Список використаних джерел

1. Будін Д. Особиста безпека в соціальних мережах. *Математичні методи, моделі та інформаційні технології у науці, освіті, економіці, виробництві:* збірник тез ІІ Всеукраїнської науково-практичної Інтернет-конференції з проблем вищої освіти і науки, м. Маріуполь, 29 квітня 2020 р. / Маріупольський державний університет; уклад. Т. В. Шабельник, О. Ф. Дяченко, А. О. Морозова, Ю. А. Лазаревська. Маріуполь: МДУ, 2020. С. 207. URL: https://repository.mu.edu.ua/jspui/bitstream/123456789/1558/1/mat_metody_2020.pdf#page=207 (дата звернення: 26.03.2024).
2. Воронцовський В. Шахрайство в інтернеті. *Фінансовий журнал ITstatti.in.ua.* 01.02.2024. URL: https://itstatti.in.ua/zarobitok-v-interneti/377-shakhrajstvo-v-interneti.html (дата звернення: 25.03.2024).
3. Кабачинський І. П. Інтернет-шахрайство – методи, ознаки та як розпізнати по телефону і в мережі. *New Voice.* 27.11.2023. URL: https://nv.ua/ukr/ukraine/events/internet-shahraystvo-metodi-oznaki-ta-yak-rozpiznati-po-telefonu-ta-v-merezhi-50362848.html (дата звернення: 20.03.2024).
4. Сабадаш В. П. Шахрайство в електронній комерції: реалії сьогодення. *Вісник Запорізького національного університету. Юридичні науки.* 2011. № 1. С. 216–220. URL: https://web.znu.edu.ua/herald/issues/2011/ur_2011_1/216-220.pdf (дата звернення: 20.03.2024).

Анотація. У роботі досліджується шахрайство у віртуальному світі. Ознаками шахрайства в соціальних мережах постають атипові моделі взаємодії, відсутність персоналізації, поширення спаму, раптові зміни в поведінці або ідентифікації облікового запису, надсилання великої кількості запитів на дружбу та прямих повідомлень від незнайомих контактів. Обачність і критичне мислення під час комунікації в соціальних мережах допоможуть виявляти та нейтралізовувати шахрайства і дадуть змогу створити безпечніше онлайнове середовище.

Ключові слова: соціальні мережі, шахрайство, девіантна поведінка, інтернет-середовище, фішинг, спам.

УДК: 004.738

Чорняк Роман Андрійович
(наук. керівник – д-р філол. наук, професор Шкіцька І. Ю.)
Західноукраїнський національний університет, м. Тернопіль

ГІБРИДНІ ВІЙНИ ЯК РІЗНОВИД ІНФОРМАЦІЙНИХ ВІЙН XXI СТ.

Гібридна війна – це форма ведення війни, що передбачає застосування політичних, воєнних, економічних, інформаційних та інших засобів для досягнення цілей. Ідеться про використання методів, стратегій і тактик, що охоплюють різні сфери впливу. Інструментами гібридних війн постають дезінформація і пропаганда, що застосовуються в медіапросторі для поширення неправдивої інформації і зміни громадської думки. Кібератаки є важливою частиною гібридної війни й мають на меті дестабілізування мережі або викрадення інформації [8].

Хоча термін «гібридна війна» виник лише у XX ст., сьогодні він активно функціонує в науковому і публіцистичному дискурсі, адже такий від війни є невід'ємним елементом конфронтації у XXI ст. Проте прояви гібридної війни супроводжують конфлікти людей із давніх часів. Незважаючи на те, що тоді розпо-

всюджувати інформацію було складно, а перевірити її правдивість практично неможливо, дезінформація була потужним засобом впливу. Прикладом цього явища були хрестові походи, для здійснення яких солдатів змушували повірити у «праведність» збройної агресії і брати участь у «священній» війні.

Поняття «гібридна війна» набуло особливої популярності після початку російської агресії проти України у 2014 році, коли Росія використала комбінацію воєнних, інформаційних і дипломатичних заходів для досягнення своїх цілей на території сусідньої країни. Війна в Україні ще раз підтвердила актуальність і необхідність вивчення гібридної війни з метою передбачення воєнного конфлікту, початком якого стала тривала інформаційна війна.

Проблема інформаційних війн привертала увагу багатьох політологів, соціологів, істориків, світових лідерів і військових експертів [7], зокрема Роджера Моландера [12], Дороти Деннінг [10], українських дослідників – Миколи Дорошка і Володимира Головченка, які написали книгу про гібридну війну проти України [5]. У книзі «Decisive Force: The new American Way of War» Ф. Хоффман також піднімає питання гібридної війни та необхідності її включення у воєнний план країн як невід'ємної частини ведення сьогоднішньої війни [11].

Для запобігання прямої конфронтації у досягненні поставлених цілей великі держави використовують свої сателіти – формально незалежні країни, фактично підпорядковані ним. Здійснюючи такі дії, агресор бажає залишатись анонімним, аби уникнути санкцій і відповідальності за дії таких підконтрольних країн. З огляду на це обираються нестабільні регіони та фінансуються терористичні угруповання для подальшої дестабілізації ситуації в регіоні або світі. Такі угруповання отримують фінансову, військову та політичну допомогу, стаючи повністю залежними від свого спонсора. Прикладом є Іран, що спонсорує йеменських хуситів, які здійснюють терористичні акти в Червоному морі, що робить найпопулярніший морський торговельний шлях небезпечним. Згадана терористична організація причетна також до неодноразового пошкодження підводних кабелів зв'язку [9].

Альтернативою неморальним діям є використання кіберпростору, що стало основним середовищем для досягнення цілей гібридної війни. Інтернет-середовище уможливлює легке втручання в політичну, культурну, економічну та інформаційну сферу країн і соціальних утворень. Кібератаки можуть бути спрямовані на різні об'єкти, включно з державними установами, критичною інфраструктурою, фінансовими системами, соціальними мережами та приватними компаніями. Ідеться про застосування різних вірусів, троянських програм, фішингу, DDoS-атак та інших методів, спрямованих на порушення функціоналу, викрадення інформації, пошкодження даних тощо.

До того ж кіберпростір є найефективнішим середовищем для розповсюдження дезінформації, маніпуляції громадською думкою та здійснення впливу на політичні процеси. Керування громадською думкою за допомогою фейків і спотворення фактів, що розпалюють ворожнечу в суспільстві, дискредитують конкретних особистостей та цілі організації, зменшують віру до влади. Залишаючись за межами воєнного конфлікту, кіберпростір у такий спосіб робить можливим негативний вплив на різні сфери діяльності країни, розхитує її єдність і стабільність.

У гібридній війні використовується широкий спектр медіаформатів для поширення думок і пропаганди, залучаються різні інформаційні канали, відео, аудіо, графіка та інші формати для досягнення цілей.

Відео, розповсюджуване на різних платформах і в соціальних мережах, є потужним засобом впливу і маніпуляції для донесення неправдивих повідомлень. Особливо контрольовані блогери передають необхідну інформацію, транслюють постановочні відео, щоб дискредитувати певну особу чи організацію. З тією ж метою використовуються дипфейки, що завдяки штучному інтелекту дають змогу згенерувати обличчя, міміку, голос та манеру мовлення політичних конкурентів [2]. Графічні матеріали також є важливим складником маніпулювання аудиторією. Це можуть бути ілюстрації, меми, афіші, реклами та інші графічні елементи, що використовуються для підсилення пропагандистських ідей або концентрації уваги в необхідному напрямі.

Найбільше середовище для здійснення впливу на масового користувача сьогодні – соціальні мережі та інтернет-платформи, що теж є простором для реалізації стратегії гібридної війни. Вони дають змогу швидко отримувати й аналізувати відповідні реакції на свої дії і водночас залишатись анонімним або прикриватися іменами відомих блогерів та свободою слова пересічних громадян.

Відносно недавно для ведення інформаційних війн стали залучати ботів – програмних агентів, що виконують завдання у мережі. Так, помітивши ключове слово чи словосполучення, автоматично чи вручну запускаються боти, наприклад, у соціальній мережі чи форумі, що під виглядом звичайних користувачів починають доводити чи захищати необхідну позицію завчасно згенерованими чи написаними повідомленнями. Це створює ажіотаж навколо теми завдяки великій активності, що поширює дезінформацію на справжніх користувачів, у яких з’явилась ця тема у вкладці «популярне» [1].

Отже, через стрімкий розвиток технологій, що дають змогу збільшити канали і способи поширення необхідних агресору ідей, спотворюють громадську думку, розпалюють конфлікти, дослідження методів і засобів ведення гібридної війни є критично важливим. Для попередження та розпізнавання агресивних дій, а також протидії їм необхідно контролювати поведінку користувачів інтернету у віртуальному просторі, створювати відповідні установи для боротьби з фейковою інформацією, підвищувати інформаційну культуру пересічних громадян, розвивати їхнє критичне мислення, виробляти навички порівняння, фільтрування та верифікації інформації. Кожен громадянин повинен усвідомлювати важливість особистої інформаційної безпеки як частину державної кібербезпеки.

Список використаних джерел

1. Березовец Т. Анексія: Острів Крим. Хроніки «гібридної війни». Київ: Брайт Стар Паблішінг, 2015. 392 с.

2. Вишняков О. Інформаційна війна з Росією: уроки виживання. ICTV (сайт). URL: fakty.ictv.ua/index/read-blog/id/1713 (дата звернення: 19.03.2024).

3. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. № 1. С. 136–141.

4. Дорошко М., Головченко В. Гібридна війна Росії проти України. Історико-політичне дослідження. Ніка-Центр. 2016. 184 с.

5. Куцька О. М. Інформаційна війна в Югославії під час проведення військової кампанії НАТО. *Військово-науковий вісник*. 2002. Вип. 4. С. 108–122.

6. Магда Є. Гібридна війна. Вижити і перемогти. Київ: Віват, 2015. 304 с.

7. Радковець Ю. Гібридна політика сучасної Росії. *Урядовий кур'єр*. 2015. 20 жовтня. URL: http://ukurier.gov.ua/uk/articles/gibridna-politika-suchasnoyi-rosiyi (дата звернення: 19.03.2024).

8. Саєнко О. Г., Степаниця С. Л. Інформаційна війна як прояв інформаційного протиборства. *Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка*. 2008. Вип. 12. С. 142–147.

9. Фісун А. О. Теоретично-категоріальне осмислення поняття «інформаційна війна» в структурі інформаційно-політичного простору. Інформаційне суспільство. 2011. Вип. 13. С. 43–48.

10. Dorothy E. R. Denning. Cryptography and Data Security. Addison-Wesley Publishing Company, Inc. 1982. 420 с.

11. Hoffaman F. G. Decisive Force: The new American Way of War. Potomac Books, Inc. 1994. 233 p.

12. Roger C. Molander. Strategic information warfare: a New Face of War. RAND, 1996. 355 с.

Анотація. У роботі акцентується на гібридних війнах як формі ведення війни, що передбачає застосування політичних, воєнних, економічних, інформаційних та інших засобів для досягнення цілей. Йдеться про використання методів, стратегій і тактик, що охоплюють різні сфери впливу.

Ключові слова: інформаційна війна, гібридна війна, соціальні мережі, конфлікт, боти, фальсифікація інформації.

УДК: 352.076

Шовдра Мар'яна Володимирівна
(наук. керівник – д-р екон. наук, професор Анісімова О. М.)
Донецький національний університет імені Василя Стуса, м. Вінниця

СТРАТЕГІЧНЕ УПРАВЛІННЯ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ СТАЛОГО РОЗВИТКУ КУЛЬТУРНОГО СЕКТОРУ МІСТА

Ідея сталого розвитку є парадигмою для сучасного та майбутнього країни. Для забезпечення досягнення цієї цілі необхідна розробка та впровадження стратегічного управління. Без належного усвідомлення важливості стратегічного управління складно реагувати на стрімкі зміни у зовнішньому середовищі та приймати обґрунтовані рішення. Неусвідомлення важливості планування може бути ознакою поганого управління в містах і країні загалом.

Мета дослідження полягає у вивченні ролі та значення стратегічного управління у контексті розвитку культурного сектору міста.

Стратегічне планування – це системний шлях до управління змінами й досягнення консенсусу в громаді [1]. Важливо зазначити, що застосування стратегічного управління у практиці діяльності органів влади розпочалося лише нещодавно. Стратегічне управління є ключовим інструментом для розвитку міста, оскіль-