

СОЦІАЛЬНІ МЕРЕЖІ В ІНТЕРНЕТІ ЯК ІНСТРУМЕНТ ПРОСУВАННЯ “ЗАРАЖЕНОЇ” ІНФОРМАЦІЇ

Ірина Мудра

Національний університет “Львівська політехніка”,
вул. Князя Романа 1/3, 79000, м. Львів, Україна

У статті проаналізовано особливості просування “зараженої” інформації через соціальні мережі. Охарактеризовано соціальні мережі в інтернеті як важливий інструмент розповсюдження пропагандистської інформації.

Ключові слова: пропаганда, маркетинг, інформаційна війна, соціальні мережі, суспільний інтернет-майданчик, ЗМІ, мас-медіа.

Постановка проблеми. З кожним роком зростає роль соціальних мереж як інструменту просування замовної, фейкової, пропагандистської інформації. Вона поширюється швидкими темпами і збирає все нових і нових прибічників. Під “зараженою” інформацією розуміємо поширення повідомлень для введення інформаційної війни. Тому важливо зрозуміти інструменти, які використовують для просування такої інформації.

Мета статті – навести інструменти, якими просувають “заражену” інформацію. Реалізація поставленої мети передбачає такі *завдання*: аналіз особливостей функціонування соціальних мереж; виявлення інструментів, якими зацікавлена сторона розповсюджує замовну інформацію; наведення застережень аби не підпасти під вплив пропагандистських інструментів.

Аналіз актуальних досліджень. Провідними західними вченими, які займалися проблемами дослідження мережевого суспільства, є Д. Белл, М. Кастельс, А. Тоффлер, А. Турен, Дж. Гэлбрейт, Р. Ингельгарт. Низка американських учених вивчають становлення соціальних мереж, розглядають основні положення та принципи їхнього використання і прогнозують їхнє майбутнє. Це, насамперед, Джозеф Б. Вальтер, Д. Вестерман, Б. Ван Дер Хейд, С. Тонг, Л. Лангвелл, Дж. Кім, Дж. Антоні. Серед науковців вивченням мережевого розвитку суспільства займаються Р. Абдеев, С. Афанасьєв, В. Біанкі, С. Дука, В. Іноземцев, С. Дятлов, Н. Моїсєєв та ін. Низка українських та російських учених займалися дослідженням Інтернету у різних його проявах – С. Бікбаєва, А. Біккулов, В. Іванов, А. Рунов досліджували питання спілкування, комунікативного середовища та діалогу в Інтернеті. А питаннями інформаційної війни в Україні займаються такі вчені як: Г. Почепцов, Е. Паршакова, Л. Макаренко та ін.

З кожним роком усе більше користувачів всесвітньої павутини створюють аканти у соціальних мережах. Зареєстровано понад 30 мільйонів українських акантів у суспільних інтернет-майданчиках, тому можна стверджувати, що більше половини українців уже зареєстровано у соціальних мережах в інтернеті. Як свідчать дослідження Інституту

Горшеніна, принаймні серед наших співвітчизників налічується 62,4 % тих, хто заходить у них щодня [1]. Соціальні мережі в інтернеті створили для того, аби аудиторія могла між собою спілкуватися, обмінюватися відео, фотографіями. Люди приходять у мережі для того, щоб поспілкуватися один з одним, або подивитися на те, що відбувається з іншими людьми, їм цікавими. Але нині, окрім цих функцій, мережі виконують функцію інформування аудиторії, продаж потрібної інформації, товару, спонукання до певної дії (наприклад взяти участь в акції), поле для введення інформаційної війни.

Соціальна мережа в Інтернеті – це програмний сервіс, який надає “площадку” для спілкування та взаємодії людей у групі за допомогою інтернет-структури, направленої на створення співтовариств з людей, які мають спільні інтереси [3, с. 229]. Але, на нашу думку, це визначення не відображає суті соціальних мереж, тому пропонуємо своє – соціальна мережа в інтернеті – це спільнота користувачів інтернету, які об’єднані спільними інтересами і зареєстровані в межах одного ресурсу, де мають можливість обмінюватися інформацією, спілкуватися за допомогою відеозв’язку, отримувати найсвіжіші новини. Соціальні мережі також можна розглядати як будь-яке онлайнове суспільство, члени якого беруть участь в обговоренні на форумі. Соціальна мережа може виникати читачами тематичного співтовариства, створеного на будь-якому сервісі блогів.

Таке формулювання дає уявлення про соціальні мережі як: організовані і керовані інструменти спілкування на основі використання електронних інформаційних технологій (Інтернету); мережі соціального спілкування саме одновимірних за характеристиками суб’єктів, тобто, спілкування на горизонтальних рівнях організації; інформаційні технологічні комплекси, що об’єднують абонентів зі спільними інтересами і потребами та відповідною технічною підготовкою, що розширює учасників інформаційних обмінів [7, с. 19].

Нині у всесвітній павутині є більше 200 структур, які можна вважати соціальними мережами. Можна виділити такі їх види: соціальні мережі на загальну тематику, ділові мережі, спеціалізовані. Але найбільш популярні це мережі на загальну тематику. Для українських користувачів інтернету найбільш популярними є “Facebook”, “ВКонтакте”, “Однокласники”. Лідирує за кількістю облікових записів “ВКонтакте” – близько 27 мільйонів, на другому місці “Однокласники” з 11 мільйонами, замикає трійку “Facebook” – 3,2 мільйони [5].

Щоб з’ясувати причини їхньої популярності та можливості через них впливати на аудиторію потрібно проаналізувати і порівняти. Кожна соціальна мережа передбачає додавання “друзів”, публікацію та обмін “особистою” і “публічною інформацією” між учасниками, коментування публічних записів. Різні соціальні мережі хоч і володіють схожими функціями, але все ж різняться між собою за їх використанням і можливостями.

“Facebook” дає користувачам можливість вибирати власні налаштування приватності та осіб, які можуть переглядати окремі частини їхнього профілю. Налаштування приватності дає змогу користувачам контролювати, хто може бачити інформацію, якою вони діляться, а також хто може знаходити їх у пошуку. Користувачі мають можливість контролювати, якими видами інформації вони автоматично діляться із друзями. Аудиторія може унеможливити певним категоріям друзів перегляд оновлень щодо деяких

видів своєї діяльності [8]. Коли користувач довго читатиме новину, то вона автоматично транслюватиметься у стрічку новин. Крім того, при натисканні на іконку “нагадувати кожен раз, коли додається активність”, додаток буде працювати в обмеженому режимі і в читача будуть запитувати, чи можуть друзі з “Facebook” бачити в новинній стрічці інформацію про прочитання матеріалу.

У соціальній мережі “Однокласники” заборонено робити посилання на сайт “ВКонтакте”. З 2010 року керівництво соцмережі скасувало платну реєстрацію, тому нині зареєструватися може кожен бажаючий. Кожен користувач бачить імена всіх, хто заходив подивитися на його анкети. Крім того, всі публічні дії користувачів (повідомлення у форумах, додавання друзів, завантаження фотографій) відображаються в доступній іншим користувачам “Стрічці активності”. Нещодавно почала діяти платна послуга “Невидимка”, при включенні якої той, кого ви відвідували, не дізнається, хто ви. Одним із способів забезпечення приватності є створення віртуала. У стрічці активності ж залишаються тільки записи загального плану, без вказівки старих прізвища та імені. Іншим способом прибрати інформацію про відвідування є видалення облікового запису, після якого у всіх відвіданих вами користувачів згадка про факт заходу перестав відображатися [6].

“ВКонтакте” вважають клоном “Facebook”. Разом з іншими соціальними мережами “ВКонтакте” часто називають одним з найзручніших джерел для витягання інформації. Хоча для переглядання сторінок користувачів потрібна реєстрація, можливо створити підроблений акаунт і використовувати його для пошуку особистих даних. Зокрема, банківські агенти використовують соціальні мережі для пошуку боржників, а служба судових приставів розсилає повідомлення боржникам про заведення проти них справ. Крім того, через сайт за користувачами стежить ФСБ [2]. Офіційно заявляється, що користувачі можуть самі вирішувати який обсяг інформації про себе розкривати, а також мають розширені можливості для управління приватністю. Ця соціальна мережа слугує зручною платформою для шахраїв. Часто листи відправляються всьому списку контактів з проханням відправити повідомлення SMS на короткий номер для отримання доступу необхідного сайту, в такому випадку розсилка здійснюється через облікові записи користувачів, комп’ютери які заражені троянськими програмами на зразок мобільного трояна Trojan— SMS.J2ME.Konov.b. Крім того, шахраї можуть отримати доступ до комп’ютера жертви, використовуючи такі віруси, як Trojan.Win32.Sturp.eu. Часто користувачі, заразивши комп’ютер хробаками Win32.HLLW.AntiDurov, втрачали інформацію.

Порівняльна характеристика найпопулярніших соціальних мереж серед українських користувачів показала, що є багато можливостей просувати “потрібну” інформацію до користувачів. Багато створює акаунти для того, аби отримувати відібрану інформацію з різних сторінок мас-медій, а не самостійно відвідують сторінки інтернет-ЗМІ. Підписання на різні сторінки суспільних інтернет-майданчиків дає можливість вести інформаційну війну. А також ще використовують такі технології: зареєстровується одна людина, або група людей, для того, аби вербувати добровольців, наприклад у ряди ДНР і ЛНР, чи скажімо, для того, аби створити своє коло друзів, яким кожен

день надсилатимуть інформацію пропагандистського змісту чи вестимуть індивідуально дискусії, які будуть мати на меті насадження вигідної позиції.

Дослідники соціальних мереж О. С. Онищенко, В. М. Горovий, В. І. Попик у монографії “Соціальні мережі як чинник розвитку громадянського суспільства” застерігають від великого різноманіття способів інформаційних впливів, які реалізуються в інформаційно-телекомунікаційних системах або через них, можна виділити такі: поширення спеціально підібраної інформації (дезінформації). Цей спосіб впливів здійснюється у формі: розсилки e-mail (електронних листів); організації новинних груп; створення сайтів з елементами інтерактивної взаємодії їх відвідувачів (чати, онлайн-голосування); розміщення інформації на приватних за змістом веб-ресурсах: у блогах, соціальних мережах [7, с. 20].

Як відбувається просування зараженої інформації за допомогою соціальних мереж – вони заохочують цікавими, оригінальними картинками, які підписані спонукальними, або інтригуючими заголовками. Важливою особливістю інтеграції псевдо-ЗМІ в соціальні мережі є виникнення зворотного зв’язку, яке також здійснюється через Інтернет-майданчики. Читачі можуть коментувати публікації авторів та висловлювати свої думки з приводу заданої теми чи проблеми, яку описав автор. Але однин незаангажований читач губиться серед інших прозомбованих, або серед коментарів фахівців з пропаганди. Не варто забувати про те, що чим більше коментарів під матеріалом, тим частіше він з’являтиметься у стрічці новин у користувачів, а також його бачитимуть друзі по інтернет-майданчику.

Варто також зауважити, що діяльність сучасних пропагандистів є доволі професійною: вони залучають зовнішніх співробітників (аутсорсерів) – талановитих програмістів, створюють спеціальні програмні продукти (троянські програми, фальшиві антивіруси, соціальні хробаки) за допомогою яких від вашого імені надсилають “заражену” інформацію, отримують доступ до вашого комп’ютеру, електронної пошти і навіть можуть з вашого аканту спілкуватися з вашими друзями. Тому і не дивно, що соціальні мережі, на думку фахівців, перебувають серед найбільш уразливих для атак злочинців поряд з інтернет-платежами, інтернет-банкінгом; віддаленими сховищами даних і програмних застосувань; онлайн-іграми; онлайн-біржовими агенціями; сайтами за технологіями Web 2.0. [7, с. 20].

Не варто забувати про те, що соціальні мережі відіграють визначальну роль при організації і підтримці мітингів, революцій. За даними спеціалістів і признаннями офіційних учасників подій, якраз “Twitter” і “Facebook” відіграли основну роль у соціальних збуреннях, названих іще “революціями” в більшості країн арабського світу, а по-іншому – технологіями керованого, як про це надіються автори “революцій”, а насправді некерованого хаосу [7, с. 21]. Тому соціальні мережі і в Україні відіграли визначну роль у революції Гідності. Вони показали себе як одні з найкращих майданчиків для підбурювання аудиторії і закликання її до дій. Отже, соціальні мережі стають одним із найнебезпечніших інструментів для повалення чи підтримки режимів. Тому користувачам потрібно уважно ставитися до різних революційних закликів.

Проблемою сайтів багатьох соціальних мереж, зокрема, є те, що їх параметри, встановлені за замовчуванням, роблять користувачів уразливими. Ті, у кого недостат-

ньо знань у сфері інформаційної безпеки, можуть і не підозрювати про необхідність зміни налаштувань з метою власного захисту. Наприклад, за замовчуванням сайти соціальних мереж можуть дозволяти використання HTML у коментарях, що дає змогу їхнім користувачам обмінюватися гіперпосиланнями, вставляти картинки і т. д. Власне це і спрощує хакеру задачу впровадження шкідливого ПЗ, бо дає можливість вставити посилання на розташований за межами сайту шкідливий код. Для захисту від описаних Web-атак використовують такі традиційні засоби, як антивіруси, які вміють працювати в режимі реального часу, блокуючи завантаження шкідливих кодів [4, с. 2]. Захистом від описаних небезпек є дотримання таких правил: змінійте постійно паролі доступу до своїх акаунтів у соціальних мережах; використовуйте лише ліцензовані антивірусні програми, або принаймні з офіційних сайтів виробників антивірусом; не добавляйте до списку друзів тих, кого ви не знаєте; не поширюйте інформацію з невідомих джерел; ігноруйте прохання від своїх друзів поширити якусь інформацію (навіть якщо вона позитивного змісту), адже вона може містити вірус; не беріть участь у провокативних дискусіях; до кожної інформації ставтеся критично, перевіряйте її; подавайте мінімум особистої інформації.

Рекомендуємо не переглядати сторінки і публікації в соціальних мережах не від ваших друзів, незважаючи на те, що вони є у вашій інформаційній стрічці. І в ніякому разі не залишати коментарі під ними, бо інакше воно працює за правилом вірусу – розповсюджується надзвичайно швидко. Будь-яку інформацію потрібно перевіряти і критично осмислювати, бо соціальні мережі є прекрасним інструментом для введення інформаційної війни.

Список використаної літератури

1. Бурлакова В. Життя офлайн. Чому українці відмовляються від соціальних мереж [Електронний ресурс] / Валерія Бурлакова. – Режим доступу: <http://tyzhden.ua/Society/85482>
2. ВКонтакте [Електронний ресурс] // Вікіпедія. – Режим доступу: <http://uk.wikipedia.org/wiki/ВКонтакте>
3. Интернет-технологии в связях с общественностью : учеб. пособие / И. А. Быков, Д. А. Мажоров, П. А. Слуцкий, О. Г. Филатова; отв. ред. И. А. Быков, О. Г. Филатова. – СПб. : Роза мира, 2010. – 275 с.
4. Кухарська Н. Вплив соціальних мереж на корпоративну інформаційну та економічну безпеку / Наталя Кухарська, Віталій Кухарський // Захист інформації і безпека інформаційних систем. 2012. – Львів, 2012. – С. 1 – 2.
5. Мінченко О. Українці в соціальних мережах: нове дослідження від Яндексa [Електронний ресурс] / Ольга Мінченко // Watcher. – Режим доступу: <http://watcher.com.ua/2014/08/21/ukrayintsi-v-sotsialnyh-merezhah-nove-doslidzhennya-vid-yandeksa/>
6. Однокласники [Електронний ресурс] // Вікіпедія. – Режим доступу: <http://uk.wikipedia.org/wiki/Одноклассники.ru>
7. Соціальні мережі як чинник розвитку громадянського суспільства : монографія / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.]; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2013. – 220 с.
8. Facebook [Електронний ресурс] // Вікіпедія. – Режим доступу: <http://uk.wikipedia.org/wiki/Facebook>

Стаття надійшла до редколегії 12.09.14

Прийнята до друку 05.10.14.

SOCIAL NETWORKING ON THE INTERNET AS A TOOL FOR PROMOTION “INFECTED” INFORMATION

Irina Mudra

*National University “Lviv Polytechnic”,
Prince Roman Str., 1/3, 79000, Lviv, Ukraine*

Every year, the role of social networks as a tool for promoting customized, feykovoyi, Advocacy information. It spreads rapidly and collects more and more supporters. Under the “infected” understand information dissemination of messages to enter the information war. It is therefore important to understand the tools that are used to promote such information.

Social networking on the Internet – is a software service that provides a platform for communication and interaction between people in the group using the internet -structures aimed at creating communities of people with common interests. This formulation provides an overview of social networks as tools organized and managed communication through the use of electronic information technology (the Internet); Social network communication is one-dimensional characteristics for subjects, ie, communication horizontal levels of the organization; information technology systems that bring together users with similar interests and needs and appropriate training to defoliate the participants exchange information.

How is contaminated media promotion through social networks - they encourage interesting, original pictures, signed by the driving or intriguing headlines. An important feature of pseudo-media integration in social networks is the occurrence of feedback, which is also done through Internet sites. Readers can comment on publications and authors to express their views on a given topic or problem described by the author. But odnin unbiased reader lost among other prozombovanyh or comments of experts to promote. Do not forget that the more comments under the material, the more he appears in the film news users, and seen by his friends on the internet site.

Key words: promotion, marketing, information warfare, social networks, public Internet site, media, media.
