ВІСНИК ПРИАЗОВСЬКОГО ДЕРЖАВНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
2022р. Серія: Технічні науки Вип. 44
p-ISSN: 2225-6733; e-ISSN: 2519-271X

122 КОМП'ЮТЕРНІ НАУКИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.738.5 **doi: 10.32782/2225-6733.44.2022.1**

© Котихова Л.Д.*

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ІТ ДЛЯ ПРОТИДІЇ ПОШИРЕННЮ РОСІЙСЬКОЇ ДЕЗІНФОРМАЦІЇ В МЕДІАПРОСТОРІ В УМОВАХ ВІЙНИ

В умовах повномасштабної війни Росії проти України важливу роль відіграє її інформаційна складова. Крім боротьби безпосередньо на фронті, зараз триває й інформаційна війна. Російська влада використовує всі можливі засоби для сіяння паніки, дезорієнтації та дезінформації серед українців. Основним джерелом поширення маніпулятивного контенту та дезінформації є соціальні мережі та інтернет-ресурси. Проблема протидії дезінформації виступає одним з найважливіших й найактуальніших сьогочасних питань. Бо для перемоги над ворогом, окрім перемоги саме армії, необхідно також одержати перемогу й на інформаційному фронті, тобто повернути свідомість частини українців у національний медіапростір. Зараз замість підходів, що розглядають проблему протидії дезінформації з точки зору інформаційної політики, більш дієвими є підходи з використанням сучасних інформаційних технологій. Для виявлення та нейтралізації загроз в інформаційному просторі з початком війни Міністерством цифрової трансформації України було створено ІТ-армію України, що є об'єднанням спеціалістів інформаційних технологій, фахівців у сфері цифрового розвитку та діджиталізації та волонтерів. Кібервійська України на своєму фронті протидіють дезінформації з боку РФ. Таким чином, ІТ-армія України відіграє важливу роль у наближенні перемоги над країною-агресором. Стаття присвячена аналізу способів використання ІТ для протидії поширенню російської пропаганди та дезінформації в українському медіапросторі в умовах війни. У статті розглянуто терміни «пропаганда», «фейк» та «дезінформація», представлено методи поширення неправдивої інформації в інформаційному просторі, описано способи протидії ворогу, що використовують воїни кіберармії.
Ключові слова: *ІТ-армія, кіберармія, пропаганда, дезінформація, фейки, війна, соціальні мережі, Інтернет.*

L.D. Kotykhova. Study of the use of IT to counter the spread of russian disinformation in the media space in war conditions. *In the face of a full-scale war of Russia against Ukraine, an important role is played by information war. The Russian authorities use all possible ways of sowing panic, disorientation and misinformation among Ukrainians. The main source of spreading manipulative content and misinformation is social networks and Internet resources. The problem of counteracting misinformation is one of the most important and relevant today's issues. Because to win the enemy, in addition to the victory of the army, it is also necessary to win on the information front, namely, to return the consciousness of part of Ukrainians to the national media space. Now, instead of approaches that consider the problem of counteracting misinformation in terms of information policy, approaches using modern information technologies are more effective. In order to identify and neutralize threats in the information space with the outbreak of the war, the Ministry of Digital Transformation of Ukraine created an IT-army of Ukraine,*

* *асистент, ДВНЗ «Приазовський державний технічний університет», м. Дніпро, kotykhova_l_d@pstu.edu*

p-ISSN: 2225-6733; e-ISSN: 2519-271X

which is an association of information technology specialists, specialists in the field of digital development and digitalization and volunteers. Ukrainian cyber military on their front counteract misinformation from the Russian Federation. Thus, the IT-army of Ukraine plays an important role in approaching the victory over the aggressor country. The article is devoted to the analysis of methods of using IT to counteract the spread of Russian misinformation in media space in war. The article examines the terms «propaganda», «fake» and «disinformation», presents the methods of spreading false information in the information space, describes the ways of countering the enemy used by the soldiers of the cyber army.
Keywords: *IT-army, cyber army, propaganda, misinformation, fakes, war, social networks, Internet.*

Постановка проблеми. З початком повномасштабного наступу країни-агресора на Україну інформаційний простір заполонила нова хвиля новин, що розповсюджують дезінформацію серед населення. Метою такого розповсюдження є дестабілізація внутрішньої ситуації в країні, створення панічних настроїв серед українців, поляризація суспільства та зміна громадської думки населення.

Російські інформаційні ресурси активно розповсюджують маніпулятивні новини, що здебільшого намагаються дискредитувати Збройні сили України в очах громадськості, а також зобразити в негативному світлі українців з територій, де ведуться активні бойові дії, та з тимчасово окупованих територій [1].

Пропаганда – це спосіб цілеспрямованого впливу та засіб змінення ставлення людей до певного явища чи події за допомогою розповсюдження спеціально підготовлених повідомлень через інформаційні ресурси [2].

Дезінформацією є спосіб впливу на людей через надання неправдивої інформації.

Фейком є інформація, що є повністю або частково недостовірною, яку видають за реальну новину.

Пропаганда та поширення дезінформації й фейків є важливими інструментами ведення інформаційної війни.

У плані оборони України та Зведеному плані територіальної оборони України від 24 лютого 2022 року вказано, що повномасштабне застосування Росією воєнної сили проти України «може супроводжуватись інформаційними кампаніями, інформаційно-психологічними операціями, кіберопераціями та спеціальними операціями проти України» [3].

Тому питання протидії інформаційним операціям Росії, а також питання збереження цілісності українського національного медіапростору, набуває особливої актуальності.

Аналіз останніх досліджень і публікацій. Сьогодні проводяться активні дослідження з ведення інформаційної війни та функціонування засобів масової інформації (ЗМІ) під час війни, бо ця проблема є надважливою.

Мельникова-Курганова О.С. під час вивчення особливостей комунікацій в блокадному Маріуполі звертає увагу на те, що «комунікація в суспільстві під час воєнних дій трансформується», а загарбники продовжують вести інформаційну боротьбу як в традиційному інформаційному просторі, так і в Інтернеті [4].

Калниболотська Є.В. називає пропаганду «некінетичним методом ведення війни у формі інформаційної атаки» [2].

Воронко О.Ю. зазначає в своїй роботі [5], що вміння протистояти пропаганді є «життєво необхідним для подальшого існування української незалежності».

Багато науковців розглядало методи протидії пропаганді та дезінформації з точки зору інформаційної політики. Однак питанню використання в цій боротьбі ІТ приділялося недостатньо уваги.

Мета дослідження – вивчення можливостей, що надають ІТ для протидії поширенню російської дезінформації в медіапросторі в умовах війни.

Виклад основного матеріалу. Росія використовує соціальні мережі та інтернет-ресурси для проведення інформаційних операцій, спрямованих проти України. Кантур О.М. зазначає, що «доступність і поширення соціальних мереж робить їх універсальним засобом для поширення дезінформації, пропаганди, мови ворожнечі тощо» [6].

p-ISSN: 2225-6733; e-ISSN: 2519-271X

Соціальні мережі та платформи, зокрема різноманітні канали, групи, чати та спільноти, стали майданчиком для ведення інформаційної війни. Дуже популярним є публікування «шок-контенту» на платформах Youtube, TikTok, Instagram та в месенджерах Viber й Telegram.

Медійні особи та відомі блогери з численною аудиторією часто за гроші підтримують у своїх дописах путінський режим. Також існують й акаунти новинних служб РФ, що дублюють у соціальним мережах пропаганду з телебачення.

Окрім цих організованих способів, до поширення дезінформації та пропаганди причетні й усі росіяни, які додають на свої сторінки посилання на фейкові дописи. Крім того, вони розпалюють суперечки та ворожнечу в коментарях під дописами та відео.

А, наприклад, в TikTok, де значну частину аудиторії становлять підлітки, створюються відео з проросійськими трендами на підтримку російської агресії.

Крім соціальних мереж значну роль у веденні інформаційної війни відіграють й сайти, що пов'язані з дезінформацією та війною в Україні. Це державні, новинні сайти, спеціалізовані інтернет-магазини з продажу військового обладнання, урядові системи та корпорації, картографічні та геоінформаційні системи тощо.

Окремою проблемою є обмеженість або взагалі відсутність правдивої інформації в зонах активних бойових дій та на тимчасово окупованих територіях. Черпак Т.В. у 2017 році розглянув у свої роботі [7] інституційні проблеми інформаційної політики на сході України, де зауважує, що «діюча влада неодмінно має протистояти цій пропаганді на тимчасово окупованих територіях, не чекаючи їх звільнення українськими військовими». Але в сучасних умовах повномасштабної війни запропоновані ним засоби щодо вдосконалення українських ЗМІ вже не можуть бути настільки ефективними, бо зараз жителі, що знаходяться в зонах бойових дій чи на тимчасово окупованих територіях, знаходяться в ізоляції від українського контенту. Через це вони є найбільш вразливими до російської пропаганди та дезінформації.

Тому тепер одним з найбільш дієвих засобів протидії пропаганді є блокування пропагандистських інтернет-ресурсів та сторінок у соціальних мережах за допомогою кіберармії.

Українські кібервійська охороняють критичну інфраструктуру та мережі в Україні, відбивають ворожі хакерські атаки та наносять власні атаки на ресурси країни-агресора, займаються кібернетичним шпіонажем, проводять інформаційні кампанії щодо захисту України, а також протидіють розповсюдженню російської дезінформації [2]. Також вони займаються публікацією та оприлюдненням секретної російської інформації, отриманої за допомогою зламів, що може допомогти в боротьбі проти загарбницької політики Росії.

ІТ-армія України захищає український кібернетичний фронт, і, хоча їх діяльність іноді не так помітна, як дії Збройних сил України, вони відіграють важливу роль у наближенні перемоги.

Українська ІТ-армія – це найпотужніша спільнота українських ІТ-фахівців, яку було створено спонтанно практично відразу після повномасштабного нападу РФ. Основним завданням ІТ-армії є створення DDoS-атак на проросійські інформаційні ресурси задля протидії окупантам. Бійці ІТ-армії здатні утримувати одночасно більше 800 цілей [8].

DDoS-атака (англ. distributed denial-of-service) – це розподілена хакерська атака, що спрямована на відключення певних сайтів. Програми для автоматизованих DDoS-атак після запуску надсилають величезну кількість запитів на зазначені цілі. Такі програми одночасно запускає велика кількість кібербійців, тому й запитів на кожен сайт-ціль надсилається така кількість, що сайти відмовляють й виходять з ладу.

ІТ-армія України складається з двох основних частин:

- волонтери, що влаштовують DDoS-атаки на різні інформаційні ресурси Росії.
- внутрішні групи, які виконують більш комплексні завдання [9].

Разом ці частини ІТ-армії відповідають за атакуючі дії для протидії поширенню дезінформації та виведення з роботи сайтів, що несуть загрозу для України. При цьому кібервоїнам потрібно бути обережними, аби не видати себе ворогам.

Окрім ІТ-спеціалістів й досвідчених хакерів в кіберармії є й новачки. Виконання кібератак різного рівня складності потребує різних навичок, до того ж, їх можна виконувати за допомогою різних варіантів програмних засобів. Тому кожен бажаючий може знайти варіант участі в кіберармії, який підійде йому за наявними в нього умовам й засобам. Й долучитися до ІТ-армії України можуть усі бажаючі, незалежно від їх навичок.

p-ISSN: 2225-6733; e-ISSN: 2519-271X

Кіберармія регулярно виконує автоматизовані системи атак на інформаційні ресурси та сервіси країни-ворога. Нові цілі та завдання формуються внутрішніми групами та керівництвом ІТ-армії. ІТ-фахівці регулярно вдосконалюють спеціальне програмне забезпечення для автоматизованих DDoS-атак, яке потім використовують й менш досвідчені кібервоїни.

Ще один засіб протидії поширенню російської дезінформації пропонує платформа «MRIYA» – синергія Кіберполіції України та волонтерів у протидії російським окупантам у медіапросторі [10].

Платформа співпрацює з підписниками, які блокують проросійські ресурси та деморалізують ворогів в соціальних мережах та платформах: Youtube, TikTok, Instagram, Viber, Telegram.

До цієї платформи також можуть приєднатися всі бажаючі. Окрім безпосереднього блокування ресурсів, кібербійці можуть й пропонувати для блокування за допомогою спеціального боту нові цілі, що займаються дезінформацією. ІТ-фахівці платформи також розробили й сервіс «MRIYA Automatic» для автоматизованої протидії російській агресії в Інтернеті.

Український кібернетичний фронт допомагають захищати хакери з усього світу. Наразі в складі кібервійськ України окрім українців є й громадяни інших країн.

Таким чином, завдяки злагодженій роботі українських ІТ-спеціалістів, Росії не вдається втілювати всі свої плани щодо ведення інформаційної війни.

Висновки

Отже, завдяки діяльності ІТ-армії України, платформи за підтримки Кіберполіції України, волонтерів та небайдужих громадян «MRIYA», а також низки інших кіберугрупувань, Росія зазнає величезної кількості кібератак та поразок своїх інформаційних кампаній.

Таким чином, українські кібервоїни:

− надійно захищають український кібернетичний фронт;
− протистоять атакам та загрозам;
− виявляють та нейтралізують російську агресію в медіапростор;
− протидіють поширенню дезінформації з боку Росії в мережі Інтернет;
− протидіють інформаційним загрозам в процесі повномасштабної війни Росії проти України;
− допомагають зберегти цілісність українського інформаційного простору.

Українські кібервійська роблять значний внесок в боротьбі з країною-агресором на інформаційному фронті.

Перелік використаних джерел:

1. Шульська Н.М. Медіаманіпуляції в умовах російсько-української війни (на прикладі локальних ЗМІ) / Н.М. Шульська, Р.С. Зінчук // Південний архів (філологічні науки). – 2022. – № 90. – С. 68-76. – Режим доступу: https://doi.org/10.32999/ksu2663-2691/2022-90-9.
2. Калниболотська Є.В. Забезпечення інформаційної безпеки України в соціальних мережах в умовах повномасштабної воєнної агресії Російської Федерації проти України / Є.В. Калниболотська. – Київ, 2022. – 69 с. – Режим доступу: https://er.nau.edu.ua/handle/NAU/55680.
3. Про введення в дію плану оборони України та Зведеного плану територіальної оборони України : Рішення Ради нац. безпеки і оборони України від 24 лютого 2022 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0033525-22#Text.
4. Мельникова-Курганова О.С. Соціальні комунікації в блокадному Маріуполі: особливості, їх види, типи комунікаторів / О.С. Мельникова-Курганова // Інформація, комунікація, суспільство: матеріали 11-ї Міжнародної наукової конференції ICS-2022. – Львів: Видавництво Львівської політехніки. – 2022. – С. 182-183.
5. Воронко О.Ю. Пропаганда 2.0 / О.Ю. Воронко // Соціально-політичні студії : наук. альманах. – 2020. – № 4. – С. 15-19.
6. Кантур О.М. Актуальні проблеми протидії інформаційним загрозам у соціальних медіа під час повномасштабного вторгнення Росії в Україну / О.М. Кантур // Наукові записки Інституту законодавства Верховної Ради України. – 2022. – № 2. – С. 102-110. – Режим доступу: https://doi.org/10.32886/instzak.2022.02.11.

7. Черпак Т.В. Інституційні проблеми інформаційної політики на сході України / Т.В. Черпак // Вісник Дніпропетровського університету. – 2017. – № 1. – С. 86-95. – (Серія: Філософія. Соціологія. Політологія).
8. Офіційний сайт боротьби проти ворога на it-фронті – IT ARMY of Ukraine [Електронний ресурс]. – Режим доступу: https://itarmy.com.ua.
9. Із кого і чого складається ІТ-армія України? Звіт Центру дослідження безпеки у Цюриху [Електронний ресурс]. – Режим доступу: https://dev.ua/news/it-armiya-ukrainy-1656515927.
10. Канал «StopRussia | MRIYA» [Електронний ресурс]. – Режим доступу: https://mriya.social/projects/channel.

References:

1. Shulska N.M., Zinchuk R.S. Mediamanipuliatsiї v umovakh rosiis'ko-ukraïns'koї viini (na prikladi lokal'nikh ZMI) [Media manipulation in the conditions of the Russian-Ukrainian war (on the example of local mass media)]. *Pivdennii arkhiv (filologichni nauki) – Southern Archive (philological sciences)*, 2022, vol. 90, pp. 68-76. **doi: 10.32999/ksu2663-2691/2022-90-9**. (Ukr.)
2. Kalnybolotska E.V. *Zabezpechennia informatsiinoї bezpeki Ukraïni v sotsial'nikh merezhakh v umovakh povno-masshtabnoї voєnnoї agresiї Rosiis'koї Federatsiї proti Ukraïni* [Ensuring information security of Ukraine in social networks in the conditions of full-scale military aggression of the Russian Federation against Ukraine]. Kyiv, 2022. 69 p. Available at: www.er.nau.edu.ua/handle/NAU/55680. (Ukr.)
3. *Rishennia Radi nats. bezpeki i oboroni Ukraïni vid 24.02.2022. Pro vvedennia v diiu planu oboroni Ukraïni ta Zvedenogo planu teritorial'noї obroni Ukraïni* (Decision of the National Council. of Security and Defense of Ukraine dated 24.02.2022. On the implementation of the Defense Plan of Ukraine and the Combined Plan of Territorial Defense of Ukraine) Available at: www.zakon.rada.gov.ua/laws/show/n0033525-22#Text (accessed 15 April 2022). (Ukr.)
4. Melnikova-Kurganova O.S. Sotsial'ni komunikatsiї v blokadnomu Mariupoli: osoblivosti, їkh vidi, tipi komunikatoriv. *Materiali 11 Mizhn. nauk. konf. «Informatsiia, komunikatsiia, suspil'stvo»* [Social communications in the blockaded Mariupol: features, their types, types of communicators. Proceedings of 11-th Int. Sci. Conf. «Information, communication, society»]. Lviv, 2022, pp. 182-183. (Ukr.)
5. Voronko O.Y. Propaganda 2.0 [Propaganda 2.0]. *Sotsial'no-politichni studiї : nauk. al'manakh – Social and political studies: sci. almanac*, 2020, no. 4, pp. 15-19. (Ukr.)
6. Kantur O.M. Aktual'ni problemi protidiї informatsiinim zagrozam u sotsial'nikh media pid chas pov-nomasshtabnogo vtorgnennia Rosiї v Ukraïnu [Current problems of countering informational threats in social media during the full-scale Russian invasion of Ukraine]. *Naukovi zapiski Institutu zakonodavstva Verkhovnoї Radi Ukraïni – Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine*, 2022, no. 2, pp. 102-110. **doi: 10.32886/instzak.2022.02.11**. (Ukr.)
7. Cherpak T.V. Institutsiini problemi informatsiinoї politiki na skhodi Ukraïni [Institutional problems of information policy in the east of Ukraine]. *Visnik Dnipropetrovs'kogo universitetu. Seriia: Filosofiia. Sotsiologiia. Politologiia – Bulletin of Dnipropetrovsky university. Series: Philosophy. Sociology. Politology*, 2017, no. 1, pp. 86-95. (Ukr.)
8. *Ofitsiinii sait borot'bi proti voroga na it-fronti – IT ARMY of Ukraine* (The official website of the fight against the enemy on the IT front - IT ARMY of Ukraine) Available at: https://itarmy.com.ua/ (accessed 10 April 2022). (Ukr.)
9. Iz kogo i chogo skladaєt'sia IT-armiia Ukraïni? Zvit Tsentru doslidzhennia bezpeki u Tsiurikhu (Who and what does the IT army of Ukraine consist of? Report of the Security Research Center in Zurich) Available at: https://dev.ua/news/it-armiya-ukrainy-1656515927 (accessed 10 May 2022). (Ukr.)
10. Kanal «StopRussia | MRIYA» (Channel «StopRussia | MRIYA») Available at: https://mriya.social/projects/channel/ (accessed 15 May 2022). (Ukr.)

Рецензент: О.І. Проніна
канд. техн. наук, доц., ДВНЗ «ПДТУ»

Стаття надійшла 20.05.2021