УДК 004.056.5:004.738.5(045)

СОЦІАЛЬНІ БОТИ ЯК ІНСТРУМЕНТ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНОГО ВПЛИВУ НА АКТОРІВ СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСІВ

К.В. Молодецька-Гринчук
кандидат технічних наук, доцент кафедри комп'ютерних технологій і моделювання систем, Житомирський національний агроекологічний університет, м. Житомир, Україна, e-mail: kmolodetska@gmail.com

Анотація. Сучасні соціальні інтернет-сервіси є одним із найбільш популярних засобів спілкування. Проте, соціальні інтернет-сервіси можуть бути використані зловмисниками для проведення інформаційних операцій проти особистості, суспільства і держави. Досвід показує, що ефективним інструментом інформаційних впливів на акторів віртуа-

льних спільнот є соціальні боти. Узагальнення і систематизація ознак використання соціальних ботів дозволили автоматизувати процедури раннього виявлення загроз інформаційній безпеці держави у віртуальних спільнотах.

Ключові слова: соціальні інтернет-сервіси, соціальні боти, інформаційна безпека, неповні дублікати, метод шинглів, індекс читабельності.

SOCIAL BOTS AS AN INSTRUMENT OF DESTRUCTIVE INFORMATIONAL INFLUENCE ON ACTORS OF SOCIAL NETWORKING SERVICES

Kateryna Molodetska-Hrynchuk
Ph.D., Associate Professor at the Information Technologies and System Modelling sub-department, Zhytomyr National Agroecological University, Zhytomyr, Ukraine, e-mail: kmolodetska@gmail.com

Abstract. Modern social networking services are the most popular means of union tub. However, the social networking services can be used by hackers to conduct information operations against the individual, society and state. Experience shows that social bots are effective information tool impacts actors virtual communities. Generalization and systematization of signs using social-bots help to automate procedures allow early detection information security of the state in virtual communities.

Keywords: social networking services, social bots, information security, incomplete duplicates, shingles, readability index.

Вступ. Соціальні інтернет-сервіси (СІС) є найпрогресивнішим засобом масової комунікації в сучасному інформаційному суспільстві. Основним носієм інформаційних повідомлень в таких сервісах виступає контент, а споживачем та генератором такого контенту виступають актори – учасники віртуальних спільнот [1]. Досвід «Арабської весни», «Кольорових революцій», останніх подій в Європі та на сході України показує, що поширення недостовірного та упередженого контенту під час проведення інформаційних операцій в СІС призводить до асоціальної реакції акторів на нього [2-4]. Події з віртуального простору поступово трансформуються у фізичний простір, що призводить до дестабілізації діючої системи управління в державі, наростання напруги у суспільстві. 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.

Дослідження оперативної робочої групи зі стратегічних комунікацій *East StratCom Task Force* [5], яка відстежує російську пропаганду в медіапросторі європейських країн, свідчать, що Україна залишається головною ціллю їх інформаційних операцій. При цьому, одним із найбільш ефективних інструментів поширення суб'єктами інформаційних операцій деструктивного контенту є СІС, для чого використовуються спеціальні інформаційні ресурси. Так, ще в 2012 р. компанією «Ітеранет» на замовлення Служби зовнішньої розвідки Російської Федерації розпочато реалізацію проекту з «вироблення нових методик моніторингу блогосфери» [6].

Спеціалізований програмний комплекс складається з трьох модулів – «*Диспут*», «*Монитор-3*» і «*Шторм-12*». Модуль «*Диспут*» використовується для моніторингу блогосфери. Отримані на попередньому етапі дані обробляє «*Монитор-3*», завданням якого є розробка методів організації та управління в інтернеті віртуальною спільнотою залучених експертів. Дані від експертів поширюються модулем «*Шторм-12*», перед яким ставляться завдання поширення інформації у великих соціальних мережах та організації інформаційної підтримки заходів по впливу на задану масову аудиторію. Крім Російської Федерації, Міністерством оборони і спецслужбами США також активно розробляються спеціалізовані програмні та апаратні засоби для управління взаємодією акторів у СІС [7]. В 2011 р. розроблено програмний комплекс *SMISC* (Соціальні медіа в стратегічній комунікації) для відслідковування ворожої до США пропаганди і допомоги ведення контрпропаганди в *Facebook*, *Twitter*, *YouTube* та інших популярних СІС. В процесі функціонуванні *SMISC* використовуються наступні технології: лінгвістичний аналіз; аналіз трендів, настроїв, громадської думки і «культурних наративів»; автоматичне створення контенту; боти і краудсорсінг [7]. Також в 2010 р. в США впроваджено програмний комплекс *Persona Management Software* з метою створення і поширення через мережу ботів заданого контенту для формування громадської думки з актуальних питань [6, 7]. Отже, як показав аналіз можливостей проведення держав світу, для проведення інформаційних операцій у СІС використовується спеціалізоване програмне забезпечення, яке застосовує соціальних ботів для поширення заданого контенту.

Метою роботи є узагальнення і систематизація ознак застосування соціальних ботів при проведенні інформаційних операцій у СІС для підвищення ефективності системи забезпечення інформаційної безпеки людини, суспільства, держави.

Матеріал і результати досліджень. *Ботами в СІС* будемо називати спеціалізовані програмні комплекси, які призначені для автоматичного виконання функцій актора засобами інтерфейсу СІС відповідно до поставленого завдання. До таких функцій актора відносять публікації заданого контенту,

ґенерацію зв'язків з іншими акторами, додавання коментарів, гештегів і відміток тощо [6]. Залежно від задач, які ставляться перед ботами у СІС, виділяють наступні їх види.

Технічні боти – використовуються для виконання одноманітних дій у СІС, наприклад, збільшення кількості схвальних відгуків («накручення лайків») для її просування у новинній стрічці, додавання простих односкладних коментарів або повторної публікації дописів («репостів»). Такі дії справляють на акторів враження високого рівня обговорення окремої теми та її актуальності й критичності для суспільства. Також технічні боти виконують функцію соціалізації інших акторів або ботів СІС шляхом додавання їх в список «друзів» чи «послідовників» для підвищення рівня довіри до них віртуальної спільноти.

Бойові боти призначені для ведення відкладених активних дій з обліковими записами акторів СІС. Такі боти отримують доступ до персональних даних актора внаслідок утворення зв'язку («друзі», «послідовники») і в момент початку інформаційної операції залучаються для його блокування, поширення заданого контенту, негативних коментарів тощо.

Тролі представляють собою найбільш агресивний тип ботів у СІС. За семантичним ядром боти знаходять необхідні публікації у СІС, публікують образливі і ворожі коментарі, провокують безглузді суперечки серед віртуальної спільноти, створюють інформаційний фон для поширення деструктивного інформаційного посилу.

Дезінформатори представляють собою тролів, які імітують діяльність реальних акторів СІС, а в деякий момент часу публікують заданий контент для інформаційного впливу на віртуальну спільноту. У випадках успішної інформаційної операції публікації ботів-дезінформаторів поширюються у СІС, висвітлюються у ЗМІ тощо до їх спростування.

Боти-спамери застосовуються у СІС для поширення беззмістовного контенту: публікація старих публікацій або їх уривків тощо. Метою даного виду ботів є ускладнення сприйняття акторами контенту, засмічення гештегів через публікацію під ним невідповідного змісту.

Слід зазначити, що соціальні боти можуть відноситися й до інших видів, окрім розглянутих, а алгоритми їх функціонування змінюються відповідно від поставлених завдань. У ролі троля можуть виступати реальні люди, які реагують на заданий ланцюг логічних конструкцій. Така поведінка пояснюється впливом маніпулятивних технологій на свідомість акторів, а нездатність до критичного сприйняття ними контенту в СІС компенсується агресивною поведінкою і нападами на співрозмовників.

Результати досліджень Латвійського Центру НАТО з покращення стратегічних комунікацій [5] 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 [6] розроблено підхід до виявлення організаційних ознак інформаційних операцій в СІС, яка полягає в такому.

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»). Досліджуваний контент розбивається на ланцюги слів однакової довжини, для яких розраховується геш-функція. Потім проводиться порівняння розрахованих на основі геш-функції сигнатур контенту. Якщо вони співпадають, то досліджуваний контент має дублікати.

Етап 2. Розрахунок показників читабельності публікацій акторів СІС. Індекс читабельності текстів визначає складність сприйняття такого контенту акторами 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. Для широкого класу задач дослідження контенту СІС доцільно скористатися автоматизованим індексом читабельності *ARI*, який забезпечує спрощення процедури дослідження складності тексту [8].

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, що вказує на соціальних ботів.

Слід зауважити, що формування остаточних висновків про проведення інформаційних операцій в СІС досягається в результаті дослідження наявності в контенті змістовних і маніпулятивних ознак, а також оцінки актора або віртуальної спільноти, які його поширюють.

Висновки. Узагальнення і систематизація організаційних ознак інформаційних операцій у СІС і соціальних ботів зокрема, 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. Hanneman R. A. Introduction to social network methods / R. A. Hanneman, M. Riddle. – Riverside, CA: University of California, Riverside, 2005. – 322 p.

2. 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.

3. Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі / Р. В. Грищук, І. О. Канкін, В. В. Охрімчук // Захист інформації. – 2015. – Т. 17. – № 1 – С. 80–86.

4. Грищук Р. В. Синергія інформаційних та кібернетичних дій / Р. В. Грищук, Ю. Г. Даник // Труди університету. – 2014. – № 6 (127). – С. 132–143.

5. «Гибридные тролли» Кремля: пропаганда в действиии. – Режим доступа: http://trip-trial.blogspot.com/2016/05/Gibridnye-trolli-Kremlja-propaganda-v-dejstvii.html (дата обращения: 2.07.2016). – Название с экрана.

6. Барабанов И. Разведка ботом / И. Барабанов, И. Сафронов, Е. Черненко // Газета КомерсантЪ. – Режим доступа: http://kommersant.ru/doc/2009256 (дата обращения: 2.07.2016). – Название с экрана.

7. Черненко Е. Агентство национальной дезинформации США // Газета КомерсантЪ. – Режим доступа: http://kommersant.ru/doc/2009289 (дата обращения: 2.07.2016). – Название с экрана.

8. William H. DuBay. The Principles of Readability Impact Information / William H. DuBay. – Costa Mesa, California, 2004. – 73 p.