НАЦІОНАЛЬНА БЕЗПЕКА

Драбчук В.П.
студент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

ПРОТИДІЯ НЕГАТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВАМ У СОЦІАЛЬНИХ МЕРЕЖАХ

З 2014 року Російська Федерація розпочала війну з Україною, основними складовими якої являються: анексія Криму в березні 2014 та збройний конфлікт на частині територій Донецької та Луганської областей з квітня 2014.

Одним з засобів інформаційної війни стало поширення пропаганди та дезінформації через ЗМІ та соціальні мережі. Розповсюджувачами пропаганди стали – блогери, журналісти, артисти тощо, так і боти та аноніми. Завдяки російській групі хакерів «Анонімний інтернаціонал» стало відомо про створення організацій (наприклад, ТОВ «Інтернет дослідження» з офісом в Ольгіно, м. Санкт-Петербург), що займалися поширенням пропаганди та дезінформації через платні публікації та коментарі в соціальних мережах. Електронні скриньки керівників цієї організації були зламані, а листи викладені у мережу Інтернет. Згодом на основі даної переписки були проведені журналістські розслідування та навіть взяті інтерв'ю у людей, що в минулому працювали там платними коментаторами.. Ця тактика не нова, в Китаї вже давно існує армія платних коментаторів, так звана Умаодан, або «50-центова армія», що складається з китайських провладних блогерів та учасників Інтернет-форумів, які пишуть тексти та коментарі за гроші для формування громадської думки в тому чи іншому напрямку. Умаодан за деякими оцінками складає 300 тисяч чоловік . Як показує досвід, подібні платні блогери та коментатори здатні вносити значний деструктивний інформаційний вплив та маніпулювати громадською думкою, що становить небезпеку для інформаційної безпеки держави. В ряді наукових робіт показано, що міркування людей в соціальній мережі в значній мірі залежать від міркувань впливових учасників даної мережі, яким вони довіряють, а також від міркувань більшості [1; 2; 3].

Існує багато наукових робіт з аналізу соціальних мереж та методів інформаційного впливу на їх користувачів з різними цілями від маркетингових до політичних, але в той же час дуже мало напрацювань стосовно того, як протидіяти даним інформаційним впливам. Хоча навіть невеликими зусиллями можна виявити деструктивні втручання в соціальні мережі. Наприклад, відразу після вбивства російського опозиційного політика Бориса Нємцова американський журналіст Алек Лун помітив, як велика кількість користувачів

Твіттеру розмістили однакові твіти. Йшлося про те, що Нємцова вбили українці. За допомогою відкритих онлайн-інструментів NodeXL та Gephi інтернет-дослідник Лоуренс Александер зібрав та візуалізував дані про користувачів, що поширювали дану інформацію та виявив понад 20 тисяч прокремлівських ботів серед твіттер-аккаунтів. Сучасні способи поширення пропаганди та дезінформації ставлять перед суспільством нові виклики, адже не існує чітких та добре працюючих механізмів захисту від негативного інформаційного впливу на суспільство через соціальні мережі.

Аналіз величезних масивів інформації та дій сотень тисяч користувачів не представляється можливим здійснювати лише з використанням людських ресурсів без втрати якості, швидкості та відсутності помилок суб'єктивного сприйняття. До того ж читати великі масиви деструктивної інформації може бути шкідливо для людської психіки. Автоматично розпізнавати агентів впливу в соціальних мережах програмними засобами видається досить перспективним методом, що дозволить оперативно відслідковувати та спростовувати фейкову інформацію, а також викривати або блокувати таких агентів і опубліковані ними матеріали [4].

Для виявлення деструктивних впливів в соціальних мережах доцільно використовувати наступні методи та засоби:

- класифікація даних;
- колаборативна фільтрація;
- експертні системи;
- лінгвістичний аналіз текстів;
- інформаційний пошук;
- когнітивне моделювання;
- стеганографічні методи виявлення джерел поширення інформації – технологія «цифрових відбитків пальців».

За допомогою таких методів та засобів можна отримувати наступну інформацію про соціальні мережі та їх інформаційне наповнення:

- виділення спільнот у соціальній мережі, що поширюють деструктивну інформацію;
- виявлення спаму;
- виявлення фейкових аккаунтів та ботів;
- виявлення різних профілів одного користувача;
- виявлення лідерів думок, через яких впливають на загальну думку;
- оцінка інформаційних впливів у соціальній мережі;
- побудова тематичного профілю інтересів користувача або групи користувачів;
- визначення прихованих атрибутів користувачів за текстами їх повідомлень;
- визначення емоційного забарвлення повідомлень;
- виявлення мовних конструкцій, характерних для НЛП та інших методик маніпулювання громадською думкою;
- виявлення джерел поширення деструктивної інформації;
- виявлення шляхів поширення деструктивної інформації.

Параметри, за якими можна проводити аналіз соціальних мереж:

- граф зв’язків між користувачами;
- хештеги;
- лайки;
- репости, ретвіти;
- списки спільнот та діячів, на які користувач підписаний;
- В якості методів нейтралізації загроз доцільно використовувати наступні:
- інформування користувачів про виявлені загрози;
- спростовування виявленої дезінформації;
- блокування екстремістських матеріалів, фейкових аккаунтів, ботів;
- фільтрація спаму;
- захист лідерів думок від деструктивного впливу, своєчасне надання їм достовірної та актуальної інформації;
- своєчасне надання актуальної інформації користувачам соціальної мережі;
- підвищення освіченості людей у сфері інформаційної безпеки .

Список використаних джерел:

1. Блог российской хакерской группы Анонимный интернационал (также известен как «Шалтай- Болтай») [Електронний ресурс]. – Режим доступу: http://b0ltai.org/

2. Гармажапова А. Где живут тролли. И кто их кормит. http://www.novayagazeta.ru/politics/59889.html [Електронний ресурс]. – Режим доступу: http://www.novayagazeta.ru/politics/59889.html .

3. Тролли из Ольгино переехали в новый четырехэтажный офис на Савушкина [Електронний ресурс]. – Режим доступу: http://www.dp.ru/a/2014/10/27/ Borotsja_s_omerzeniem_mo/.

4. Кристина Лерман, Руми Жош, Таван Сурачавала Социальное заражение: исследование распространения информации с помощью пользовательских графов на ресурсах Digg та Twitter [Електронний ресурс] – Режим доступу: http://webscience.ru/details/socialnoe-zarazhenie-issledovanie-rasprostraneniyainformacii-s-pomoshchyu-polzovatelskih .