к.т.н. Молодецька-Гринчук К.В. (ЖНАЕУ)

ПІДХІД ДО ВИЯВЛЕННЯ ОРГАНІЗАЦІЙНИХ ОЗНАК ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

Сьогодні соціальні інтернет-сервіси (СІС) увійшли практично у всі сфери суспільного життя і є ефективними засобами комунікації між учасниками віртуальних спільнот, яких називають акторами. Перевагами СІС є високі темпи поширення контенту між акторами, транскордонні можливості організації акторів у групи за спільними інтересами тощо. Однак, завдяки високій популярності СІС останнім часом стали засобом проведення інформаційних операцій проти людини, суспільства, держави [1]. У [2] показано, що залежно від поставленої мети інформаційні операції у СІС розрізняються за способом реалізації. У свою чергу, досвід „гібридної війни" з Російською Федерацією показав також, що увесь спектр інформаційних операцій у СІС має ряд характерних ознак, встановлення особливостей і дослідження яких може бути використано для організації ефективної протидії [1]. З метою поширення у СІС контенту деструктивного змісту суб'єкти інформаційних операцій використовують різноманітні методи, засоби і технології інформаційного впливу, що істотно ускладнює процедури їх виявлення, оцінювання та протидію. Тому своєчасне виявлення ознак інформаційних операцій є актуальним теоретико-прикладним завданням, яке потребує свого розв'язання на шляху вирішення проблеми забезпечення інформаційної безпеки держави. Загальним недоліком існуючих досліджень щодо виявлення і оцінювання загроз інформаційній безпеці держави у СІС є відсутність комплексного підходу, який узагальнює різні ознаки інформаційних операцій. Аналіз особливостей проведених інформаційних операцій у СІС показує, що вони пов'язані з сукупністю окремих ознак, повне врахування яких в процесі функціонуванні системи інформаційної безпеки держави набуває вигляду задачі експоненціальної складності. Тому перспективним напрямком досліджень є групування ознак інформаційних операцій за спільними ознаками з подальшим їх дослідженням. Метою досліджень є розроблення підходу до виявлення організаційних ознак інформаційних операцій у СІС для підвищення ефективності функціонування системи забезпечення інформаційної безпеки людини, суспільства, держави.

Під *інформаційною операцією в СІС* у публікації будемо розуміти взаємопов'язаний комплекс інформаційних акцій з маніпулювання контентом, який цілеспрямовано здійснюється для досягнення поставленої мети шляхом прихованого впливу на акторів віртуальних спільнот і управління індивідуальною чи суспільною свідомістю. Як показав аналіз можливостей проведення держав світу, для проведення інформаційних операцій у СІС використовується спеціалізоване програмне забезпечення, яке використовує соціальних ботів для поширення заданого контенту. Результати досліджень Латвійського Центру НАТО з покращення стратегічних комунікацій [3] показали, що ознаками гібридних тролів у СІС є: коментарі публікацій інших акторів або віртуальних спільнот великої довжини; зміст таких коментарів не відповідає тематиці діалогу; прояви ворожості і агресивності; містять велику кількість граматичних помилок тощо. Однак, наявність усіх перерахованих ознак у актора СІС не доводить, що він є гібридним тролем. Внаслідок аналізу і узагальнення ознак застосування спеціалізованих інформаційних ресурсів у СІС і ботів зокрема розроблено підхід до виявлення організаційних ознак інформаційних операцій в СІС, сутність якого зводиться до такого.

Обмеження. Аналізу підлягає контент СІС текстового типу, а дослідження зображень та відео не проводиться. Вибір контенту для досягнення мети дослідження проводиться експертами або спеціальними підрозділами відповідно до вимог критичності і значущості його тематики для громадянського суспільства.

Етап 1. *Виявлення дублікатів публікацій контенту або коментарів акторів у СІС.* Для реалізації даного етапу необхідно скористатися алгоритмом, який задовольняє умову швидкодії для оперативного моніторингу СІС в інформаційному просторі. Тому серед відомих підходів до виявлення неповних дублікатів обрано алгоритм шинглів («лусочок»).

Сутність алгоритму полягає у виявленні повторів ланцюгів слів у досліджуваному контенті та наведена нижче.

Крок 1 полягає в канонізації досліджуваного текстового контенту шляхом його приведення до заданого нормального виду.

З цією метою видаляються смайли, хештеги, HTML теги, гіперпосилання, знаки пунктуації, прийменники, сполучники й інші компоненти, які не несуть змістовного навантаження контенту. В окремих випадках слід здійснювати нормалізацію іменників до однини називного відмінка. *Крок 2* призначений для розбиття нормалізованого тексту на шингли. Вибір значення довжини шингла залежить від довжини самого тексту і лежить в інтервалі [5;10].

Зростання довжини вихідного тексту вимагає збільшення цього показника. На *кроці 3* обчислюється геш шинглів текстового контенту, який порівнюється, з використанням функцій (SHA1, HAVAL, MD5, CRC32 тощо) і записується в двовимірний масив даних. Після цього випадково обирають зі збережених гешів шинглів значення для порівняння між собою. Заключний *крок 4* зводиться до розрахунку показника відповідності порівнюваного текстового контенту як співвідношення кількості гешів шинглів з однаковими значеннями до їх загальної кількості.

Етап 2. *Розрахунок показників читабельності публікацій акторів СІС.* Індекс читабельності текстів визначає складність такого контенту для сприйняття актором віртуальної спільноти. Ефективність використання такого показника для детектування деструктивних інформаційних посилів у СІС пояснюється наявністю мовного бар'єру між українськими користувачами і зарубіжними суб'єктами інформаційних операцій. В інтересах підвищення ефективності системи інформаційної безпеки держави для широкого класу задач контенту СІС доцільно скористатися автоматизованим індексом читабельності ARI, який на відміну від інших показників, забезпечує спрощення процедури дослідження складності тексту.

Етап 3. *Ведення діалогу з актором, який аналізується*. Для перевірки актора, чи є він реальною особистістю, а не ботом, доцільно задати йому запитання на деяку тематику. В більшості випадків поява відповіді на задане запитання неможлива, що пояснюється вищезгаданим мовним бар'єром ботів і реальних акторів СІС. Іноді сформульована відповідь і її ключові слова можуть не відповідати тематиці запитання.

Отже, в результаті проведених досліджень вперше розроблено підхід до виявлення організаційних ознак інформаційних операцій в СІС, який дозволяє автоматизувати процедури раннього виявлення загроз інформаційній безпеці держави у віртуальних спільнотах.

Запропонована технологія відрізняється від існуючих підходів до виявлення інформаційних операцій врахуванням функціонування спеціалізованого програмного забезпечення у СІС для впливу на інформаційний простір і акторів.

ЛІТЕРАТУРА:

1. Грищук Р. В. Основи кібернетичної безпеки : моногр. / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

2. Молодецька К. В. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах / К. В. Молодецька // Защита информации. – 2016. – Вып. 23. – С. 75 – 87.

3. „Гибридные тролли" Кремля: пропаганда в действии [Электронный ресурс]. – Режим доступа: http://trip-trial.blogspot.com/2016/05/Gibridnye-trolli-Kremlja-propaganda-v-dejstvii.html (дата обращения: 23.10.2016 р.). – Название с экрана.