УДК: 321 (477) DOI 10.17721/2415-88IX.2024.92.383-397

Гончаренко Дмитро Юрійович

Приватний вищий навчальний заклад «Європейський університет» (м. Київ, Україна)

https://orcid.org/0009-0002-9387-6708

e-mail: dhoncharenko@e-u.edu.ua

СТРАТЕГІЧНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ УКРАЇНИ З РФ

Резюме

У статті досліджено актуальну проблематику — інформаційний фронт російської агресії після початку повномасштабного вторгнення військ рф в Україну. Хоча інформаційні атаки з використанням інструментарію деструктивної пропаганди з боку росії були в Україні з 2014 року, кількість таких атак значно зросла з 24 лютого 2022 року. Не дивлячись на те, що Україна почала зміцнювати свій інформаційний захист 10 років тому, все ж стало зрозуміло що кроків у цьому напрямі виявилось недостатньо. Першочергово це зумовлено нерівністю початкових ресурсів для ведення інформаційної війни. Тож Україна змушена переважно захищатись від російської інформаційної навали, зрідка завдаючи «ударів» у відповідь. Проте, навіть з такою, порівняно не великою кількістю ресурсів, інформаційний фронт російської агресії не зазнав суттєвих успіхів на даний час. Зазначимо що для перемоги в інформаційній війні треба виділяти велику кількість ресурсів протягом тривалого часу. Щоправда, на жаль, Україна не має зараз ані достатньої кількості вільних ресурсів, ані часу для досягнення беззаперечного успіху. Тож ключовим питанням лишається «що Україна може зробити зараз щоб покращити своє становище».

Для досягнення поставленої мети визначення ефективних заходів та напрямків для зміцнення національної інформаційної безпеки України — було використано комплекс загальнонаукових, логічних та емпіричних методів.

Зроблено висновки що для протидії інформаційній агресії рф необхідно вдосконалити законодавчу базу(особливо в сфері захисту персональних даних); створити потужну інформаційну інфраструктуру незалежних медіа, які можуть працювати за стандартами країн ЄС; надати повноваження

інститутам у сфері інформаційної безпеки; розвинути стратегічні комунікації та запустити кампанію з медіаграмотності і критичного мислення.

Ключові слова: інформаційна безпека, інформаційна війна, дезінформація, пропаганда, «фейкові новини».

Вступ

Після 24 лютого 2022 року для громадян України кардинально змінилась ситуація. Атаки та диверсії в інформаційному просторі тепер виступають як потужна зброя, оскільки війна розгортається не лише на полі бою, але й в інформаційні площині. Звичайне, спокійне інформаційне середовище мирного періоду руйнується і перетворюється на інформаційний фронт. Свідомість людини поглинається своєрідним інформаційний шумом через чутки, фейки та маніпуляції, які спрямовані на послаблення, і кінець-кінцем — знищення здатності до самоідентифікації та самовизначення. Ця ситуація є надзвичайно небезпечною, і може призвести до глобальної української дезорієнтації.

На даному етапі війни українське суспільство ставить перед собою завдання визначення ефективних заходів та напрямків для зміцнення національної інформаційної безпеки України. Необхідність адаптації до інформаційних загроз визначає важливість розгляду зміни характеру інформаційних загроз та необхідність адаптації стратегій безпеки до нових викликів. Це вимагає глибокого аналізу і оцінки динаміки інформаційного середовища.

Загальна проблема полягає в тому, як розробити та впровадити стратегії забезпечення інформаційної безпеки, що ефективно адаптуються до інформаційної війни, враховуючи специфічні умови та виклики, які ставляться перед Україною та Російською Федерацією.

Серед закордонних і вітчизняних дослідників обраної тематики спочатку треба виокремити загальну тему інформаційних воєн, впливу інформації на свідомість, та маніпулятивних технологій. Серед таких можемо виділити праці Р. Невсон, Е. Райхборн-К'єннеруд, Т. Гюбер, В. Немет, Ф. Аркос, В. Михаель, М. Айшервуд, Р. Волкер, Дж. Уізер, Дж. Девіс, Дж. Маккуен, А. Якобс, М. Марсілі, П. Каллен, М. Джонс, К. Пінненіемі, Х. Сміт, Дж. Аркілл, Е. Аронсон, О. Бойко, А. С. Дафф, С. Жданенко, Ю. Калиновський.

Щодо питання дезінформації та фейкових новин в сучасній науці широко використовуються праці світових учених Ф. Пратто, А. Дешена, С. Френди, Н. Діаса тощо.

Детальніше про інформаційну війну України та рф писали вітчизняні науковці після повномасштабного вторгнення 24 лютого 2022 року. Особливо цінними є праці В. Галіпчака, Л. Дунаєвої, Я. Чмира, Л. Мазуренко. Також слід відмітити низку авторів які спрямували свої зусилля на детальному огляді питання дезінформації, фейкових новин та пропаганді. Серед таких можемо

назвати С. Балана, А. Гурківську, С. Куцепала, О. Черненко, О. Новакову, А.Руднєву, Ю. Мальовану та інших.

Метою статті є дослідження та аналіз стратегічних підходів до забезпечення інформаційної безпеки в контексті інформаційної війни між Україною та рф, визначення ефективних заходів та напрямків для зміцнення національної інформаційної безпеки України.

Серед завдань які забезпечують досягнення поставленої мети можемо виділити головні. Провести огляд наукової літератури та досліджень, що стосуються тематики стратегій забезпечення інформаційної безпеки в умовах інформаційної війни. Визначити ключові терміни, такі як інформаційна безпека, інформаційна війна, пропаганда, дезінформація, фейкові новини. Дослідити актуальні виклики інформаційної війни України з рф. Визначити основні цілі та завдання стратегії забезпечення інформаційної безпеки. Провести оцінку результатів та ефективності різних стратегій, запропонованих для зміцнення інформаційної безпеки України. Сформулювати основні висновки дослідження та надати рекомендації для подальших стратегічних дій у сфері інформаційної безпеки.

Методи дослідження

Для виконання поставлених завдань були використані наступні методи: аналіз, синтез, моделювання, вивчення документів, контент-аналіз та аналіз статистичного матеріалу.

Результати дослідження

Законодавство України дає визначення, цілі, мету та завдання інформаційної безпеки. У ст. 17 Конституції України чітко вказано: «охорона суверенітету та цілісності України, економічної та інформаційної безпеки є найголовнішими функціями Української держави» [1]. Доктрина інформаційної безпеки України визначає інформаційну безпеку як важливу самостійну сферу забезпечення національної безпеки [2]. Указом Президента України № 685/2021 від 15.10.2021 р. [3] було схвалено Стратегію інформаційної безпеки. Вона врегульовує питання посилення можливостей забезпечення інформаційної безпеки України, її інформаційного простору. Доктрина покликана посилити оборону держави, забезпечити цілісність та суверенітет України. Захистити демократію в цілому, та права і свободи людини і громадянина зокрема.

Дослідниця Л. Мазуренко виділяє наступні компоненти інформаційної безпеки:

- інформаційно-технічна — додержання законності та правопорядку в кіберпросторі (захист від незаконного доступу, хакерських проникнень до комп'ютерних мереж та сайтів, комп'ютерних вірусів, незаконного використання телерадіомовних частот, радіоелектронних атак та ін.);

- інформаційно-психологічний захист психічного стану суспільства та держави від деструктивного інформаційного впливу. Авторка підкреслює, що особливо гостро він відчувається у воєнний час через велику кількість емоцій, які заважають критично оцінювати та аналізувати ситуацію, а також інформацію, яка поширюється в соціальних медіа. В цей час інформація стає ще одним видом зброї ворога [4].

Як і в будь-якій сфері можемо виділити основні проблеми інформаційної безпеки України:

- слабкий розвиток національної інформаційної інфраструктури;
- невизначеність у державній політиці щодо формування українського інформаційного простору;
- застарілість українських інформаційних технологій;
- інноваційні загрози, які вимагають ефективних рішень «тут і зараз»;
- відсутність комплексних інституцій для забезпечення системи інформаційної безпеки в державному управлінні.

Серед основних проблем інформаційної безпеки України — інформаційна війна та викривлення фактів з боку Російської Федерації. Для ефективної протидії цим труднощам необхідні комплексні заходи та оперативні рішення.

РФ щодня посилює свій інформаційний вплив на Україну, розповсюджуючи нові наративи та меседжі. До прикладу дослідниці А. Руднєва і Ю. Мальована виділяють наступні змістові зразки: розпалювання ворожнечі в Україні між владою та населенням, маніпулювання темою «зради»; заперечення української культури, приниження національних здобутків, традицій, історії, переписування історичного минулого України та нав'язування комплексу «меншовартості», абсурдних цілей вторгнення під гаслами «денацифікації» і «демілітаризації», навішування ярликів «нацизму» [5].

Умови повномасштабного вторгнення росії в Україну, яке розпочалося з 24.02.2022, призвели до посилення ролі інформаційного аспекту в національній безпеці України. Вторгнення рф на нашу територію визначається не тільки активним збройним протистоянням, але й інформаційно-психологічною боротьбою. Вона включає широкий спектр маніпулятивних, пропагандистських методів, кібератак, дезінформації, а також захоплення інформаційного простору на окупованих територіях. Особливістю сучасної війни російської федерації та України є агресивна інформаційна політика, інформаційно-психологічний тиск та операції, які зараз мають таке саме ключове значення як і безпосереднє фізичне поле бою. Це підкреслює актуальність інформаційної політики та безпеки України як ключового фактору національної єдності, збереження демократії та підтримки державного суверенітету та територіальної цілісності.

Не дивлячись на те, що український інформаційний сектор зараз знаходиться чи не в найкращому становищі за весь період незалежності України, все ж слід окреслити певні недоліки на проблеми України в інформаційні війні проти Росії.

Серед проблем український дослідник І. Лубкович виділяє:

- дефіцит інформаційної протидії органів державної влади;
- неоперативність, несвоєчасне реагування на конкретну інформацію/дезінформацію, запізніла подача власної інформації;
- низька ефективність ведення інформаційної війни та порівняно менша кількість засобів;
- недостатність матеріальних ресурсів [6].

Інформаційна війна (ІВ) — форма протиборства між різними суб'єктами (державами, неурядовими, економічними або іншими структурами), яка передбачає проведення комплексу заходів із завдання шкоди інформаційній сфері протилежної сторони та захисту власної безпеки інформаційної [7].

Заміна інформаційної реальності, примус повірити в цю нову реальність та сприйняти її є основною метою інформаційної війни. Сучасна інформаційна війна за руйнуваннями психології як суспільної так і кожної особи окремо досягає наслідків збройного протистояння. Маніпуляція масами — основне завдання інформаційної війни. Ворожі погляди та шкідливі ідеї глибоко проникають у свідомість об'єкта ведення інформаційної війни [8, с. 179].

Основною ціллю інформаційної війни є нагнітання паніки та страху, для викликання певних емоцій. Людина втрачає здатність критично оцінювати реальність, а її головною задачею стає позбавлення від страху [9]. Інструментами нагнітання страху є пропаганда, чутки, плітки, поголос, дезінформація та поширення «фейків». Пропаганда — це «прихована спроба сформувати сприйняття, розум і поведінку суспільства для досягнення корисливих цілей» [10, с. 4]. Зазвичай пропаганду поділяють на конструктивну (позитивну) та деструктивну (негативну). Позитивна пропаганда покликана виховати загальнолюдські цінності. Вона використовується в інтересах всього суспільства. На противагу їй негативна пропаганда діє в інтересах певного кола осіб. Вона ставить за мету розпалити соціальну ворожнечу, підігріти соціальні конфлікти, нав'язати деструктив у взаємовідносинах тощо [9, с. 203-207]. Подання інформації в спотвореному вигляді, часто упередженому; зміщення акценту уваги; підвищена драматичність важливих відомостей, покликана розпалити негативні емоції — основні стратегії деструктивної пропаганди.

Серед основних інформаційних загроз для України що надходили від рф ще з 2014 р. були наступні:

- для розповсюдження антиукраїнських наративів використовувались демократія та свобода слова;

- серед бізнесменів західного світу і політиків формувався проросійський естеблішмент, особливо він залучався для виправдання анексії регіонів та дискредитації санкційного впливу;

- російська православна церква в Україні формувала свій канал пропаганди для тиску на українське суспільство з середини з ціллю виокремлення від українського соціуму осіб за релігійною приналежністю;

- перехід анексованих росією територій в стан «інформаційного вакууму» для припинення розповсюдження українських наративів серед мешканців тимчасово окупованих територій;

- загальне створення атмосфери деструктиву, нестабільності, незахищеності та внутрішнього конфлікту в українському соціумі [11, с. 11-12].

Інформаційні загрози ускладнились з огляду на збільшення доступу до інформації з 2014 до 2022 року, а також швидкості її поширення. До прикладу в 2014 році тільки 4% абонентів мобільних операторів мали швидкість передачі 3G, на 2022 рік таких абонентів вже 89%. Різко зріс також відсоток користувачів інтернетом, розширились вікові рамки та швидкість мережі [12; 13]. Дезінформація мала місце поряд зі зброєю завжди, проте натепер, враховуючи вищенаведені факти, її масштаби та охоплення суттєво змінились.

Лютий 2022 року ознаменував активізацію російський інформаційних операцій проти України та Західного світу. Наративи російської кампанії з дезінформації суттєво змінились. До прикладу до повномасштабного вторгнення рф в Україну основним завдання інформаційних операцій був історичний ревізіонізм. Після—абсурд російської дезінформації піднявся на новий рівень. Серед прикладів є «нацистський уряд в Україні», «сіоністські теорії змови», «українські біологічні лабораторії з тренування бойових комах» тощо. Російська дезінформація використовується для підриву діяльності суперників, заплутування та відволікання від важливіших але менш приємних новин.

Люди схильні поширювати неправду значно швидше аніж правду. До прикладу, твіти з неправдивою інформацією на 70% частіше поширюються за правдиві; фактичні пости у мережі Facebook привертають в шість разів менше уваги ніж неправдиві [14]. Алгоритми соціальних мереж значно посилюють можливості дезінформації. Таким чином суспільство плутається, а суб'єкту дезінформування легше просувати свої наративи.

Основні зусилля російської дезінформації спрямовані на створення штучного розколу як в середині України так і між різними країнами. Ключові теми лишаються незмінними: операції чужих країн на території України (американські лабораторії, французькі найманці та британські офіцери), постійна «зрада» українського уряду, релігійне питання тощо.

У сучасній інформаційній війни дезінформація трансформувалась настільки, що виокремила ще один інструмент під назвою «фейкові новини».

Основна відмінність між дезінформацією і фейковими новинами полягає в залученості суб'єкта до розповсюдження нової інформації. Окрім традиційної зміни реальності особи, яку ставила за мету дезінформація, фейкові новини нарощують свій вплив до іншої мети — поширення перекрученої інформації із новою швидкістю. Дослідники зараз виділяють три аспекти «фейк-ньюз»:

Зміст новин. Фактично залишається незмінним порівняно з дезінформацією.

Контекст залучення та вірусності контенту.

Зміна об'єкта дезінформації на суб'єкта («жертва» довірливо сприймає інформацію і починає її поширювати, стає «співучасником») [15].

«Фейкові новини (від англ. «fake» — брехня, фальш) — це неправдива інформація, яка цілеспрямовано розповсюджується зацікавленими особами, що переслідують свої (зазвичай політичні) цілі, або бажають заробити на інтернет-трафіку» [16, с. 114]. Дослідники зазначають, що «фейкові новини можна визначити як інформаційний продукт, у складі якого частково або повністю відсутня правдива інформація» [17, с. 54]. Отже, фейкові новини — це частково викривлений або повністю неправдивий інформаційний продукт (текст, фото- та відеоматеріали, звукові повідомлення тощо), який поширюється з метою дезінформації та дестабілізації об'єкта, для якого він спродукований [15].

Відповідати на виклики інформаційної війни українська влада почала ще з 2014 року. По-перше, змінилось сприйняття росії українцями — українці почали обережніше сприймати інформацію з російських джерел. По-друге, значно виросли знання українців про методи дезінформації і, як наслідок, підвищився рівень критичного мислення. По-третє, свій розвиток отримали українські медіа, які вдосконалили свої практики та запровадили нові стандарти розповсюдження інформації. По-четверте, українська влада запровадила нові інструменти контролю за інформацією та прописала доктрину інформаційної безпеки. По-п'яте, Україна значно посилила своє міжнародне співробітництво у сфері інформаційної безпеки задля отримання додаткової підтримки та ресурсів для інформаційної війни. По-шосте, в Україні суттєво розвинулось громадянське суспільство. Відтак активісти і організації стали важливою складовою боротьби проти росії в інформаційному просторі.

Сучасна інформаційна війна, що ведеться між росією та Україну вміщує в себе найсучасніші теорії комунікації поряд з політологією, психологією та соціологією. Єдина кінцева мета — переконати людей, змінити їх думку. Кінцева ціль інформаційної війни — повне заволодіння інформаційним простором супротивника для передачі своєї інформації. Фейкові новини є одним з інструментів ведення такої війни.

На думку науковців основними заходами, що можуть запобігти поширенню фейкових новин у соціальних мережах є встановлення чітких

правил та регламенту, додаткова перевірка фактів та втручання окремого користувача [15].

Першим запобіжником розповсюдження фейкових новин є захист персональних даних, як наприклад General Data Protection Regulation в Європейському Союзі. Відтак унеможливиться підробка даних користувачів, а створення фейкових акаунтів стане дедалі складніше. Україні слід спочатку зрозуміти суть захисту персональних даних і розробити найкращу стратегію.

Другим запобіжником може виступити створення окремих груп для перевірки фактів найпоширеніших новин, а також джерел їх написання. Така робота є не найефективнішим методом боротьби із фейковими новинами, але вона може бути найшвидше реалізована.

Третім запобіжником виступає стратегія розвитку критичного мислення у користувачів інтернету. Це довготривалий процес, але цілеспрямована державна політика призведе до найкращих результатів у цій площині.

Критичне мислення — це специфічний вид розумової діяльності, результатом якої є виявлення негативних інформаційних впливів за допомогою логіки та рефлексії, що детермінує аналіз та оцінку дійсності та виведення на основі цього власного виваженого висновку [18].

Інструментарій критичного мислення надасть можливість особі протистояти цілеспрямованій деструктивній пропаганді супротивника. Уміння піддавати все сумніву, аналізувати прочитаний матеріал та рефлексувати дає можливість аргументовано спростувати тези та положення інформаційної кампанії.

Іншою відповіддю на загрози інформаційної війни виступають стратегічні комунікації, включаючи протидію дезінформації, питання пов'язані з інформаційною безпекою, а також комунікації зі ЗМІ та громадськістю.

Європейський Союз є взірцем з питань стратегічних комунікацій. За відносно невеликий період часу були прийняті такі рамкові документи як Глобальна стратегія ЄС, План дій із стратегічних комунікацій ЄС, Спільний рамковий документ з протидії гібридним загрозам. Визначення ж стратегічних комунікацій якнайкраще висвітлює Доповідь «Стратегічні комунікації ЄС у світлі протидії пропаганді» Генерального Директорату зовнішньої політики Європейського Парламенту. «Стратегічні комунікації — систематична серія сталих та послідовних заходів, що проводяться на стратегічному, операційному та тактичному рівнях, що дає змогу зрозуміти цільові аудиторії та визначити ефективні канали для сприяння й підтримки окремих типів поведінки» [11, с. 5].

Україна, в свою чергу, має своє поняття терміну «стратегічні комунікації — скоординоване і належне використання комунікативних можливостей держави — публічної дипломатії, зв'язків із громадськістю,

військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави» [2]. Таке визначення викладене у Доктрині інформаційної безпеки та Воєнній доктрині України.

Росія використовує різні потужні технології та засоби стратегічних комунікацій: фейковий контент перебігу бойових дій, намагання одноосібно привласнити бойове інформування, встановити інформаційну перевагу у зоні бойових дій, використання популярних діячів російської культури на окупованих територіях тощо. Все це використовується як психологічна зброя проти українців і державних інститутів. Відповідно головним завданням стратегічних комунікацій є зменшення і знищення інформаційної загрози для країни.

Для глобальних стратегічних комунікацій також є необхідністю завдавати превентивний удар, захоплювати ініціативу в інформаційному просторі. Розуміння необхідності та інструментарію дії в площині стратегічних комунікацій дасть можливість створювати власну інформаційну реальність.

Одним з ефективних кроків боротьби з інформаційними загрозами стало створення в Україні Центру стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України. Основною метою Центру є інформаційний захист від ворожого впливу. Основними завданнями є розробка і створення дієвого механізму та стратегії протидії дезінформації, а також об'єднання зусиль різних соціальних груп для боротьби з дезінформацією, просування українського контенту в інформаційному просторі та реагування на фейкові новини. Серед напрямків роботи є розробка стратегічних комунікацій, в тому числі українські інформаційні компанії, протидія російським інформаційним кампаніям та введення у засоби комунікації влади українських наративів; створення і розвиток онлайн-ресурсу для протидії інформаційним атаками та моніторинг російських інформаційних атак [19].

Хоча й основи демократичної держави є досить вразливими для пропаганди противника, але вони також є потужним механізмом захисту. Свобода слова, друку, зібрання, незалежність ЗМІ — виступають ключовими цінностями та мотивацією у боротьбі проти агресора.

Щоб не потрапити в тенета ворожих інформаційних ресурсів і не стати розповсюджувачем дезінформації варто дотримуватися таких принципів:

Критичне мислення. Суспільству варто вміти аналізувати та критично оцінювати контекст матеріалу. Розпізнавати пропаганду, маніпуляції та їх завдання й зміст. А також вивчити медіа, яке займається розповсюдженням ненадійного контенту.

Швидке, правдиве та об'єктивне висвітлення новин та інформації. Сьогодні в Україні існує безліч інформаційних ресурсів, які не лише забезпечують громадян інформацією, а й мають велику підтримку та довіру населення. До таких ресурсів відносяться: ЗМІ, інтернет-видання, офіційні

звернення до громадян, соціальні мережі тощо. Постійне та інформативне висвітлення подій, особливо під час війни допомагає суспільству розпізнати фейкові новини та виявити проросійський вплив. Від початку повномасштабного вторгнення Міністерство культури та інформаційної політики спільно з Офісом президента України запровадили на всіх українських ТВ-каналах телемарафон «Єдині Новини». Це один з прикладів, який дуже добре спрацював в період всеохоплюючої тривоги та наляканості. Марафон транслював і продовжує транслювати всю інформацію про вторгнення агресора, переміщення ворожої техніки загарбників, всі військові події, втрати та успіхи Збройних Сил України. Звернення Президента України та коментарі представників влади (прем'єр-міністра, міністрів, пресслужб, СБУ, ГУР МО тощо) дали чітке розуміння, що влада з народом і вся країна рішуче налаштована відбивати ворога. Потужне протистояння на інформаційному фронті дало впевненість українцям, які проживають у прифронтових зонах бойових дій про те, що вони не забуті. Тим самим це знизило рівень паніки та покращило їх моральний та психологічний стан.

Відповідальність. За створення та розповсюдження будь-якого виду дезінформації (чуток, фейків, свідомо перекрученої чи невірної інформації тощо), особливо в часи війни, варто запровадити кримінальну відповідальність.

Контроль. Для виявлення дезінформації необхідно посилити контроль за ЗМІ, а особливо за соціальними мережами та месенджерами. Швидке виявлення підроблених акаунтів дозволить розпізнавати осередки створення дезінформації та її поширення. Наприклад, «WhatsApp особливим символом маркує повідомлення, які пересилалися багато разів, що є важливою ознакою фейку». [4]

Захист інформаційного простору. Для протидії дезінформації водночас потрібно піклуватися про інформаційний простір. Війна в Україні супроводжується потужними кібератаками та DOS-атаками. Аби створити потужний захист у кіберпросторі працює Ситуаційний центр забезпечення кібербезпеки при Службі безпеки України. Центр в реальному часі проводить постійну роботу з відстеження ситуації в кіберпросторі, аналізує та керує всією інформаційною безпекою держави. Ці дії дають можливість швидко виявити, знайти, зреагувати та попередити кіберзагрози в українському інформпросторі. Також, при Національній поліції України є спеціально сформований підрозділ — Департамент кіберполіції. Він займається виявленням і знешкодженням злочинів, які створюють і поширюють різні фейки та діпфейки. Також, можна говорити, що в Україні від моменту повномасштабного вторгнення сформувався громадський рух кіберспротиву агресору. Так звана «КіберАрмія» здійснює атаки на ворога в кіберпросторі та завдають йому чималих збитків. До цієї армії входять прості люди та професійні

програмісти, айтішники. Спільними зусиллями вони зривають всі плани ворога.

Аби забезпечити інформаційну безпеку України на достатньо високому рівні потрібно спрямувати всі зусилля на підтримку інформаційної політики держави та розвиток загальної інформаційної стратегії України. Пріоритетами є: забезпечення розвитку існуючого інформаційного осередку України та повне осучаснення системи інформаційної безпеки нашої держави, ефективна реалізація української інформполітики та створення законодавчої бази з питань забезпечення інформаційної безпеки, імплементація та інтеграція України до глобалізованого європейського інформпростору.

Задля того щоб виграти інформаційну війну Україні потрібно мати сильну інформаційну стратегію, якої будуть притримуватися всі ЗМІ, інтернет-видання, соціальні мережі тощо. Вона має бути інтегрована не лише в медіапросторі, а поширеною серед всього суспільства України. Завдяки сильній інформаційній безпеці та стійкості громадян до різного виду дезінформації ми зможемо гідно протистояти інформаційній агресії росії. Лише аналітичне та критичне мислення, захист кіберпростору та співпраця з міжнародними ЗМІ забезпечить українцям інформаційну перемогу та потужний розвиток інформаційному простору нашої держави у майбутньому.

Висновки

Підсумовуючи, варто зазначити що Україна почала готуватись до інформаційної війни з рф від 2014 року. В період з 2014 до 2022 було прийнято основні документи, які регламентують інформаційну політику в Україні. Проте, не дивлячись на фундаментальну підготовку, після 24 лютого Україна стикнулась з певними проблемами в інформаційній площині. Серед основних можемо назвати застарілість інформаційних технологій, слабкий розвиток національної інформаційної інфраструктури та відсутність потужних інститутів для інформаційної безпеки сфери державного управління.

Після початку повномасштабного вторгнення рф збільшила потужності інформаційної війни в Україні. Так до звичної дезінформації, чуток, пліток і поголосу додалась значна частка фейкових новин, як нового інструменту деструктивної пропаганди.

Для протидії як старим так і новим викликам необхідно вдосконалити законодавчу базу (особливо в сфері захисту персональних даних); створити потужну інформаційну інфраструктуру незалежних медіа, які можуть працювати за стандартами країн ЄС; надати повноваження інститутам у сфері інформаційної безпеки; розвинути стратегічні комунікації та запустити кампанію з медіаграмотності і критичного мислення.

Список посилань

1. Конституція України. Чинна редакція від 01.01.2020 [Електронний ресурс]. Режим доступу до ресурсу: *https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text*
2. Доктрина інформаційної безпеки України. Затверджена Указом президента України від 25 лютого 2017 року № 47/2017 [Електронний ресурс]. Режим доступу до ресурсу: *https://zakon.rada.gov.ua/laws/show/47/2017#Text*
3. Указ Президента України № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [Електронний ресурс]. Режим доступу до ресурсу: *https://zakon.rada.gov.ua/laws/show/685/2021#Text*
4. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. Вісник Харківського національного університету імені В.Н. Каразіна; серія «Питання політології». 2022. №42. С. 50-57. *https://doi.org/10.26565/2220-8089-2022-42-08*
5. Мальована Ю., Руднєва А. Інформаційний фронт російської агресії в Україні. Вісник Львівського університету. Серія філософсько-політологічні студії. 2022. №34. С.186-192.
6. Лубкович І.М. Місце українських медій в інформаційній війні 2013-2014 рр. Наукові записки інституту журналістики. 2014. № 56. С.182-187.
7. Мирний В. В., Мороз А. С. Інформаційна війна [Електронний ресурс]. *Велика українська енциклопедія. 2022.* Режим доступу до ресурсу: https://vue.gov.ua/Інформаційна війна.
8. Шпилик С. Інформаційна війна, пропаганда та pr: такі схожі й такі різні. Галицький економічний вісник. 2014. № 4(47). С. 178-188.
9. Pratkanis A.R., Aronson E. Age of Propaganda: The Everyday Use and Abuse of Persuasion. *NY: Henry Holt and Company.* 2001.
10. Jowett G., O'Donnell V. Propaganda & persuasion. Sixth edition. *Thousand Oaks, Calif. : SAGE, 15.*, 2015.
11. Стратегічні комунікації у фокусі співробітництва Україна — ЄС — НАТО в сучасних умовах. *Київ: Центр глобалістики «Стратегія XXI».* 2019.
12. International Telecommunication Union (2021) [Електронний ресурс], *ITU Data Hub*. Retrieved from *https://datahub.itu.int/data/?e=UKR*
13. The Economist, The invasion of Ukraine is not the first social media war, but it is the most viral [Електронний ресурс]. 2022. Режим доступу до ресурсу: *https://www.economist.com/international/the-invasion-of-ukraine-is-not-the-first-social-media-war-but-it-is-the-most-viral/21808456*

14. Brown, S., MIT Sloan Research About Social Media, Misinformation, and Elections, *MIT* [Електронний ресурс]. 2020. Режим доступу до ресурсу: *https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections*
15. Батрименко О., Неліпа Д. Фейк-ньюз у соціальних мережах як маніпулятивний засіб інформаційної війни. Вісник Львівського університету. Серія філософсько-політологічні студії. 2022. № 44. С. 86-91.
16. Пятіна Д.Д., Мєлєкєсцев К. І. Фейкові новини як засібінформаційної війни. Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса. 2020 №2 (12). С. 113-116.
17. Невельська-Гордєєва О. Створення альтернативної реальності в сучасних мас-медіа. *Міждисциплінарний дискурс у дослідженні феномену соціального: збірник матеріалів міжнародної науково-практичної конференції* (28 березня 2019 р., м. Київ). С. 54-55.
18. Куцепал С. В. Критичне мислення як засіб спротиву в інформаційній війні. Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія. 2022. № 3 (54). С. 104–115.
19. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. Урядовий портал [Електронний ресурс]. *Міністерство культури та інформаційної політики України*, опубліковано 01 квітня 2021. Режим доступу до ресурсу: *https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki*

References

1. Constitution of Ukraine. *https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text* (in Ukrainian).
2. On the Doctrine of Information Security of Ukraine: Decree of the President of Ukraine No.47/2017 «On the Decision of the National Security and Defense Council of Ukraine dated December 29, 2016 «On the Doctrine of Information Security of Ukraine». *https://zakon.rada.gov.ua/laws/show/47/2017#Text (in Ukrainian)*
3. About the decision of the National Security and Defense Council of Ukraine 2021: Decree of the President of Ukraine No. 685/2021 dated October 15, 2021 «On Information Security Strategy». *https://zakon.rada.gov.ua/laws/show/685/2021#Text* [in Ukrainian].
4. Mazurenko L. (2022). Information security in the terms Russian-Ukrainian war: challenges and threats, *The Journal of V.N.Karazin Kharkiv National University, Series Issues of Political Science*, 42, p 50-57.

5. Rudneva A., Malovana Y. (2022) Information front of Russian aggression in Ukraine 2022 *Visnyk of the Lviv University. Series Philos.-Political Studies,* 44, p. 186–192.
6. Lubkovych, I. (2014). Place of Ukrainian media in the informational war of 2013–2014. *Scientific notes of the Institute of Journalism,* 56, p. 182–187.
7. Myrnyi V., Moroz A. (2023) Information war, *Great Ukrainian encyclopedia*. https://vue.gov.ua/Інформаційна війна (in Ukrainian).
8. Shpylyk S. (2014). Information warfare, propaganda and PR: so similar and so different. *Galician Economic Visnyk,* 47(4), p. 178–188.
9. Pratkanis A.R., Aronson E. (2001). Age of Propaganda: The Everyday Use and Abuse of Persuasion. *NY: Henry Holt and Company.*
10. Jowett G., O'Donnell V. (2015). Propaganda & persuasion. Sixth edition. *Thousand Oaks, Calif. : SAGE, 15.*
11. Strategic communications in the focus of Ukraine — EU — NATO cooperation in modern conditions (2019). *Kyiv: Center for Global Studies «Strategy XXI».*
12. International Telecommunication Union (2021), *ITU Data Hub*. *https://datahub.itu.int/data/?e=UKR*
13. The Economist (2022), The invasion of Ukraine is not the first social media war, but it is the most viral. *https://www.economist.com/international/the-invasion-of-ukraine-is-not-the-first-social-media-war-but-it-is-the-most-viral/21808456*
14. Brown, S. (2020), MIT Sloan Research About Social Media, Misinformation, and Elections, *MIT*. *https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections*
15. Batrymenko O., Nelipa D. (2022). Fake news in social networks as a manipulative tool of information warfare, *Visnyk of the Lviv University, series philos.-political studies*, 44, 86-91.
16. Pyatina D., Melekyestsev K. (2020) Fake news as a means of information warfare. *Visnyk of the student scientific society of Donetsk National University named after Vasyl Stus,* 2(14), p. 54-57.
17. Nevelska-Gordeeva O. (2019). Creating an alternative reality in modern mass media. *Multidisciplinary discourse and the end of a social phenomenon: mother rials of the international scientific and practical conference* (March 28, 2019, Kyiv), p. 54-55.
18. Kutsepal S. (2022). Critical Thinking as a Means of Resistance in Information War, *The Bulletin of Yaroslav Mudryi National Law University. Series:Philosophy, Philosophy of Law, Political Science, Sociology,* 3(54), p. 104-114
19. The Center for Strategic Communications and Information Security was presented. Government portal. Ministry of Culture and Information Policy of Ukraine, published on April 1, 2021. *https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki*

UDC: 321 (477) DOI 10.17721/2415-88IX.2024.92.383-387

Dmytro Honcharenko
P.H.E.I. «European University» (Kyiv, Ukraine)
https://orcid.org/0009-0002-9387-6708
e-mail: dhoncharenko@e-u.edu.ua

STRATEGIC APPROACHES TO ENSURING INFORMATION SECURITY IN THE CONDITIONS OF UKRAINE'S INFORMATION WAR WITH RUSSIA

Abstract

The article examines a topical problem — the information front of Russian aggression after the start of a full-scale invasion of Russian troops into Ukraine. Although information attacks using tools of destructive propaganda by Russia have been in Ukraine since 2014, the number of such attacks has increased significantly since February 24, 2022. Even though Ukraine began to strengthen its information protection 10 years ago, it became clear that the steps in this direction were not enough. First of all, this is caused by the inequality of the initial resources for conducting an information war. Therefore, Ukraine is mainly forced to defend itself against the Russian informational onslaught, occasionally striking back. However, even with such a relatively small amount of resources, the information front of Russian aggression has not experienced significant success so far. It should be noted that to win the information war, it is necessary to allocate a large amount of resources for a long time. However, unfortunately, Ukraine currently has neither a sufficient amount of free resources nor time to achieve indisputable success. So, the key question remains «What Ukraine can do now to improve its situation».

To achieve the set goal of determining effective measures and directions for strengthening the national information security of Ukraine, a complex of general scientific, logical, and empirical methods was used.

Conclusions were made that to counter the informational aggression of the Russian Federation, it is necessary to improve the legislative framework (especially in the field of personal data protection); to create a powerful information infrastructure of independent media that can work according to the standards of EU countries; grant authority to institutes in the field of information security; develop strategic communications and launch a media literacy and critical thinking campaign.

Keywords: information security, information war, disinformation, propaganda, «fake news».

Стаття надійшла до редакції 19.04.24