічних операцій під час інформаційної війни в мережі Інтернет. Узагальнено засоби та ознаки маніпулятивного впливу на учасників спілкування, зокрема у соціальних мережах.

Ключові слова: тролінг, троль, інформаційно-психологічні операції, аналіз тональності, рекурентні нейронні мережі, аналіз емоційності тексту.

Abstract

The phenomenon of trolling as a kind of information psychological operations during warfare is researched. The signs and means of manipulative influence on the participants in communication including social networks are generalized.

Keywords: trolling, troll, information psychological operations, sentiment analysis, recurrent neural networks, text emotion analysis.

Вступ

Однією з цілей інформаційної війни є вплив на морально-психологічний стан протилежної сторони: позбавити її сили та спроможності протистояти, деморалізувати. Для ведення інформаційних війн використовується своя специфічна зброя – інформаційні операції: інформаційно-психологічні впливи на людину та інформаційно-технічні впливи на кіберпростір.

Швидкий розвиток мережі Інтернет спричинив активізацію комунікації в суспільстві та відкрив широкі можливості для технологій маніпулятивного впливу. Термін «маніпуляція» розглядається як прихований психологічний вплив на мотивацію людини з метою змінити її погляди, інтереси та поведінку [1].

Метою роботи є з'ясування й узагальнення засобів та ознак технології маніпулятивного впливу – тролінгу – в соціальних мережах для підвищення ефективності його розпізнавання.

Результати дослідження

Одним із найяскравіших проявів маніпуляції за допомогою інформаційно-психологічних операцій, є тролінг (англ. Trolling – «виспівування») – процес розміщення в Інтернеті провокаційних повідомлень з метою посилення соціальної напруги шляхом порушення правил етичних норм комунікації в мережі Інтернет [1]. Особу, яка займається тролінгом, називають тролем. Разом із поданням засобами масової інформації винятково агресивного контенту новин [2] тролінг стає живильним середовищем для подальшої фрустрації суспільства та штучно сформованої поляризації його думки.

Тролі застосовують такі основні операції:

– навмисна гра на почуттях людей із врахуванням спрямованості співтовариства (наприклад, поява на форумі любителів кішок коментаря зі списком страв із кошатини);

– офтоп або офтопік (англ. off topic – «поза темою») – будь-яке повідомлення в мережі Інтернет, що не стосується заздалегідь визначеної теми спілкування;

– спонукання на суперечку (наприклад, коментарі з расистським змістом);

– самовпевнені висловлювання: вираження власної думки як загальновизнаного факту без аргументації або аналізу, розпалювання «холівар» (англ. holy war – «священна війна»);

– спойлер (англ. spoiler – «перешкода») – навмисна публікація розв'язки свіжого й популярного на даний час кінофільму або художнього твору;

– постмодерація повідомлень, окремих тем або новин – так званий «флейм» (англ. flame –

«полум’я», «вогонь»);

– будь-яка комбінація вищенаведеного: наприклад, троль поєднує спонукання на суперечку з бідністю мови й поганими манерами, разом з цим висуваючи самовпевнені висловлювання.

Повідомлення, які надсилають тролі, мають образливий характер, неетичну критику та не змістове, а саме емоційне наповнення. Емоційна складова спеціально підготовленої інформації і, як наслідок, відповідний стан соціуму може максимально сприяти ефективному поширенню інформації або, навпаки, створювати умови для повного неприйняття інформації [3]. Тому для виявлення тролінгу першочергово слід визначити тональність повідомлень. Метою цього є з’ясування позиції користувача відносно досліджуваних об’єктів або подій, що зводиться до віднесення тональності публікації до попередньо визначеної категорії – негативна, позитивна, нейтральна (рис. 1).

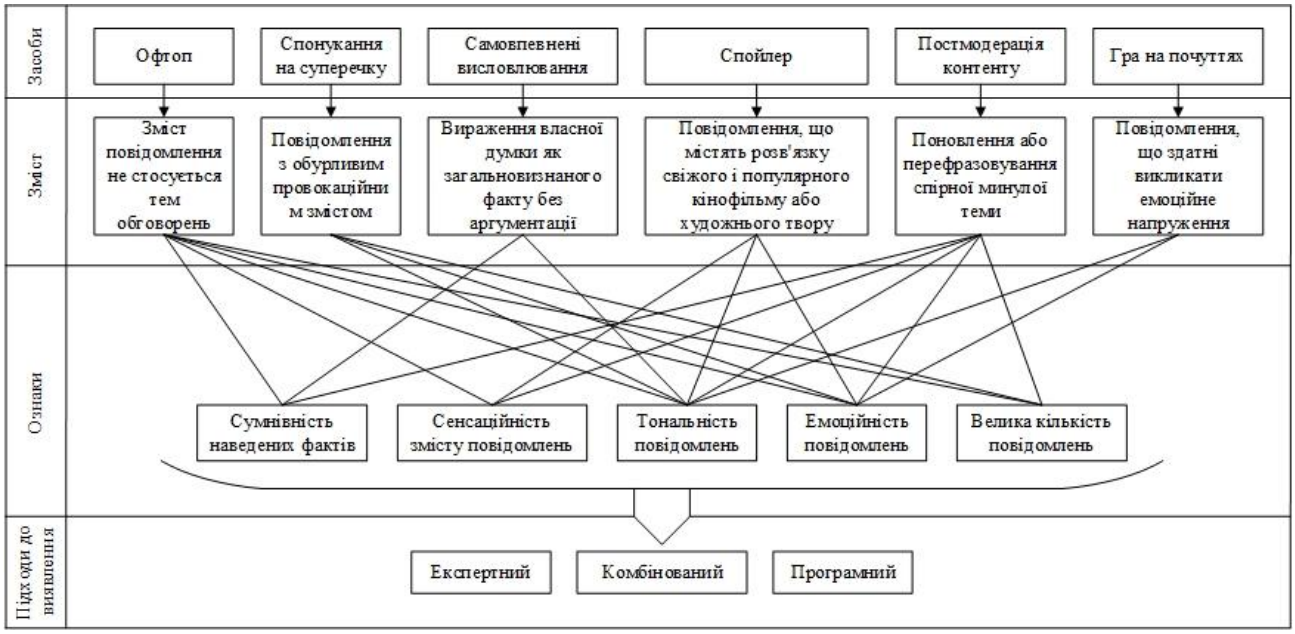

Рис. 1. Основні засоби та ознаки тролінгу

Для аналізу тональності текстових даних доцільно застосовувати глибоке навчання рекурентних нейронних мереж, яке не викликає складнощів із перенавчанням, на відмінну від згорткових та повнозв’язних нейронних мереж.

Також для виявлення тролінгу в соціальних мережах необхідно виокремлювати в публікаціях такі не менш важливі ознаки його застосування:

– емоційність повідомлення, що використовується для відображення емоційного стану його автора і проявляється у перенасиченні тексту прислівниками, вигуками, лексемами емоційного характеру тощо. Оскільки тролінг є засобом агресивного впливу, що викликає агресію у відповідь, особливу увагу варто звертати на контент з негативною тональністю. Тому лексеми емоційного характеру доцільно поділити на групи, кожна з яких відповідатиме поведінці, стану, почуттю, чуттєвій реакції чи емоції людини, які вирізняються своєю негативністю та викликані прочитаним повідомленням. Такі групи можуть містити лексеми, що, наприклад, викликають страх, агресивну ворожість, відразу тощо. Для кожної такої групи необхідно сформувати свій емоційний словник [4];

– сумнівність наведених фактів, що визначається відсутністю джерел та авторів інформації, недостатньою аргументацією, посиланнями на думку широкого загалу, наявністю риторичних запитань та ненадійних висловлювань;

– сенсаційність повідомлення, що має на меті привернути увагу завдяки посиланням на заяви епатажних осіб, вживанню слів, які підвищують тривожність, створюють атмосферу швидкоплинності й терміновості явищ;

– велика кількість повідомлень. У соціальних мережах велика увага користувачами звертається на ті публікації, які зосередили навколо себе велику кількість учасників, тобто які зібрали більшу кількість репостів, коментарів, «лайків» [5]. Розміщуючи багато коментарів, тролі зумовлюють соціалізацію цього контенту та створюють ілюзію активного обговорення, їх значущості та

критичності. Як правило, до цього вдаються соціальні тролі [6].

Варто зазначити, що виявлення наведених ознак застосування тролінгу є складноформалізованим завданням, що вимагає застосування комбінованого підходу, що грунтується на використанні експертного та програмного підходів (див. рис. 1).

Висновки

Аналіз основних засобів тролінгу засвідчив, що не існує загально-визначених правил чи дій для його запобігання. Кожен з користувачів мережі Інтернет самостійно, залежно від ситуації чи умов виникнення ознак маніпулювання, обирає свої методи захисту, але, незважаючи на це, найголовнішим способом протидії тролінгу в першу чергу є його розпізнавання. Саме тому доцільно розробити методику виявлення тролінгу як технології маніпулятивного впливу.

REFERENCES

1. Кокарча Ю. А. Тролінг як засіб політичної маніпуляції в Інтернет-просторі [Електронний ресурс] / Ю. А. Кокарча // Науковий часопис НПУ імені М. П. Драгоманова. Серія 22 : Політичні науки та методика викладання соціально-політичних дисциплін. – Режим доступу : http://enpuir.npu.edu.ua/bitstream/123456789/17544/1/Kokarcha.pdf. – Назва з екрану.

2. Савінова Н. А. Інформаційна політика України у дискурсі безпеки людини і громадянина : зб. матер. наук.-практ. конф. ["Актуальні проблеми управління інформаційною безпекою держави"], (м. Київ, 19 березня 2015 року) / Н. А. Савінова. – Київ : Центр навчальної, наукової та періодичних видань НА СБ України, 2015. – С. 119–123.

3. Дудатьєв А. В. Інформаційна безпека соціотехнічних систем: модель інформаційного впливу [Електронний ресурс] / Дудатьєв А. В., Войтович О. П. // Інформаційні технології та комп'ютерна інженерія. – Режим доступу : https://itce.vntu.edu.ua/index.php/itce/article/view/657/401. – Назва з екрану.

4. Островська В. М. Семантичний аналіз Великих Даних у задачах кібербезпеки / Островська В., Войтович О. // Інформаційні технології та комп'ютерне моделювання. – Івано-Франківськ, 2017. – С. 256–259.

5. Voitovych O. Badania sieci społecznych jako źródła informacji w czasie wojny [Електронний ресурс] / Voitovych O., Holovenko V. // Inżynier XXI wieku projectujemy przyszlosc : monografia / [pod red. : Jacek Rysiński]. – Режим доступу : https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17254/2688.pdf?sequence=3. – Назва з екрану.

6. Молодецька К. В. Підхід до виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах / К. В. Молодецька // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в АТО : зб. матер. IX наук.-практ. конф., 25 листоп. 2016 р. – Київ: ВІТІ, 2016. – С. 130–131.

Островська Вероніка Михайлівна – студентка групи БС–17м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: nika.ostrovska21@gmail.com

Науковий керівник: ***Войтович Олеся Петрівна*** – канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Ostrovska Veronika M. – Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, email: nika.ostrovska21@gmail.com

Supervisor: ***Voitovych Olesia P.*** – Cand. Sc. (Eng), Assistant Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia