ІНФОРМАЦІЙНА ВІЙНА: ТЕХНОЛОГІЇ ТА ІНСТРУМЕНТИ

Вікторія Ярмолюк,
здобувач першого (бакалаврського) рівня вищої освіти,
спеціальність 061 Журналістика,
Луцький національний технічний університет
Науковий керівник –
доктор філологічних наук,
професор кафедри іноземної та української філології
Луцького національного технічного університету
Людмила Мялковська

Невід'ємними складниками інформаційної війни є *технології,* які полягають у використанні посилених інформаційних конкретизованих атак з боку країни-агресора на певну державу.

Цифрова ера, що зародилася у кінці 90-х – початку XXI ст., сприяла розвитку інформаційних маніпуляцій. Засоби масової комунікації стали поділятися на *реальні медіа* та *сміттярки* (ресурси, які імітують онлайн-медіа та підсилюють руйнацію інформаційного імунітету). Відповідно споживачі інформаційного продукту почали довіряти *сайтам-сміттяркам*, які абсолютно не несли відповідальності за те, яку інформацію вони подають, останні ж – почали тиснути на емоції людей.

Провідним інструментом ведення інформаційної війни є *моніторинг* та *добування наших даних*. Маючи інформацію, представники країни-ворога здатні використовувати її проти нас. Ця здатність підсилилася після початку повномасштабного вторгнення: українці масово поширювали інформацію, яка була у відкритому доступі, а це лише сприяло ворогам в отриманні певних геолокацій. Прикладом щодо сказаного можуть бути небезпечні листи, які надходили на електронні пошти українців, про це у грудні 2022 року інформували «Суспільне. Новини» [4]. Інтернет-видання подало поради, як захистити себе від таких повідомлень: «бути обережним перед відкриттям подібних листів чи повідомлень; звертати увагу на домен – державні органи і установи можуть надсилати листи тільки з доменів GOV.UA; не відкривати й не завантажувати підозрілі файли» [4]. То самостійно протистояти дезінформації,

яка вражає думки, погляди та переконання українців, та були ознайомлені з новітніми цифровими можливостями і засобами безпеки, що виходять за рамки традиційних методів захисту, таких як двофакторна аутентифікація чи ланцюг паролів.

Відомо, що ворог захищає власну інформацію, країна-агресор активно просуває спотворені факти про свої дії з метою формування певного образу, прагне *змінити суспільну думку*, яка могла б вплинути на розкол всередині українського суспільства.

На формування громадської думки впливає і російський медіаконтент, де висвітлюється лише та інформація, яка потрібна для країни-агресора. Проте жоден вид конфлікту не відбувається без тиску на психологічний стан людей, моральний занепад суспільства – одна із цілей ворога. Саме його застосовують росіяни до українців, використовуючи *мову ненависті* як прийом, що допоможе заполонити все інфополе. Такий метод потрібний для того, щоб скерувати дії українського населення в потрібне русло та підірвати його моральний стан.

К. Ілюк, фахівець з комунікацій у сфері безпеки і оборони, зазначає: «Умовно, якщо росіяни це адресують українській аудиторії, то завданням буде переконати перестати підтримувати армію і владу та не вірити в українську перемогу, не жертвувати гроші, бути готовими йти на поступки. В контексті російської аудиторії – це бездія. Вони закликають не робити нічого, не виходити на протести, не намагатися якимось чином критикувати режим» [1].

Країна-агресор прагне замінити реальні свідчення про все, що відбувається. Простеживши риторику російської спільноти, можна дійти висновку, що вона імітує «правдиву» інформацію. Росія намагається переконати своє суспільство у своїй всемогутності, а визнання того, що саме вона розпочала війну проти України не входить у її плани.

Українці – це народ, який протягом довгих років сформував довіру один до одного та продовжує це робити навіть попри перешкоди, які створює росія. Сьогодні українське суспільство вважає, що інтеграція абсолютно усіх людей допоможе перемогти країну-агресора. З одного боку, це правильне судження, що спрямовує рух до перемоги. А з іншого, – наше суспільство розуміє, що ін-

формаційна війна росії проти України впливає на погляди тих людей, які прихильно сприймають *ідею російського світу* [3]. Такі групи населення продовжують допомагати ворогу та розповсюджувати дезінформацію.

Інформаційна маніпуляція *в економічній сфері* також важлива для агресора, росія блокує надходження інформації щодо економічного стану України [6]. Повномасштабне вторгнення негативно вплинуло на економіку нашої держави, зокрема, скоротилося фінансування, зменшилася кількість фахівців. Для вирішення цієї проблеми потрібно сприяти поверненню спеціалістів з-за кордону, які продовжать розвивати нашу державу. Проведення дискусії із європейськими партнерами щодо залучення їх для відновлення/ розвитку економіки України теж дуже важливе.

Ще одним поширеним інструментом ведення інформаційної війни є протистояння в інтернеті, тобто – *кібервійна* [2]. Ворог хоче послабити нашу державу. Такий спосіб досягнення росіянами своєї мети у війні був поширений ще задовго до початку повномасштабного вторгнення. Саме росіяни вперше здійснили *масову кібератаку в інформаційному середовищі*, яке діє завдяки комп'ютерним системам.

Ворог використовує два прийоми у кібервійні. Перший полягає у виманюванні інформації про персональні дані користувачів мережі. Наслідком цього може стати потрапляння вірусів на пристрій користувача, що спричиняє перекидання на шкідливі сайти [7]. Другий прийом полягає у розповсюдженні програмного забезпечення, яке може нашкодити [7]. Така шкідлива система оброблення та передавання інформації стає на заваді нормальному функціонуванню пристрою.

Використання інтернет-ресурсів для застосування інформаційних й технологічних засобів – це основна мета росіян, що передбачає проникнення у систему мережі внутрішньодержавного простору України.

Завдання ворога – просування *політичних ідеологій* своєї країни нашій. Така відкрита кібервійна показала, куди потрібно рухатися, щоб протистояти цьому. Так, наша держава сформувала сильну армію в інтернеті, яка активно бореться з кібервійною. По-

перше, спеціалісти цієї сфери активно поширюють заклики про захист українського кіберпростору, це – вдала ідея, адже в результаті ми бачимо ефективність такого захисту. По-друге, тепер ми здатні здійснювати контркібератаки проти країни-агресора [2].

Аналізуючи такі дії росії, потрібно *посилювати заходи з кібербезпеки* та *медіаграмотності населення*. Для цього, по-перше, варто розвивати критичне мислення як ключовий інструмент протистояння дезінформації, що є особливо актуальним у контексті сучасних реалій, по-друге, – самостійно протистояти дезінформації, яка вражає думки, погляди та переконання українців, та бути ознайомленим із новітніми цифровими можливостями і засобами безпеки, що виходять за рамки традиційних методів захисту, таких як двофакторна аутентифікація чи ланцюг паролів.

Отже, технології та інструменти інформаційної війни – різноманітні, серед них – технології пропаганди, що спрямовані на спотворення інформації, дезорієнтацію для тих, хто її отримує, фейкові новини, фейкові медіаресурси, інформаційні технології, до яких належать кібервійни, кібератаки, зініційовані країною-агресором.

Список використаних джерел

1. Кульченко В. Новомова: як російська пропаганда намагається конструювати реальність росіян і деморалізувати українців за допомогою слів. URL :https://rpr.org.ua/news/novomova-iak-rosiyska-propahanda-namahaietsia-konstruiuvaty-realnist-rosiian-i-demoralizuvaty-ukraintsiv-za-dopomohoiu-sliv/
2. Курочко Н. Як росія та Україна воюють на кіберфронті. URL: https://www.epravda.com.ua/columns/2022/09/28/691925/
3. Російський світ (геополітика). URL: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B8%D0%B9_%D1%81%D0%B2%D1%96%D1%82_(%D0%B3%D0%B5%D0%BE%D0%BF%D0%BE%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0)
4. Собенко Н. «Як розпізнати дрон-камікадзе»: Українців попереджають про небезпечні листи нібито від ДСНС. URL: https://suspilne.media/335068-ak-rozpiznati-dron-kamikadze-ukraincev-poperedzaut-pro-nebezpecni-listi-nibito-vid-dsns/

5. Топчій О. Росія за допомогою кібератак намагається тероризувати українців – Politico. URL: https://www.unian.ua/techno/communications/rossiya-pri-pomoshchi-kiberatak-pytaetsya-terrorizirovat-ukraincev-politico-12106917.html
6. Шварц Д. Вирватись з мороку: як виживала та змінювалась економіка України за рік війни. URL: https://www.unian.ua/economics/finance/virvatis-z-moroku-yak-vizhivala-ta-zminyuvalas-ekonomika-ukrajini-za-rik-viyni-12157020.html
7. Щиголь Ю. Кібервійна: російські хакери використовують проти України два основні інструменти. URL: https://www.ukrinform.ua/rubric-technology/3478085-kibervijna-rosijski-hakeri-vikoristovuut-proti-ukraini-dva-osnovni-instrumenti.html