УДК 316.6:659.9

ПРАКТИКА ВИКОРИСТАННЯ МЕРЕЖІ ІНТЕРНЕТ В ІНФОРМАЦІЙНІЙ ВІЙНІ

А. С. Сінько
здобувач третього (освітньо-наукового) рівня Факультету журналістики
Науковий керівник – д.н.соц.ком., професор О. А. Мітчук

Київський столичний університет імені Бориса Грінченка,
м. Київ, Україна

У статті досліджено практику використання мережі інтернет у веденні інформаційної війни. Визначено, що об'єктом інтернет-атак дедалі частіше стають інформаційні ресурси, виведення з ладу або ускладнення функціювання яких може завдати ворожій стороні значних економічних збитків.
Ключові слова: мережа інтернет, інформаційна війна, інтернет-атака, інформаційні ресурси, економічні збитки.

The article examines the practice of using the Internet in waging information warfare. It has been determined that the object of the Internet is increasingly becoming information resources, the disabling or complicating the functioning of which can cause significant economic losses to the hostile side.
Keywords: Internet, information war, Internet attack, information resources, economic damage.

Нині інтернет дедалі активніше і масштабніше використовується в інтересах інформаційного протистояння учасників конфліктів, тобто суб'єктів інформаційних воєн. Мережа забезпечує широкі можливості для впливу на формування громадської думки, ухвалення політичних, економічних і військових рішень, на інформаційні ресурси ворога і поширення спеціально підготовленої інформації (дезінформації), а також для організації інформаційних атак (постає зручною платформою), комунікації, уможливлює миттєвий обмін інформацією, ускладнює правові аспекти ідентифікації відповідальних осіб, організацій, зрештою, країн за скоєні інформаційні злочини.

Метою роботи є дослідження практики використання мережі інтернет у веденні інформаційної війни.

Теоретичною базою дослідження послугували праці О. Запорожця, Т. Ісокової, О. Саприкіна, О. Черних тощо.

Згідно зі словниковими дефініціями, інтернет – це найбільша глобальна комп'ютерна мережа, що поєднує десятки мільйонів абонентів у понад 150 країнах світу.

Аналізуючи роль мережі в інформаційних війнах сучасності, політологиня Оксана Запорожець у розвідці «Практика використання мережі інтернет в інформаційній війні» підкреслює, що «мережа інтернет є ідеальним простором для горизонтальної пропаганди, що імітує живе неформальне спілкування і відрізняється масштабністю, безперервністю, високою швидкістю поширення інформації, використанням принципів вірусного маркетингу тощо» [1]. Дослідниця вважає, що зразками ефективного використання мережі Інтернет в інформаційній війні є інформаційні операції РФ у зв'язку з політичною кризою в Україні 2014 року. Вона розцінює інформаційну війну Росії як таку, що діє за «мережевими принципами» і характеризується «невидимістю».

Війну здійснюють безпосередньо користувачі-активісти, які «не мають прямого зв'язку з урядовими структурами і публікують нібито свої повідомлення та коментарі. У зв'язку з

цим практично неможливо або надзвичайно складно чітко визначити замовників і довести причетність до таких інформаційних операцій конкретної держави», – стверджує Оксана Запорожець [1].

Політологиня виділила декілька напрямів російської інформаційної війни у площині максимально ефективного використання можливостей і ресурсів мережі Інтернет. За її словами, в інтернет-просторі Росія і проросійські активісти діють у двох основних напрямах:

1) публікація численних коментарів в онлайн-медіа під статтями про події в Україні;

2) поширення пропагандистських повідомлень, відео та фотоматеріалів у соціальних медіа (соціальні мережі, блоги, форуми, фото і відеохостинги тощо) [1].

Відзначимо, що російські структури зорганізували публікацію гігантської кількості тенденційно забарвлених коментарів у популярних інтернет-медіа. За інформацією очільника піар-агенції «Ньюсфронт», під час виборчої кампанії президента України, а також у період збройного протистояння на Сході на популярних інтернет-сайтах, виданнях, сторінках коментарі залишають так звані «тролі», тобто анонімні інтернет-провокатори, а не реальні звичайні користувачі.

В умовах гегемонії Фейсбуку в сучасній Україні з огляду на заборону і повний занепад російських соціальних мереж, сформувалося нове поняття «бот», тобто тролі, які діють виключно у Фейсбуці. Очевидно, що всі тролі та боти отримують відповідну платню за свою діяльність. Так, Оксана Запорожець навіть наводить дані хакерської спільноти з Харкова Anonimous International, що з квітня 2014 року Росія провадить антиукраїнську інформаційну кампанію, тобто інформаційну війну, безпосередніми активізаторами й рушіями якої є 310 працівників спеціального Агентства інтернет-досліджень у Санкт-Петербурзі. Діяльність цих працівників власне полягає в розміщенні не менше 50 тенденційних і агресивних повідомлень у день на відповідних українських сайтах і в популярних соціальних мережах.

Загальна оцінка й аналіз цих коментарів засвідчує використання постійних повторюваних шаблонів: антимайданівські, антипрезидентські гасла, гасла про «гейропу», антиєвропейські заклики, захист «руського міру» та Владіміра Путіна. Йдеться, зокрема, також про популярне поняття в сучасному дискурсі «мова ворожнечі» (hate speech), застосування якої передбачає образи, цькування, навішування ярликів, прізвиська, агресивний стиль повідомлень і намагання розпалити національну, релігійну, політичну та інші види ворожнечі, апелюючи до гострих тем або подаючи нейтральну інформацію в деформованому, емоційно напруженому вигляді. Мову ворожнечі активно застосовують ЗМК, зокрема російські в боротьбі проти України.

Олена Черних наголошує, що мова ненависті – це «всі форми вираження, котрі поширюють, розпалюють, підтримують, виправдовують расову ненависть, ксенофобію, антисемітизм чи інші форми ненависті, в т.ч. нетерпимості, що виявляється у формі агресивного націоналізму, дискримінації і ворожого ставлення до меншин, іммігрантів, та осіб іноземного походження» [4]. Словосполучення «всі форми вираження» має на увазі не лише мову, тобто вербальне вираження, а й візуалізацію (картинки, фото, малюнки, скетчі тощо). Тамара Ісакова у статті «Мова ворожнечі як проблема українського інформаційного простору» наголошує, що мова ворожнечі ґрунтується на соціальних стереотипах, упередженнях і дискримінації, вона є частиною комунікації, заснованої на упередженнях і дискримінації [2, С. 90].

До прикладів руйнівної дії мови ненависті дослідниця зараховує вплив радіостанції «Радіо Тисячі Пагорбів» у Руанді на розпалювання масштабного геноциду і етнічної чистки в країні 1994 року. Ісакова вказує, що «мішенями мови ворожнечі можуть бути не тільки люди, які належать до інших етносів і рас, а й багато інших соціальних груп: інваліди, люди похилого віку, представники нетрадиційної сексуальної орієнтації тощо.

Особливою групою-мішенню можуть стати мігранти, які не належать до інших етносів і рас (рос. «понаехали», «лимита»)» [2, С. 92]. В українських реаліях у соціальних медіа, мережах та Інтернеті загалом активно побутують такі зразки національно і політично специфічної лексики мови ворожнечі, як: «вата, ватники, вышеватники, гейропа, гиркнулся, дачинг, диванные войска, диванная сотня, домбанатя, домбасс, ермолки, запрещёнка, каламойша, колорады, кровополитика, крымнаш, крымнашки, ленинопад, луганда, лугандон, няш-маш, руина, майданутые, майданята, моторолы, нанор¤оссия, намкрыш, новопендосия, отдонбасить, псакнуть, псакинг, правосеки, пидораша, реконструкторы, решеткин, свидомит, укробойцы, укроп, укропия, укры, хунта, фашизм тощо» [2, С. 94].

Пропаганда в соціальних медіа є складною для ідентифікації з огляду на масштабність антиукраїнської кампанії і залучення гігантської кількості виконавців. У соціальних мережах існує велика кількість антиукраїнських спільнот, що займаються пропагандою і дезінформацією щодо українського питання й України.

Величезну роль у дискурсі таких медіа відіграють «фейки», тобто брехливі новини, що нерідко використовують технологію сенсації й інші маніпулятивні механізми і технології й надзвичайно загострюють суспільне напруження. «Для визначення подібних «вкидань» і «зливання» інформації, інтернет-спільнота запропонувала та використовує термін фейк (від англ. fake – підробка, фальшивка) – фальсифікація, підробка, те, що виглядає як справжнє, хоча таким не є. Фейками також можуть бути облікові записи в соціальних мережах, сторінки або сайти зі змістом, схожим на основний сайт» [3, С. 75].

Багато уваги присвятив вивченню ролі інтернету в інформаційних війнах дослідник О. Саприкін. Так, у розвідці «Інтернет-ресурси як інструмент інформаційної війни й інформаційна безпека України» він пише про симулякри в межах новітньої російської «війни смислів» проти України [3, С. 73]. Відомими прикладами таких сучасних симулякрів (тобто фіктивних, вигаданих концептуальних уявлень про події, явища, дії, персон, які використовують із метою змінити громадську думку, уявлення суспільства і міжнародної спільноти в цілому про країну-агресора) є «фашисти в Києві», «звірства каральних батальйонів», «розіп'яті хлопчики», використання Україною заборонених озброєнь тощо.

Як слушно вказує Тамара Ісакова, «прояви мови ворожнечі в сепаратистських ЗМІ сьогодні поділяють на: мілітаристського характеру («хунта», «карателі»), українські слова як зневажливі («власть незалежной», «разговаривать на мове»), спотворення імен та прізвищ, а також візуальні елементи, зокрема фотомонтаж. Ці категорії трапляються як у друкованих та інтернет-виданнях, так і на сепаратистському ТБ» [2, С. 95].

Нині активне використання мережі Інтернет для ведення інформаційного протистояння зумовлено існуванням суттєвих переваг і додаткових можливостей в зіставленні з іншими традиційними формами і методами ведення війни.

Найпоширенішим напрямом використання глобальної мережі в інтересах вищезгаданого протистояння є заміна інформаційного змісту сайтів, яка полягає в підміні сторінок або їх окремих елементів в результаті злому. Такі дії робляться в основному для залучення уваги до атакуючої сторони, демонстрації своїх можливостей або є способом вираження певної політичної позиції. Крім прямої підміни сторінок, широко використовується реєстрація в пошукових системах сайтів протилежного змісту за однаковими ключовими словами, а також перенаправлення (підміну) посилань на іншу адресу, що призводить до відкриття спеціально підготовлених протилежною стороною сторінок.

Особливо виокремимо так звані «семантичні атаки», які полягають у зламі сторінок і подальшому акуратному (без помітних слідів злому) розміщенні на них завідомо неправдивої інформації. Подібним атакам, як правило, піддають часто відвідувані інформаційні сторінки, змісту яких користувачі повністю довіряють.

Ще одним напрямом використання Інтернету в інтересах інформаційного протистояння є злам або зниження ефективності функціювання структурних елементів мережі.

Найчастіше вживаними способами зниження ефективності функціювання її окремих елементів є такі.

1. «Бомбардування» мережі електронними листами. Такий спосіб вважається однією з форм «віртуальної блокади», оскільки відправка великої кількості електронних послань в одну адресу протягом короткого часу ускладнює або робить неможливим отримання (виділення) адресатом «легальних» листів із загального їх масиву, а іноді може призвести і до порушення роботи обслуговуючих серверів.

Так, під час конфлікту в Косово обидві сторони регулярно піддавали «поштовому бомбардуванню» різні урядові організації. Скоординована розсилка американськими хакерами протягом декількох днів понад 500 тис. листів призвела до повного виведення з ладу урядового сайту Югославії. Водночас представник НАТО Джимі Ши відзначав, що їх поштовий сервер тривалий час отримував щодня понад 2 тис. послань тільки від одного адресанта.

2. DOS-атаки, проведення яких, по суті, аналогічне до технології масової розсилки електронних листів одному адресату і полягає в генерації величезної кількості звернень до вибраного сайту. Це призводить до уповільнення роботи обслуговуючого сервера або повного припинення зовнішнього доступу до нього.

3. Впровадження комп'ютерних вірусів. Під час кібератак у гібридній війні використовують різні способи впровадження вірусів. Стратеги інформаційної війни розробляють спеціальні «бойові» різновиди комп'ютерних вірусів. Так, військове відомство Тайваню створило близько 1 тис. подібних вірусів, які в випадку кризової ситуації можуть вивести з ладу комп'ютерні системи КНР. Їхня здатність проривати телекомунікаційну мережу суперника на практиці перевірена в ході навчань.

Отож, розвиток мережі Інтернет в епоху глобалізації супроводжується все ширшим використанням наданих нею можливостей для здійснення інформаційного протиборства, зростанням координації, масштабів і складності дій її учасників, суб'єктів, якими є як держави або їх коаліції, так і окремі організовані групи, зокрема, екстремістські і терористичні. Об'єктом інтернет-атак дедалі частіше стають інформаційні ресурси, виведення з ладу або ускладнення функціювання яких може завдати ворожій стороні значних економічних збитків або викликати великий суспільний резонанс.

1. Запорожець О. Практика використання мережі інтернет в інформаційній війні. *Міжнародні відносини. Сер. Політичні науки*. 2014. Вип. 4. **2**. Ісакова Т. Мова ворожнечі як проблема українського інформаційного простору. *Стратегічні пріоритети. Сер. Політика*. 2016. № 4. С. 90–97. **3.** Саприкін О. Інтернет-ресурси як інструмент інформаційної війни й інформаційна безпека України. *Бібліотекознавство. Документознавство. Інформологія*. 2015. № 2. С. 72–77. **4.** Черних О. Мова ненависті, мова ворожнечі. *ACADEMIA*. URL:http://www.academia.edu/10332206/%D0%9C%D0%9E%D0%92%D0%90_%D0%92%D0%9E%D0%A0%D0%9E%D0%96%D0%9D%D0%95%D0%A7%D0%86_%D0%9C%D0%9E%D0%92%D0%90_%D0%9D%D0%95%D0%9D%D0%90%D0%92%D0%98%D0%A1%D0%A2%D0%86 (дата звернення: 04.04.2024).