УДК 002.1-021.3:070.16]351.746.1
DOI https://doi.org/10.32782/2312-1815/2024-19-15

Михайло Микитин
ORCID:0009-0009-8286-2897

ЗНАЧЕННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

У статті досліджено важливість інформаційного простору в контексті національної безпеки держави. Основну увагу приділено різноманітним інструментам та формам дезінформації, які можуть використовуватися для впливу на державні інститути. Автором проаналізовано, як негативна пропаганда може впливати на суспільне сприйняття та маніпулювати інформаційним середовищем. Особливу увагу приділено кібератакам, що є важливим інструментом для здійснення дестабілізаційних заходів, а також їхньому потенціалу завдати шкоди національним інтересам та безпеці. У статті розглядаються механізми протидії таким загрозам та висвітлюються можливі заходи з боку держави для забезпечення інформаційної безпеки.

Додатково, стаття аналізує різні аспекти впливу інформаційних атак на суспільство, включаючи психологічний і соціальний виміри. Обговорено методи поширення дезінформації, такі як фейкові новини та маніпулятивні повідомлення в соціальних мережах, що створюють простір для хаосу та недовіри в суспільстві. Автор також звертає увагу на роль державних та недержавних акторів у проведенні таких інформаційних операцій, досліджує мотиви та цілі цих суб'єктів. У висновку статті розглядаються можливі стратегії захисту інформаційного простору, включаючи розвиток медіаграмотності серед населення, підготовку фахівців у сфері захисту інформаційної безпеки, а також покращення технічних засобів захисту від кібератак.

Ключові слова: *інформаційне середовище, дезінформація, національний сектор безпеки, кібератаки, кіберзагрози.*

Вступ. Збільшення кількості дезінформації, фейкових новин та кібератак, що покликані впливати на громадську думку, політичну стабільність та економічну безпеку, створює серйозні виклики для національної безпеки держави. Проблема полягає у визначенні та аналізі загроз, які виникають у зв'язку з використанням інформаційного простору для дестабілізації національної безпеки. Ключовим аспектом є той факт, що різноманітні інструменти та форми дезінформації, включаючи пропаганду та кібератаки, можуть суттєво впливати на суспільне сприйняття, маніпулювати громадською думкою та завдати шкоди національним інтересам.

В процесі проведення дослідження проаналізовано низку джерел та наукових праць, які відображають особливості процесів впливу на інформаційний простір як складову частину системи національної безпеки держави. Зокрема, О.Полотай у своїй статті «Інформаційна та кібербезпека: виклики та проблеми в умовах сьогодення»[5] підкреслює важливість інформаційної безпеки для прогресивного розвитку України як суверенної та демократичної держави. Володіння інформацією визначається як ключовий фактор, що пов'язаний з правами, свободами громадян та інтересами суспільства і держави. Основні проблеми забезпечення інформаційної безпеки в Україні включають засилля іноземної медіа продукції, зниження наукового потенціалу у сфері інформатизації, мовну проблему, поширення викривленої інформації в міжнародному просторі, відставання у високотехнологічних галузях, а також розголошення державної та конфіденційної інформації.

Інша дослідниця, Бойко Г. [1] розглядає вплив соціальних мереж на користувачів та суспільство. Авторка зазначає, що користувачі можуть занурюватися в стан, близький до психологічного трансу, що призводить до втрати відчуття реальності та сприйняття інформації без

критичного осмислення. Соціальні мережі використовуються як інструмент впливу та збору інформації, де користувачі, не підозрюючи, розкривають особисті дані. Також наголошується на використанні соціальних мереж для маніпулювання суспільною думкою та контролю над державами. Крім того, соціальні мережі служать каналом комунікації між громадянами та владою, підвищуючи доступність і відкритість політиків.

Цікавим є статистичне дослідження Дж. Муді про стан кібербезпеки 75 країн світу, у якому науковець визначив рейтинг найбільш захищених та найменш захищених держав. У контексті нашого дослідження цікавою є методологія оцінки рівня кіберзахищеності тієї чи іншої країни. Для визначення рівня кібербезпеки країн було використано 15 критеріїв, кожен з яких мав однакову вагу. Країни отримали бали на основі їхнього рейтингу за кожним критерієм: найменш захищеним країнам нараховувалося 100 балів, найбільш захищеним – 0 балів.

Більшість науковців своїх працях науковці зосередили увагу на віртуальній частині взаємодії українського суспільства, інформаційній безпеці та загрозах, що можуть виникнути у мережевому просторі. Зокрема, важливим є досвід Служби безпеки України [2] у контексті інформаційної безпеки і кіберзагроз та дослідження відділу цифрової безпеки компанії Microsoft, у якому розкривається масштаб та цілі російських кібератак на інфраструктуру України [13].

Мета статті полягає у всебічному дослідженні значення інформаційного простору в контексті національної безпеки держави. Це включає аналіз основних загроз, пов'язаних з дезінформацією, кіберзагрозами та іншими формами інформаційного впливу, а також визначення ролі державних та недержавних акторів у цих процесах.

Матеріал і методи дослідження. У роботі застосовано загальні та спеціальні методи наукового дослідження, які дали змогу визначити значення інформаційного простору в контексті національної безпеки держави, розкрити його структуру та вплив на безпекову ситуацію. Зокрема, контент-аналіз дозволив проаналізувати, дані, стратегії та документи, що стосуються функціонування інформаційного простору та його захисту від зовнішніх і внутрішніх загроз. Застосування системного аналізу дало можливість виявити основні елементи інформаційного простору та їхній вплив на стабільність держави. Результати аналізу вказують на необхідність удосконалення правових та організаційних механізмів захисту інформаційного простору, щоб протидіяти викликам інформаційної війни та забезпечити національну безпеку. Використання методу моделювання та прогнозування дозволило оцінити можливі сценарії розвитку інформаційних загроз і розробити рекомендації для їх попередження та зменшення їхнього впливу на державні інституції та суспільство.

Результати та обговорення. Актуальність питань забезпечення інформаційної безпеки України та відповідної протидії деструктивним інформаційним впливам зростає з кожним днем. Простір інформацій немає чітких законів та меж, що у свою чергу робить конфлікти ще більш небезпечними, а їхні наслідки можуть впливати на велику кількість цивільного населення, чому є ряд причин:

По-перше, інформаційне середовище стало доступним засобом впливу на формування громадської думки та масових настроїв. Залежно від того, які повідомлення та інформація поширюються, може виникати або зменшуватися рівень довіри до влади, соціальна напруженість, чи навіть загроза національній єдності.

По-друге, інформаційне середовище може бути використане для дестабілізації національного сектору через розповсюдження дезінформації, фейкових новин та маніпулятивної інформації. Це може призвести до загострення конфліктів, розпалювання міжнаціональних або політичних протистоянь, а також підірвати довіру до демократичних інститутів. Маніпулювання інформаційним простором з використанням кіберпростору, стали характерною рисою сучасних збройних конфліктів.

По-третє, інформаційне середовище на сьогодні активно використовується для здійснення кібератак на національний сектор, включаючи критичну інфраструктуру, електронні системи управління та комунікаційні мережі.

Традиційним інструментом впливу на інформаційне середовище були мас-медіа, за допомогою яких здійснювалася пряма або опосередкована трансляція ідей та думок між автором і отримувачем у вигляді конкретних повідомлень. Зазвичай, мас-медіа поділяються на такі групи за специфікою їхньої діяльності:

– друкована преса (газети, журнали, бюлетені та інші видання);
– аудіовізуальні медіа (радіо та телемовлення, інтернет);
– інформаційні служби (прес-служби, прес-бюро, агенції, центри громадських зв'язків тощо);
– рекламно-інформаційні носії (зовнішня реклама, візуальна реклама та інші);
– засоби масової культури (кіно, театри, концерти та інші події) [4, с. 55–56].

Важливим аспектом досліджуваного питання є різниця між дезінформацією та пропагандою. Найчастіше пропаганда та дезінформація сприймають як тотожні поняття. Однак пропаганда як така не має негативного підтексту, вона може бути як негативною, так і позитивною. А вже дезінформація завідома неправдива, маніпулятивна інформація, метою якої є нанести шкоди. Вона може проявлятися у вигляді сфабрикованого або навмисно маніпулятивного аудіовізуального контенту, навмисно створених теорій або чуток, що поширюються з метою завдати шкоди або викликати недовіру [8].

Проявами дезінформації можуть бути наступні форми:

1. Сатира або пародія: використовується без наміру завдати шкоду, швидше їх розглядають як види мистецтва. Проте, їх можна використовувати для навмисного поширення чуток, а в разі будь-яких звинувачень їх легко відкинути як щось, що не потрібно сприймати серйозно. Цю форму легко створити та поширити, може функціонувати поза початковим (гумористичним) змістом [11].

2. Неправдиві асоціації: заголовки, візуальні ефекти, підписи що не відповідають змісту. Спершу може здатися що такі асоціації (наприклад, заголовки клік-бейти) не приносять шкоди, однак у широкій перспективі така практика має потенціал підриву довіри до медіа та може сприяти поляризації суджень [17].

3. Контент який вводить в оману: використання неправдивої інформації щоб висвітлити проблему чи особу у вигідному для подавача інформації світлі. Тут йде мова про обрізання фотографій або вибіркове цитування та підбір статистичних даних для підтримки якогось аргументу. Часто можна бачити цей вид маніпулятивного контенту, не підозрюючи про це, оскільки для його виявлення потрібне дослідження та перевірка джерел, співставлення інформації з іншими джерелами [11].

4. Неправдивий контекст: при використанні даної форми дезінформації, справжні факти поширюються з неправдивою контекстною інформацією. Наприклад фотографія, котра була поширена відповідно до нового наративу. Цей вид дезінформації є доволі поширеним та небезпечним, так як поширюваний контент є справжнім, тому його важко заперечити, але в той самий час він переосмислений іншим способом.

5. Шахрайський контент: форма дезінформації при якій подавач видає себе за першоджерело при цьому використовують довіру, кінцевого споживача до певної організації, особи, бренду тощо. Багато спроб фішингу створюються саме так: використовується логотип або назва відомого бренду, щоб створити враження, доречний контент [7].

6. Маніпулятивний контент: зазвичай це стосується фотографій і відео, які змінені таким чином, що вони виглядають досить реальними, але загальний зміст справжнього контенту відрізняється від спланованого штучно [15].

7. Сфабрикований контент: новий контент на 100% неправдивий, призначений для обману та завдання шкоди. Контент повністю неправдивий, єдиною межею є уява творця такого контенту. Неозброєним оком відрізнити справжній контент від сфабрикованого вкрай складно. Якщо вам доводилося бачити «глибокі фейки», які часто можна віднести до категорії «сфабрикованого контенту», ви знаєте, наскільки сильно це впливає на нашу довіру до повідомлень, які ми бачимо [13].

Наявність «фейкових новин» і потенційно маніпулятивного контенту в ЗМІ не є чимось новим, але ця сфера значно розширилася з появою Інтернету та цифрових медіа, які стали доступними для всіх, хто має доступ до Інтернету [15].

Попри те що цифрову епоху називають «золотою ерою для журналістики» насправді вона уможливила доступ до значних масивів даних, що призвело до революційних журналістських розслідувань, нових моделей транскордонних спільних репортажів, а також доступ до скарбниць знань і різноманітних джерел за допомогою одного кліку миші. Вона також створила безпрецедентні виклики та структурні зміни в індустрії новин, що тривають і досі. Журналістика перебуває під постійним тиском, стикаючись з конвергенцією віртуальних новин тут і зараз, які підживлюють «інформаційний безлад» [10, с. 58]. Еволюційний процес зближення сфери новин із віртуальним світом відкрив нові можливості для впливу на інформаційне середовище. Такий вплив здійснюється шляхом створенням груп новин з інтерактивними елементами (онлайн-голосування, опитування, чати), блогів, розсилкою [2]. Те, як інформація подана, може сильно вплинути на наше сприйняття і рецепцію цієї інформації. Такі емоції, як страх, гордість, гнів або співчуття, запускаються в обхід логічних міркувань і викликають негайну, вісцеральну реакцію.

Соціальні мережі можуть служити інструментом для поширення негативної пропаганди, організаторів революцій і переворотів, що стає очевидним з прикладів історії та впливу на громадську думку. Вони можуть бути використані для маніпулювання та створення хаосу в суспільстві, а також для контролю над державою [3, с. 24]. Пропаганда далеко не пережиток минулого, оскільки вона продовжує розвиватися та адаптуватися до мінливого комунікаційного ландшафту. Сьогодні вона пронизує наш цифровий простір, впливаючи на наші думки та дії у дуже різний спосіб. Цифрові платформи дозволяють швидко і широко поширювати інформацію, що робить їх ідеальним інструментом для пропаганди. Ці нові платформи дозволили державним діячам, політичним партіям, екстремістським групам та іншим суб'єктам впливати на громадську думку в безпрецедентних масштабах [8].

Соціальні мережі впливають на взаємодію між державними органами та громадянами. Офіційні сторінки політиків та органів влади у соціальних мережах роблять їх більш доступними та зближують з народом. Однак, багато повідомлень на таких сторінках мають політичну спрямованість і впливають на громадську думку. Пропаганда використовує силу асоціацій, щоб пов'язати ідеї, людей або події з певними емоціями або сприйняттям. Наприклад, якщо пов'язати політичного діяча, який виступає проти, з негативними образами чи поняттями, це може викликати таке ж негативне сприйняття цього діяча [8]. Поширення дезінформації становить дедалі серйознішу загрозу для вільних і демократичних суспільств. Оскільки деякі країни борються з відступом від демократії, загрози для інформаційної екосистеми, заснованої на фактах, можуть поширюватися в геометричній прогресії і кидати виклик соціальній згуртованості та демократичному дискурсу. Це особливо актуально під час конфліктів і воєн, де інформаційне середовище стало ареною для боротьби в онлайн-просторі та стратегічних інформаційних операцій.

Водночас соціальні мережі виконують не лише роль інструменту впливу, але й служать майданчиком для збирання інформації. Користувачі, навіть не підозрюючи, передають свої дані і стають вразливими перед вторгненням у своє приватне життя. Наприклад, дослідження вчених Кембриджського університету показали, що лайки та інші активності в соціальних мережах можуть розкрити багато про користувача [2].

Значущість соціальних мереж у сучасному українському суспільстві робить їх перспективною ціллю в інформаційній війні, також і через відсутність адекватної правової бази, що б регламентувала такі форми інформаційних каналів [1]. Вони стають причиною для занепокоєння, коли використовуються обманним або зловмисним чином для маніпулювання

громадською думкою, поширення дезінформації або розпалювання ненависті. Розпізнавання цих принципів в інформації, яку ми споживаємо, є важливим першим кроком у розпізнаванні негативної пропаганди та захисту від її впливу.

Останні роки свідчать про трансформацію інформаційної безпеки, що перетікає в область кібербезпеки. Кіберзагрози розвиваються на швидкому треку, а кіберзлочини стають більш вдосконаленими, краще організованими та транснаціональними [6, с. 150]. Це пояснюється тим, що Інтернет, цифрові сервіси та інформаційно-комунікаційні технології стали неодмінною складовою глобальної економіки: від електронного документообігу та інтернет-магазинів до онлайн-банкінгу. Зі зростанням залежності бізнесу та підприємництва від використання ІКТ також зростають кіберризики і кіберзагрози, що вимагає негайної реакції для їх запобігання або вирішення, а також глибокого розуміння факторів ризику всіма зацікавленими сторонами. Система кібербезпеки повинна функціонувати в інтересах громадськості, служити як постачальникам послуг, так і їх користувачам [5, с. 3].

Найбільш використовуваними типами кібератак є:

1. Знищення – атаки, спрямовані на безповоротне видалення даних або пошкодження систем, що унеможливлює їх відновлення. Під час війни з'явилося шкідливе програмне забезпечення типу «wiper», націлене на українські державні установи та інші сектори. Ці атаки можуть мати довготривалі наслідки для організацій, якщо вони не зможуть отримати резервні копії або перезавантажити системи.

2. Виведення з ладу – атаки, що призводять до тимчасового переривання послуг або операцій через, наприклад, збільшення трафіку або шифрування систем. DDoS-атаки активно використовувалися під час конфлікту як проти українських організацій на ранніх стадіях вторгнення, так і проти російських організацій після заклику українського уряду створити ІТ-армію, а також проти державних установ у деяких країнах-членах НАТО після запровадження санкцій проти Російської Федерації. Ці атаки суттєво вплинули на зв'язність телекомунікаційних та інтернет-послуг по всій Україні, а також на доступність веб-сайтів в Україні, Російській Федерації та інших частинах світу.

3. Витік даних – атаки, що призводять до крадіжки або витоку даних або отримання даних з метою шпигунства, спостереження або розвідки [16].

У спеціальному звіті від відділу цифрової безпеки Microsoft від 27 квітня 2022 р. вказано, що на початку повномасштабного вторгнення понад 40% кібер деструктивних атак були спрямовані на організації в секторах критичної інфраструктури, які могли мати негативні наслідки другого порядку для уряду, армії, економіки та населення, економіку та людей. 32 % деструктивних інцидентів торкнулися українських урядових організацій на національному, регіональному та міському рівнях. На основі аналізу кібератак було зроблено висновок, що кібернетичні та наземні військові операції, були спрямовані на досягнення схожих цілей. Групи загроз часто націлювалися на одні й ті ж сектори або географічні місця в один і той же час. Аналіз сигналів Microsoft показує високу концентрацію зловмисної мережевої активності, яка часто збігалася з бойовими діями високої інтенсивності протягом перших шести тижнів вторгнення [13, с. 8–10].

Висновки. У сучасних економічних, політичних та військових конфліктах інформаційний простір стає важливою складовою національної безпеки держави. У цьому контексті зріс вплив та масштаби інформаційних війн, що спрямовані на забезпечення переваг у протистоянні шляхом блокування інформаційних потоків та завдання шкоди системам управління. Це може включати кібератаки, організацію протестів та терористичні акції. Інформаційно-психологічні операції вже стали невід'ємною частиною стратегій управління військами, політичними та економічними процесами. З розвитком віртуального простору конфлікти переносяться до інтернету, де вони приймають форму мережевих онлайн битв. Тому є важливими розвиток стандартів та підготовка фахівців для ефективного протистояння в інформаційній сфері. Такі заходи допомагають реагувати на виклики та компенсувати відсутність досвіду та інструментів.

Література:

1. Бойко Н. Віртуальність як частина життя сучасної людини URL: http://intkonf.org/boyko-ga-virtualnist-yak-harakteristika-zhittediyalnostilyudini-21-stolittya

2. Інформаційна та кібербезпека в сучасному світі: досвід СБУ. 2018 р. URL: https://www.6262.com.ua/news/2095459/informacijna-ta-kiberbezpeka-v-sucasnomu-sviti-dosvid-sbu

3. Ковальська Л. А. Ретроспективний потенціал інформаційних ресурсів: теоретичні аспекти. *Бібліотекознавство. Документознавство. Інформологія*. Київ, 2020. № 3. С. 23–31.

4. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ : ВІКНУ, 2016. 286 с.

5. Полотай О. Інформаційна та кібербезпека: виклики та проблеми в умовах сьогодення. Львівський державний університет безпеки життєдіяльності, м. Львів, Україна. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/11399/1/Polotai_Tezy.pdf

6. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*, ТОМ 21, № 3, липень-вересень, 2019. С. 150–157.

7. DeSantis campaign shares apparent AI-generated fake images of Trump and Fauci. URL: https://www.npr.org/2023/06/08/1181097435/desantis-campaign-shares-apparent-ai-generated-fake-images-of-trump-and-fauci

8. CounteringDisinformation.URL:https://lms.hive-mind.community/mod/scorm/player.php?a=1&currentorg=Countering_Disinformation_ORG&scoid=2

9. Hsiao E. How is propaganda designed and why is it so effective? URL: https://uxdesign.cc/how-is-propaganda-designed-and-why-is-it-so-effective-c8ae59363845

10. Ireton Ch., J. Posetti. Journalism, 'Fake News' & Disinformation. Handbook for Journalism Education and Training. United Nations Educational, Scientific and Cultural Organization, Paris, 2018. URL: https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000265552&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_upload_b32bbe07-eead-4498-8d19-f4e32251a6d7%3F_%3D265552eng.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000265552/PDF/265552eng.pdf#%5B%7B%22num%22%3A106%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C16%2C820%2C0%5D

11. Misinformation vs. Disinformation. URL: https://insights.taylorandfrancis.com/social-justice/misinformation-vs-disinformation/

12. National Strategies. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

13. Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/re4vwwd

14. The People Onscreen Are Fake. The Disinformation Is Real. URL: https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html

15. Trninić D., Kuprešanin-Vukelić A., Bokan J. Perception of "Fake News" and Potentially Manipulative Content in Digital Media – A Generational Approach. URL: https://www.mdpi.com/2075-4698/12/1/3

16. Ukraine: 100 days of war in cyberspace. URL: https://cyberpeaceinstitute.org/news/ukraine-100-days-of-war-in-cyberspace/

17. You'll be outraged at how easy it was to get you to click on this headline. URL: https://www.wired.com/2015/12/psychology-of-clickbait/ойко Г. А. Віртуальність як частина життєдіяльності людини сучасності. URL: https://www.wired.com/2015/12/psychology-of-clickbait/

References:

1. Boyko, H. A. Virtualnist yak chastyna zhyttia suchasnoi liudyny [Virtuality as part of modern human life]. URL: http://intkonf.org/boyko-ga-virtualnist-yak-harakteristika-zhittediyalnostilyudini-21-stolittya

2. Informatsiina ta kiberbezpeka v suchasnomu sviti: dosvid SBU [Information and cyber security in the modern world: experience of the SBU]. URL: https://www.6262.com.ua/news/2095459/informacijna-ta-kiberbezpeka-v-sucasnomu-sviti-dosvid-sbu

3. Kovalska, L. A. (2020). Retrospektyvnyi potentsial informatsiinykh resursiv: teoretychni aspekty. [Retrospective potential of information resources]: theoretical aspects. Library science. Documentary science. *Informatology.* Kyiv, No. 3. P. 23–31.

4. Kurban, O.V. (2016). Suchasni informatsiini viiny v merezhevomu on-lain prostori [Modern information wars in the online network space]. Kyiv : VIKNU, 286 p.

5. Polotai, O. Informatsiina ta kiberbezpeka: vyklyky ta problemy v umovakh sohodennia [Information and cyber security: challenges and problems in today's conditions]. Lviv State University of Life Safety, Lviv, Ukraine. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/11399/1/Polotai_Tezy.pdf

6. Trofymenko, O., Prokop, Yu., Loginova, N., & Zadereyko, O. (2019). Kiberbezpeka Ukrainy: analiz suchasnoho stanu [Cybersecurity of Ukraine]: analysis of the current state. *Information Protection*, Volume 21, No. 3, July-September P. 150–157.

7. DeSantis campaign shares apparent AI-generated fake images of Trump and Fauci. Retrieved from https://www.npr.org/2023/06/08/1181097435/desantis-campaign-shares-apparent-ai-generated-fake-images-of-trump-and-fauci

8. Countering Disinformation. Retrieved from https://lms.hive-mind.community/mod/scorm/player.php?a=1&currentorg=Countering_Disinformation_ORG&scoid=2

9. Hsiao, E. How is propaganda designed and why is it so effective? Retrieved from https://uxdesign.cc/how-is-propaganda-designed-and-why-is-it-so-effective-c8ae59363845

10. Ireton, Ch., & J. Posetti. (2018). Journalism, 'Fake News' &Disinformation. Handbook for Journalism Education and Training. United Nations Educational, Scientific and Cultural Organization, Paris, Retrieved from https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000265552&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_upload_b32bbe07-eead-4498-8d19-f4e32251a6d7%3F_%3D265552eng.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000265552/PDF/265552eng.pdf#%5B%7B%22num%22%3A106%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C16%2C820%2C0%5D

11. Misinformation vs. Disinformation. Retrieved from https://insights.taylorandfrancis.com/social-justice/misinformation-vs-disinformation/

12. National Strategies. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

13. Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/re4vwwd

14. The People Onscreen Are Fake. The Disinformation Is Real. Retrieved from https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html

15. Trninić, D., Kuprešanin-Vukelić, A., & Bokan, J. Perception of "Fake News" and Potentially Manipulative Content in Digital Media—A Generational Approach. Retrieved from https://www.mdpi.com/2075-4698/12/1/3

16. Ukraine: 100 days of war in cyberspace. Retrieved from https://cyberpeaceinstitute.org/news/ukraine-100-days-of-war-in-cyberspace/

17. You'll be outraged at how easy it was to get you to click on this headline. Retrieved from https://www.wired.com/2015/12/psychology-of-clickbait/

Mykhailo Mykytyn. The importance of information space in the context of national security of the state

The article examines the importance of the information space in the context of national security. The focus is on various tools and forms of disinformation that can be used to influence state institutions. The author analyzes how negative propaganda can influence public perception and manipulate the information environment. Particular attention is paid to cyberattacks, which are an important tool for destabilizing measures, as well as their potential to harm national interests and security. The article discusses the mechanisms for countering such threats and highlights possible measures by the state to ensure information security.

In addition, the article analyzes various aspects of the impact of information attacks on society, including psychological and social dimensions. It discusses the methods of spreading disinformation, such as fake news and manipulative messages on social media, which create space for chaos and distrust in society. The author also draws attention to the role of state and non-state actors in conducting such information operations, and explores the motives and goals of these actors. The article concludes with a discussion of possible strategies

for protecting the information space, including the development of media literacy among the population, training of specialists in the field of information security, and improvement of technical means of protection against cyberattacks.

Key words: *information environment, disinformation, national security sector, cyberattacks, cyber threats.*

Відомості про автора:
Михайло Микитин – аспірант за спеціальністю 052 – Політологія,
Прикарпатський національний університет імені Василя Стефаника.