КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.738.5:329.09.5 DOI: https://doi.org/10.32515/2664-262X.2024.10(41).2.23-31

О.П. Доренський, доц., канд. техн. наук, **О.С. Улічев**, канд. техн. наук,
К. О. Задорожний, студ., **А.С. Коваленко**, асист., **Г.М. Дрєєва**, докторка філософії
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
e-mail: dorenskyiop@kntu.kr.ua, askin79@gmail.com, kostazadoroznij9@gmail.com

Концептуальна модель системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони

Стаття присвячена актуальній проблемі підвищення ефективності інформаційного протиборства, що провадиться координаційним органом з питань національної безпеки і оборони – центром протидії дезінформації. Мета дослідження досягається шляхом синтезу концептуальної моделі системи інформаційного протиборства, її застосування для виявлення слабких сторін та, як наслідок, удосконалення механізму протидії дезінформації задля підвищення його ефективності: забезпечення результативності протидії деструктивним інформаційним впливам і кампаніям, пропаганді, реальним та потенційним загрозам в інформаційній сфері, запобігання спробам маніпулювання громадською думкою. Означений механізм протидії передбачає реагування на дезінформаційні атаки шляхом створення і розміщення відповідного контенту в соціальних мережах. Водночас, результати цього дослідження показали недостатність охоплення цільової авдиторії WhatsApp, що формує недолік системи інформаційного протиборства, який закономірно чинить негативний вплив на ефективність її функціонування. Крім того, аналіз результатів цього дослідження показала важливість удосконалення процесу детектування інформаційних загроз за допомогою ІТ, технологій і інструментів штучного інтелекту, що дозволить скоротити час виявлення загроз в інформаційній сфері. Тож, для вирішення існуючої проблеми пропонується розширити охоплення цільової авдиторії WhatsApp для підвищення ефективності протидії дезінформації координаційним органом, який бере участь в забезпеченні інформаційної безпеки держави, виявленні й протидії дезінформації, пропаганді, деструктивним інфовпливам, проводить заходи для протидії загрозам в інформаційній сфері. Практична цінність отриманих результатів полягає в зменшенні вразливості органів виконавчої влади та суспільства до інформаційних загроз шляхом підвищення ефективності протидії дезінформації. Водночас, це забезпечить зростання результативності інформаційного реагування на дезінформацію, пропаганду і маніпуляції, скоротить час між появою фейкової інформації та її виявленням, забезпечить ефективне оцінювання ризиків для національної безпеки в інформаційному просторі.

інформаційна безпека, дезінформація, інформаційне протиборство, концептуальна модель, соціальні мережі, WhatsApp

Постановка проблеми. Дезінформація є реальною загрозою безпеки громадянина, суспільства і держави, що закономірно робить протидію їй пріоритетним завданням системи забезпечення національної безпеки України. Зростання кількості та масштабів дезінформаційних кампаній, спрямованих на українське суспільство, вкрай гостро актуалізує потребу в максимально ефективній системі інформаційного протиборства. Проблемою, яка виникає у протидії дезінформації та інформаційної безпеки, є відсутність комплексного підходу, концентрації на простих інструментах виявлення фейків та ігнорування системних рішень, що впливатимуть на весь спектр соціальної взаємодії в суспільстві. Система протидії дезінформації може охоплювати значний спектр ситуацій: не тільки дописи ботів у соціальних мережах або оплачені ворогами держави медіасюжети. Якщо поставитися до дезінформації ширше, як до

сукупності негативних впливів на інститути або індивідів, то інструменти протидії постануть в іншому світлі, як значно масштабніші від простих спростувань чи лекцій з медіаграмотності [1]. Отже, гостро стоїть задача забезпечення ефективності діяльності інституцій, які відповідають за протидію дезінформації, – координаційного органу з питань національної безпеки і оборони, до функцій якого належить участь в забезпеченні інформаційної безпеки держави, виявлення й протидія дезінформації, пропаганді, деструктивним інформаційним впливам, проведення заходів для протидії реальним і потенційним загрозам в інформаційній сфері, запобігання спробам маніпулювання громадською думкою [2].

Аналіз останніх досліджень і публікацій [3-7,12-16] показав широке коло прогалин та недоліків в ефективності системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони, ґрунтовні дослідження проведені Інститутом інформаційної безпеки. В праці [4] аргументовано неефективність моніторингу ЦПД і запропонована матриця загроз, яка має сконцентрувати діяльність винятково на актуальних цілях: «в ній весь масив зібраних повідомлень поділяється на теми за «контентними» ознаками; тем не може бути більше шести-семи, оскільки для обслуговування кожної з них потрібна, щонайменше, окрема людина; до таких тем може бути віднесено війну та окупацію, історію; культуру (мову), дії та реформи держави, міжнародні відносини України; кожна тема складається із загальних дворівневих наративів» [4]; також є меседжі – неправдиві повідомлення. Деякі дослідження також вказують на проблему раннього виявлення фейків та повільного реагування на дезінформацію, пропонують автоматичну детекцію, за допомогою якої можна досягнути головної цілі – скорочення часу між розповсюдженням фейку і урядовим реагуванням на нього. Водночас, у дослідженнях не розглядається питання забезпечення стійкої ефективності системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони в частині покриття цільової авдиторії у соціальних мережах задля реалізації результативної протидії дезінформації, пропаганді, деструктивним інформаційним впливам, маніпулюванню суспільною думкою. Разом з тим, у працях [14-15] запропоновані підходи підвищення ефективності протидії пропаганді сепаратизму і антиукраїнської ідеології в соціальних мережах.

Постановка мети й задач дослідження. У контексті забезпечення інформаційно-психологічної безпеки Центр протидії дезінформації при Раді національної безпеки і оборони (ЦПД) в Україні є ключовою державною інституцією. Проте існують суперечності та невизначеності щодо ефективності і дієвості його функціонування щодо забезпечення результативної протидії дезінформації у соціальних мережах.

Метою цієї праці є підвищення ефективності заходів протидії дезінформації шляхом синтезу і застосування концептуальної моделі системи інформаційного протиборства координаційного органу з питань національної безпеки і оборони держави (ЦПД).

Основні завдання дослідження: 1) аналіз діяльності ЦПД на основі публічно доступних даних та офіційних звітів, вивчення ефективності інструментів та стратегій, які використовує Центр протидії дезінформації, зокрема у сфері моніторингу й аналізу інформаційного простору; 2) оцінювання впливу роботи ЦПД на процеси протидії дезінформації в Україні та її ефективність у контексті сучасних викликів і загроз; 3) побудова концептуальної моделі системи інформаційного протиборства координаційного органу з питань національної безпеки і оборони (ЦПД); 4) застосування розробленої моделі для виявлення сильних та слабких сторін системи

протидії дезінформації, а також розроблення практичних пропозицій задля підвищення ефективності заходів протидії дезінформації.

Виклад основного матеріалу. Центр протидії дезінформації при РНБО виконує завдання проведення заходів з протидії поточним і передбачуваним загрозам національній безпеці та інтересам України в інформаційній сфері [2]. Цей координаційний орган з питань національної безпеки і оборони бере безпосередню участь в протидії російській агресії, тому його пріоритетною діяльністю є «оперативне інформування населення, розкриття дезінформації та маніпуляцій, забезпечення інформаційної безпеки, боротьба з інформаційним тероризмом» [2], а відповідно до завдань, визначених Указом Президента України від 7 травня 2021 року № 187/2021, ЦПД реалізовує такі основні функції:

- моніторинг та аналіз: оцінювання інформаційного простору України та загроз інформаційній безпеці;
- виявлення загроз: дослідження чинників, що формують загрози, прогнозування їх наслідків для національних інтересів;
- інформаційна підтримка: надання аналітичних матеріалів для протидії дезінформації і маніпуляціям громадською думкою;
- розроблення концептуальних пропозицій, створення підходів до протидії дезінформації та координації дій органів виконавчої влади;
- розширення спроможності сектору безпеки та оборони, проведення системних заходів для зміцнення можливостей протиборства;
- правове забезпечення: удосконалення законодавства і наукових підходів в сфері інформаційної безпеки;
- стратегічні комунікації: розвиток системи стратегічних комунікацій та координація відповідних заходів;
- оцінювання загроз: створення інтегрованої системи для оцінки інформаційних загроз та оперативного реагування.

Синтез концептуальної моделі. Загалом ЦПД забезпечує реагування й протидію дезінформації. Перше – шляхом моніторингу (детектування) загроз інформаційній безпеці, друге – верифікацією результатів детектування кампаній з боку іноземних держав, пропаганди, дезінформації і деструктивних інформаційних впливів на українське суспільство (їх джерелами є, серед інших, інтернетні ресурси, радіомовлення, телебачення), прийняття управлінських рішень, створення контенту для інформаційного протиборства. В межах своїх функцій ЦПД забезпечує взаємодію з громадськістю: просування створеного контенту у медіа, в інтернеті, поширення громадськими ініціативами й об’єднаннями. Із вебресурсів для розміщення дезінформаційного контенту застосовуються офіційні вебсайти Центру та РНБО, вебпортал АрміяInform [3], а також соціальні мережі: Facebook, TikTok, Instagram, Viber, X (Twitter), Telegram, YouTube, WhatsApp. У сукупності перелічені активності мають забезпечувати зниження вразливості органів виконавчої влади, загроз національним інтересам держави, довіра суспільства до української влади. Означене стало підґрунтям для побудови концептуальної моделі системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони – ЦПД, – яка представлена на рисунку 1.

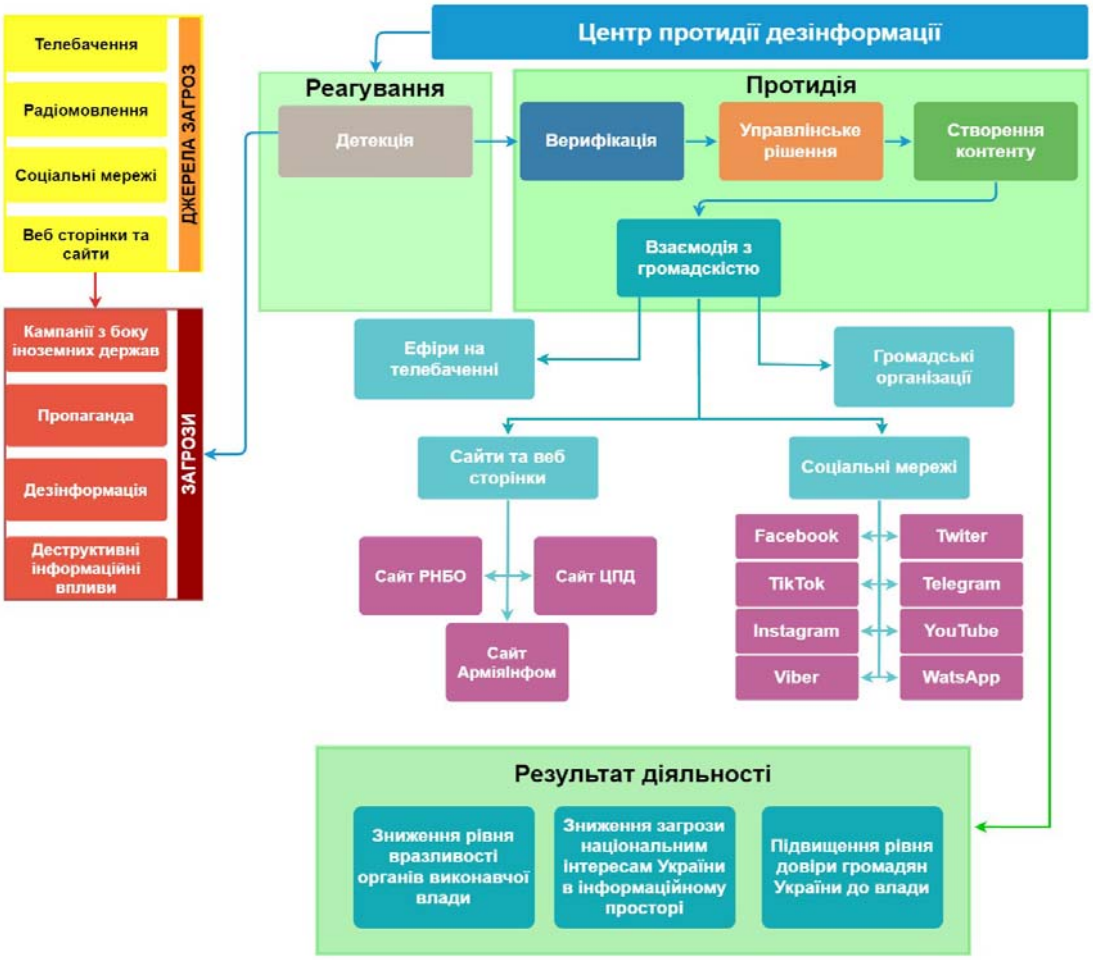

Рисунок 1 – Концептуальна модель системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони

Джерело: розроблено авторами

Оцінювання ефективності системи протидії дезінформації. Відповідно до українського бюджетного законодавства, показниками роботи Центру загалом є двадцяти звітів про результати виявлених інформаційних загрози у сфері національної безпеки та оборони України, проведення десяти заходів з інформаційної безпеки, спрямованих на підвищення захищеності суб'єктів сектору безпеки та оборони, подання п’ятидесяти (щотижневих) матеріалів до РНБОУ України за результатами моніторингу подій та явищ дезінформації, пропаганди та маніпулювання громадською думкою в інформаційному просторі України, а також одна науково-дослідницька робота з питань боротьби з дезінформацією.

Одним з основних факторів успішності кризових комунікацій у контексті спростування дезінформації є оперативність реагування на появу таких матеріалів. Ефективним вважається термін до 90 хвилин між поширенням неправдивої інформації та виходом офіційної реакції з боку уповноваженого представника держави [4]. Ще одним критерієм оцінки загрози в інформаційній сфері є «повторюваність повідомлення»: інтенсивність появи схожих повідомлень у різних медіа, соціальних мережах та месенджерах. При активному повторенні інформації фактор правдивості втрачає свою значимість і важливо надати швидку й комплексну відповідь на негативну інформацію або одночасно просунути позитивні меседжі. На цьому етапі ключовим

стає здатність доцільного спрямування своєї позиції до всіх цільових авдиторій, використовуючи повний спектр комунікаційних інструментів.

Із завдань та індикаторів роботи Центру випливає, що основною метою роботи є моніторинг інформаційного поля та подальше виявлення повідомлень, що містять дезінформацію. Наразі ЦПД функціонує як аналітична установа, здіснює моніторинг інформаційного простору з метою виявлення запланованих дезінформаційних атак, неправдивих новин та заяв, а також відстежує зовнішні деструктивні наративи, які поширює російська пропаганда. Центр реагує на дезінформаційні атаки шляхом розміщення спростувань та проведення інформаційно-аналітичних розвідок. Для поширення результатів своєї роботи зі створення контенту для протидії дезінформації Центр, серед інших інтернетних ресурсів, сторінки у соціальних мережах, які мають таку авдиторію: Instagram - 31,5 тис., X (Twitter) - 4953, Viber - 445 тис., Facebook - 38 тис., YouTube - 15,3 тис., Telegram - 63 тис., TikTok - 44,8 тис., WhatsApp – 107. Гістаграма зазначеної кількості підписників представлена на рисунку 2.

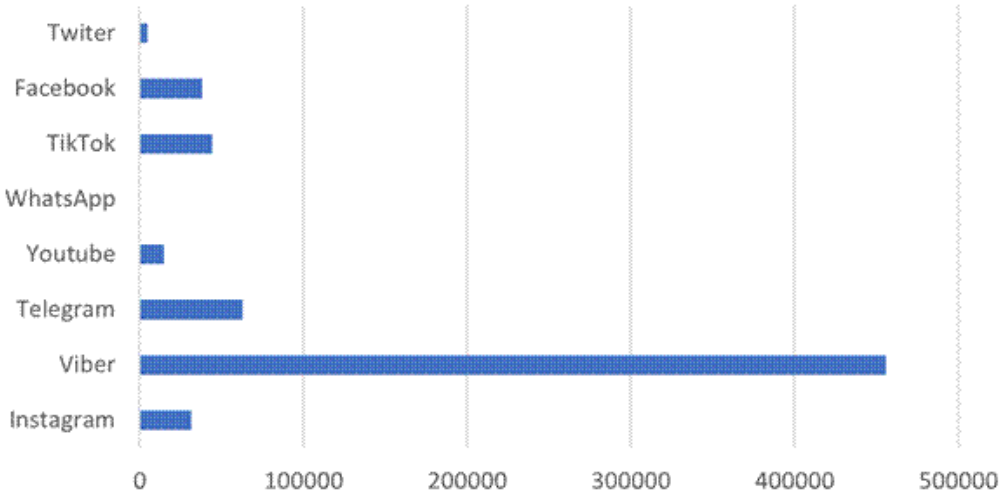

Рисунок 2 – Гістограма авдиторії ЦПД в соціальних мережах – цифрових засобах інформаційного протиборства координаційного органу з питань національної безпеки і оборони

Джерело: розроблено авторами

Охоплення цільової авдиторії є вкрай важливим критерієм у протидії дезінформації. Найменше покриття, як бачимо, забезпечено у пропрієтарному месенджері для смартфонів WhatsApp. Тож, слід провести заходи для розширення (залучення) авдиторії у цьому сервісі. Варто зазначити, що за даними одного з українських операторів мобільного зв'язку WhatsApp використовують понад 5 млн абонентів [9], а згідно з результатами опитування Internews у 2023 році [10] – 11% українців. Також дослідження [10] вказує на світову тенденцію до збільшення застосування WhatsApp в задачах зв'язків з громадськістю, поширення інформації, тобто, що є очевидним, протидії дезінформації зокрема.

Реагування на факт дезінформації спростуванням загалом є лише одним з можливих інструментів. Так, майже повна відсутність проактивної роботи в цьому напрямі може свідчити або про відсутність налагодженої системи моніторингу інформаційних загроз і можливості прогнозувати ризики, або ж про вибірковий підхід до протидії дезінформації.

Із запропонованої моделі (рис.1) випливає завдання удосконалення функції детектування. Робота ЦПД має бути спрямована на створення і використання

інструментів, які дозволять відслідковувати інформаційні атаки на ранніх стадіях їх розгортання. Такі інструменти мають бути максимально автоматизовані, застосовувати складні алгоритми моніторингу інформаційного простору в усіх його сегментах, апаратний комплекс, що дозволятиме обробляти величезні масиви інформації, сучасні технології штучного інтелекту [11, 16]. Крім того, відповідно до результатів дослідження [3], для завдань, пов'язаних з моніторингом інформації та його аналітичним супроводом, а також підготовкою звітів, існують державні установи на кшталт Національного інституту стратегічних досліджень чи незалежного аналітичного центру «Український інститут майбутнього», який як спільний проєкт представників українського бізнесу, політики і громадського сектору «прогнозує зміни та моделює можливі сценарії розвитку подій в Україні, надає компетентну оцінку українським подіям, формулює практичні рекомендації до дій, пропонує ефективні рішення, надає майданчик для дискусій на актуальні теми» [17], а у сфері факт-чекінгу та підвищення медіаграмотності населення згідно з [3] успішно діють команди, які вже продемонстрували свою спроможність і результативність.

Підвищення ефективності заходів протидії дезінформації. Аналіз отриманих результатів дослідження, зокрема моделі системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони, вказує на необхідність удосконалення процесу детекції інформаційних загроз та фейкових повідомлень, а також гострої необхідності розширення інформаційної діяльності, збільшення цільової авдиторії ЦПД в месенджері WhatsApp.

Для розв'язку першої задачі пропонується впровадити концепцію інтегрованої системи оцінки та моніторингу інформаційних загроз та оперативного реагування на них, застосування технологій ШІ. Ця система має автоматично аналізувати великий обсяг даних, наближеному до реального часу, й порівнювати їх з історичними даними, виявляти патерни, спільні характеристики в повідомленнях, авторах, групах авторів. Крім того, удосконалення дозволить оцінювати оригінальність та повторюваність фрагментів текстів, створювати автоматичні реферати про інформаційні події на основі повідомлень. Основна мета застосування зазначеного підходу – скорочення часу між моментом появи інформації та моментом її виявлення системою.

Розв'язок задачі збільшення покриття у WhatsApp полягає в проведенні заходів збільшення авдиторії [12] в зазначеному пропрієтарному месенджері, що дозволить підвищити ефективність протидії дезінформації за рахунок збільшення охопленої медійної групи під час інформаційної діяльності координаційного органу з питань національної безпеки і оборони.

Висновки:

1. Представлені у цій праці результати аналізу існуючих досліджень і публікацій показали, що для підвищення ефективності заходів протидії дезінформації слід вирішити завдання синтезу концептуальної моделі інформаційного протиборства, що дозволить визначити слабкі й сильні сторони системи, запропонувати метод розв'язку науково-практичної задачі забезпечення ефективної діяльності інституцій, які відповідають за протидію дезінформації, – координаційного органу з питань національної безпеки і оборони.

2. Результати оцінювання ефективності діяльності ЦПД на процеси протидії дезінформації в Україні показали, що, попри фактично існуючий потенціал, пропрієтарний месенджер WhatsApp має найменше, критично мале охоплення авдиторії, хоча ним користуються значна частина абонентів мобільного інтернету в Україні. Крім того, недостатнім є рівень цифровізації моніторингу, який на сьогодні

вимагає аналізування великих обсягів інформації, зокрема з використанням технологій штучного інтелекту.

3. Для побудови концептуальної моделі системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони проведено дослідження ЦДП. Тож, в її базис покладені функцію створення контенту для інформаційного протиборства та взаємодію з громадськістю через просування контенту в медіа і соціальних мережах, тобто реагування на загрози інформаційній безпеці шляхом моніторингу та верифікації дезінформаційних кампаній, зокрема від іноземних держав та інших джерел пропаганди і деструктивних інформаційних впливів, а також засоби, які для цього використовуються: інтернетні ресурси, радіо, телебачення, соціальні мережі.

4. Аналіз запропонованої моделі і результатів дослідження показав гостру необхідність розширення покриття цільової авдиторії через соціальні мережі та месенджери, удосконалення системи детектування інформаційних атак, зокрема за допомогою інформаційних систем, складних алгоритмів моніторингу і технологій штучного інтелекту, а також недостатню проактивність роботи координаційного органу з питань національної безпеки і оборони. Практичними результатами цієї праці є обґрунтована необхідність удосконалення детекції інформаційних загроз, задача використання технологій ШІ для виявлення і реагування на загрози, збільшення охоплення цільової авдиторії у WhatsApp. Це дозволить підвищити ефективність роботи координаційного органу з питань національної безпеки і оборони за рахунок скорочення часу між появою фейкової інформації та її виявленням, збільшення результативності реагування на дезінформацію завдяки розширенню цільової аудиторії і застосуванню сучасних ІТ.

За результатами цього дослідження сформульовано, обґрунтовано і внесено на розгляд ЦДП практичні рекомендації щодо розширення присутності в ключових месенджерах для забезпечення протидії дезінформації. Їх врахування дозволить розширити коло цільової авдиторії для протидії дезінформації, пропаганди, деструктивним інформаційним впливам та кампаній. Очікуваним ефектом цього є зниження рівня вразливості органів виконавчої влади та суспільства до загроз інформаційного характеру завдяки ефективним підходам до здійснення оцінювання ризиків і загроз національним інтересам України в інформаційному просторі шляхом імплементації підходів раннього попередження про загрози інформаційного характеру. Водночас, означене забезпечить скорочення інтервалу часу між настанням резонансної події (або появи інформації про неї) та інформаційним реагуванням на неї.

Список літератури

1. Біденко А., Золотухін Д., Тарабукін О. Біла книга протидії дезінформації. К.: Інститут інформаційної безпеки, 2022. 62 с. URL: https://www.infosecurity.institute/Проекти-1/-2 (дата звернення: 17.04.2024).
2. Про Центр. Центр протидії дезінформації. URL: https://cpd.gov.ua/documents/про-центр/ (дата звернення: 01.05.2024).
3. Біденко А. Центр протидії дезінформації: філософія проти менеджменту. ГО «Детектор медіа» : сайт. URL: https://detector.media/infospace/article/185107/2021-02-22-tsentr-protydii-dezinformatsii-filosofiya-proty-menedzhmentu/ (дата звернення: 01.05.2024).
4. Золотухін Д. Центр протидії дезінформації: практика імплементації. ГО «Детектор медіа» : сайт. URL: https://detector.media/infospace/article/185586/2021-03-08-tsentr-protydii-dezinformatsii-praktyka-implementatsii/ (дата звернення: 01.05.2024).
5. Золотухін Д. Матриця загроз інформаційної сфери. ГО «Детектор медіа» : сайт. URL: https://detector.media/infospace/article/186798/2021-04-08-matrytsya-zagroz-informatsiynoi-sfery/ (дата звернення: 01.05.2024).

6. Золотухін Д. Як має працювати Центр протидії дезінформації. ГО «Детектор медіа» : сайт. URL: https://detector.media/infospace/article/185077/2021-02-20-yak-maie-pratsyuvaty-tsentr-protydii-dezinformatsii-poyasnennya-napaltsyakh/ (дата звернення: 01.05.2024).
7. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації» : Указ Президента України від 19.03.2021 №106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text (дата звернення: 01.05.2024).
8. Питання Центру протидії дезінформації : Указ Президента України від 07.05.2021 №187/2021. URL: https://www.president.gov.ua/documents/1872021-38841 (дата звернення: 01.05.2024).
9. АрміяInform : сайт. Міністерство оборони України. URL: https://armyinform.com.ua/ (дата звернення: 10.04.2024).
10. Коцофане О. Які соцмережі і месенджери найпопулярніші серед українців. Webpromo. URL: https://web-promo.ua/ua/blog/kakie-socseti-i-messendzhery-samye-populyarnye-sredi-ukraincev/ (дата звернення: 01.05.2024).
11. Українські медіа, ставлення та довіра у 2023 р. : Опитування USAID-Internews щодо споживання медіа. Internews. URL: https://internews.in.ua/wp-content/uploads/2023/10/Ukrainski-media-stavlennia-ta-dovira-2023r.pdf (дата звернення: 01.05.2024).
12. Гбур З.В. Використання штучного інтелекту в інформаційній безпеці України. Державне управління: удосконалення та розвиток. 2022. № 1. DOI: 10.32702/2307-2156-2022.1.2.
13. Леонов Я. В., Васильківський Д. М., Бойко В. Д. Еволюція інформаційного маркетингу: стратегії та технології в сучасному бізнесі. Ефективна економіка. 2024. № 2. DOI: http://doi.org/10.32702/2307-2105.2024.2.27. URL: http://nbuv.gov.ua/UJRN/efek_2024_2_29 (дата звернення: 02.09.2024).
14. Доренський О.П. Модель поведінки держави в умовах проявів ознак інформаційної експансії, агресії, війни. Інформаційна безпека держави, суспільства та особистості : Всеукр. наук.- практ. конф., 16 квіт. 2015 р., м. Кіровоград : зб. тез доп. – Кіровоград: КНТУ, 2015. С. 131-133. URI: https://dspace.kntu.kr.ua/handle/ 123456789/6100 (дата звернення: 17.04.2024).
15. Колодяжний І.О., Доренський О.П. Методологічні засади підвищення ефективності протидії антиукраїнській пропаганді в соціальних мережах. Інформаційні технології – 2019 : VI всеукр. наук.-практ. конф. молодих науковців, 16 трав. 2019 р., м. Київ. К. : Київ. унт ім. Б. Грінченка, 2019. С. 53-54. URL: https://fitm.kubg.edu.ua/images/stories/Departments/kitmd/zbirnuk/zbirn_tez_materialiv_konf_IT_2019.pdf (дата звернення: 17.04.2024).
16. Трофименко О., Логінова Н., Соколов А., Чикунов П., Ахмаметьєва Г. Штучний інтелект у військовій сфері. *Кібербезпека: освіта, наука, техніка*. № 1(25). С. 161-176. DOI 10.28925/2663-4023.2024.25.161176.
17. Про інститут. Український інститут майбутнього. URL: https://uifuture.org/pro-institut/ (дата звернення: 17.08.2024).

References

1. Bidenko, A., Zolotukhin, D., & Tarabukin, O. (2022). *Disinformation White Paper*. Kyiv: Institute of Information Security https://www.infosecurity.institute/Проекти-1/-2.
2. About the Center. (n.d.). Tsentr protydii dezinformatsii. https://cpd.gov.ua/documents/про-центр/.
3. Bidenko, A. (2021, February 22). Center for Countering Disinformation: Philosophy vs. Management. Detektor media. https://detector.media/infospace/article/185107/2021-02-22-tsentr-protydii-dezinformatsii-filosofiya-proty-menedzhmentu/.
4. Zolotukhin, D. (2021, March 8). Center for Countering Disinformation: Implementation Practice. Detektor media. https://detector.media/infospace/article/185586/2021-03-08-tsentr-protydii-dezinformatsii-praktyka-implementatsii/
5. Zolotukhin, D. (2021, April 8). Matrix of threats to the information sphere. Detektor media. https://detector.media/infospace/article/186798/2021-04-08-matrytsya-zagroz-informatsiynoi-sfery/.
6. Zolotukhin, D. (2021, February 20). How the Center for Countering Disinformation Should Work. Detektor media. https://detector.media/infospace/article/185077/2021-02-20-yak-maie-pratsyuvaty-tsentr-protydii-dezinformatsii-poyasnennya-napaltsyakh/.
7. Decree of the President of Ukraine On the Decision of the National Security and Defense Council of Ukraine of March 11, 2021 “On the Establishment of the Center for Countering Disinformation” №106/2021. (2021, March 19). https://zakon.rada.gov.ua/laws/show/106/2021#Text.
8. Question from the Center for Countering Disinformation: Decree of the President of Ukraine. (2021, May 7). №187/2021. https://www.president.gov.ua/documents/1872021-38841.

9. ArmyInform. (n.d.). Ministerstvo oborony Ukrainy. https://armyinform.com.ua/.
10. Kotsofane, O.(2021, February 15) What social networks and messengers are most popular among Ukrainians. Webpromo. https://web-promo.ua/ua/blog/kakie-socseti-i-messendzhery-samye-populyarnye-sredi-ukraincev/.
11. Ukrainian Media, Attitudes and Trust in 2023: USAID - Internews Media Consumption Survey. Internews. https://internews.in.ua/wp-content/uploads/2023/10/Ukrainski-media-stavlennia-ta-dovira-2023r.pdf.
12. Hbur, Z.V. (2022). The use of artificial intelligence in information security in Ukraine. Derzhavne upravlinnia: udoskonalennia ta rozvytok. № 1. [in Ukrainian]. https://www.doi.org/10.32702/2307-2156-2022.1.2.
13. Leonov, Ya.V., Vasylkivskyi, D.M., & Boiko, V.D. (2024). The Evolution of Information Marketing: Strategies and Technologies in Modern Business. Efektyvna ekonomika, № 2. [in Ukrainian]. http://doi.org/10.32702/2307-2105.2024.2.27.
14. Dorenskyi, O.P. (2015) Model of state behavior in conditions of manifestations of signs of information expansion, aggression, war. Informatsiina bezpeka derzhavy, suspilstva ta osobystosti : zbirnyk tez dopovidei vseukraisnkoi naukovo- praktychnoi konferentsii (pp. 131-133) Kirovohrad: KNTU [in Ukrainian]. https://dspace.kntu.kr.ua/handle/123456789/6100.
15. Kolodiazhnyi, I.O., & Dorenskyi, O.P. (2019) Methodological principles for increasing the effectiveness of countering anti-Ukrainian propaganda in social networks. Informatsiini tekhnolohii – 2019 : vseukrainska naukovo-praktychna konferentsiia molodykh naukovtsiv (pp. 53-54). Kyiv : KU im. B. Hrinchenka [in Ukrainian]. https://fitm.kubg.edu.ua/images/stories/Departments/kitmd/zbirnuk/zbirn_tez_materialiv_konf_IT_2019.pdf.
16. Trofymenko, O., Lohinova, N., Sokolov, A., Chykunov, P., & Akhmametieva, H. (2024) Artificial intelligence in the military sphere. *Kiberbezpeka: osvita, nauka, tekhnika*, № 1(25), 161-176. http://doi.org/10.28925/2663-4023.2024.25.161176.
17. About the Institute. (n.d.). Ukrainskyi instytut maibutnoho. https://uifuture.org/pro-institut/.

Oleksandr Dorenskyi, Assoc. Prof., PhD tech. sci., **Oleksandr Ulichev**, PhD tech. sci.,
Kostiantyn Zadorozhnyi, student, **Anastasiia Kovalenko**, assistent, **Hanna Drieieva**, PhD
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

The Conceptual Model of the Information Counteraction System of the Coordination Center for National Security and Defense Issues

The article examines the pressing issue of enhancing the efficiency of information confrontation conducted by the coordination body responsible for national security and defense – the Center for Countering Disinformation. The goal of this study is achieved by synthesizing a conceptual model of the information confrontation system, applying this model to identify weaknesses, and improving the mechanism for countering disinformation to enhance its efficiency. This improvement ensures effective resistance to destructive informational influences and campaigns, propaganda, real and potential threats in the information sphere, and prevents attempts to manipulate public opinion.

The proposed mechanism for countering disinformation involves responding to disinformation attacks by creating and distributing content on social media platforms. The results revealed insufficient coverage of the target audience on WhatsApp, highlighting a deficiency in the information confrontation system that adversely affects the efficiency of countering disinformation. The research also demonstrates the importance of enhancing the detection process for informational threats using IT, advanced technologies, and artificial intelligence tools. This approach will reduce the time required to identify threats in the information sphere. To address the existing problem, the study suggests expanding the coverage of the target audience on WhatsApp to improve the efficiency of the coordination body's disinformation countermeasures. This body plays a key role in ensuring the state’s informational security, identifying and countering disinformation, propaganda, and destructive informational influences, as well as conducting measures to mitigate threats in the information domain.

The practical value of this research lies in reducing the vulnerability of executive authorities and society to informational threats by enhancing the effectiveness of disinformation countermeasures. Additionally, it will improve the responsiveness to disinformation, propaganda, and manipulation, shorten the time between the emergence and detection of fake information, and ensure effective risk assessment for Ukraine's national security in the information space.

information security, disinformation, information counteraction, conceptual model, social media, WhatsApp

Одержано (Received) 08.11.2024 *Прорецензовано (Reviewed) 10.12.2024*
Прийнято до друку (Approved) 23.12.2024