Крап Андрій Павлович

Стратегії захисту національної безпеки від інформаційних атак і пропаганди

УДК 351.86:004.738.5:316.77
DOI https://doi.org/10.24195/2414-9616.2024-5.10

Крап Андрій Павлович
кандидат політичних наук,
доцент кафедри суспільно-гуманітарних та фундаментальних дисциплін
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»
вул. Фрометівська, 2, Київ, Україна
ORCID: 0000-0002-4443-3364

У статті досліджено сучасні стратегії захисту національної безпеки від інформаційних атак і пропаганди, які стали невід'ємною частиною гібридних загроз у глобалізованому цифровому світі. Метою дослідження є всебічне теоретичне осмислення природи інформаційних загроз і формування ефективних механізмів їхньої нейтралізації. У статті проаналізовано ключові аспекти інформаційної війни, механізми впливу пропаганди та роль цифрових технологій у її поширенні.

На досягнення поставленої мети використано міждисциплінарний підхід, що включає системний аналіз, метод порівняльного аналізу, історико-генетичний метод, структурно-функціональний підхід, а також контент-аналіз сучасних пропагандистських наративів. Це забезпечило багатовимірний підхід до аналізу явищ, пов'язаних із інформаційною війною.

У результаті дослідження визначено основні типи інформаційних атак і пропагандистських наративів, зокрема ті, що спрямовані на маніпуляцію громадською свідомістю, викривлення історичних фактів і підрив довіри до державних інституцій. Встановлено, що ефективні стратегії протидії повинні включати розвиток кібербезпеки, підвищення рівня медіаграмотності, створення позитивного інформаційного порядку денного та вдосконалення нормативно-правової бази.

Наукова новизна статті полягає у синтезі теоретичних і практичних підходів до захисту інформаційного простору, що враховують когнітивні, технологічні та соціокультурні аспекти. Теоретичне значення роботи полягає у систематизації знань про механізми інформаційної війни, тоді як практичне значення – у розробці рекомендацій для державних інституцій, громадянського суспільства та міжнародних організацій.

Ключові слова: *інформаційна війна, пропаганда, національна безпека, дезінформація, соціальні мережі, кібербезпека, когнітивні атаки.*

Вступ. Сучасний світ зіткнувся з безпрецедентними викликами в контексті інформаційної безпеки, що безпосередньо впливають на національну безпеку кожної держави, незалежно від її географічного розташування чи рівня економічного розвитку. Інформаційні атаки та пропаганда, що вкорінюються у цифровому середовищі (особливо у вигляді маніпуляцій у соціальних мережах), стали ефективним інструментом ведення гібридних воєн, здатним змінювати суспільні настрої, політичні орієнтири та навіть підривати засади державного суверенітету. Гадаємо, такі феномени не лише є наслідком технологічного прогресу, а й відображають кризу традиційних механізмів комунікації та управління інформаційними потоками.

Очевидно, що сучасні стратегії захисту національної безпеки в умовах інформаційного протиборства повинні враховувати не лише технічні аспекти кібербезпеки, а й глибинні соціально-психологічні механізми впливу пропаганди, а також культурно-ціннісний контекст суспільств. З урахуванням викладеного вище, особливої уваги заслуговує інтерпретація проблеми з позицій міждисциплінарного підходу, що поєднує здобутки кібернетики, соціології, політології та правознавства. На наше переконання, такий підхід дозволяє не лише глибше зрозуміти природу інформаційних загроз, а й окреслити комплексний інструментарій для їхнього нейтралізування.

Особливе місце у вивченні цього феномену займають наукові школи, що аналізують пропаганду як частину ширшого явища комунікативного домінування. Наприклад, прихильники теорії «фабрик консенсусу» (розробленої Н. Хомським і Е. Германом) наголошують на тому, що інформаційні атаки спрямовані на формування керованої реальності, тоді як представники критичної соціології зосереджуються на соціальній дезінтеграції, що виникає внаслідок маніпулятивного впливу. Водночас, у рамках постмодерністського дискурсу (зокрема, у працях Ж. Бодрійяра) інформаційна війна трактується як спосіб симуляції дійсності, де пропаганда слугує засобом контролю над свідомістю.

Гадаємо, важливість порушеної теми зумовлена не лише теоретичним, а й прикладним значенням дослідження, оскільки інформаційна безпека нині є ключовим компонентом стійкості державних інституцій. У цьому контексті стаття покликана не лише проаналізувати сучасні стратегії захисту національної безпеки від інформаційних атак і пропаганди, а й запропонувати нові підходи, які відповідають викликам глобалізованого цифрового світу.

Аналіз останніх досліджень і публікацій. Аналіз сучасної літератури, присвяченої проблемам інформаційної війни, пропаганди та їх впливу на національну безпеку, демонструє широкий спектр підходів до цих питань. Вивчення динаміки пропагандистських атак, зокрема їхньої інтенсивності та хронології, ретельно досліджено у роботі А. Барановського-Дьюї [1]. Автор наголошує на

важливості стратегічного аналізу у виявленні ключових чинників, що визначають ефективність інформаційних атак.

К. Кріллі у своєму дослідженні акцентує увагу на інформаційній війні як новому полі бою, де тероризм і пропаганда набули глобального масштабу завдяки Інтернету [2]. Його висновки підкреслюють роль цифрових технологій у трансформації традиційних методів маніпуляції суспільною свідомістю.

Водночас В. Денисенко аналізує загрози, які створюють пропаганда та інформаційна війна для національної безпеки Литви [3]. Його праця пропонує цінні емпіричні дані, які дозволяють порівняти досвід Литви з іншими постраданськими країнами.

Огляд боротьби з китайською пропагандою в умовах виборчої кампанії Тайваню у 2020 році подано в дослідженні А. Хуана [4]. Автор виділяє ключові методи протидії дезінформації, наголошуючи на важливості багатовекторного підходу.

І. Іфтиме та М. Іфтиме зосереджують свою увагу на основних інструментах когнітивних атак, таких як дезінформація та пропаганда [5]. Їхній підхід інтегрує аспекти психології та інформаційних технологій, що створює багатогранну картину сучасних інформаційних загроз.

Дослідження К. Кіфорчука привертає увагу до частотного аналізу російських пропагандистських Telegram-каналів [6]. Це дослідження робить внесок у розуміння механізмів поширення пропаганди у цифрових мережах.

Праця О. Кравченка, В. Веклича, М. Крихівського та Т. Мадриги пропонує комплексний огляд проблем кібербезпеки у контексті інформаційної війни [7]. Авторами підкреслено важливість синхронізації технологічних і політичних стратегій.

С. Макдональд у своїй монографії звертається до аналізу інформаційних війн XXI століття, акцентуючи увагу на операціях обману та змінених образах [8]. Його висновки є актуальними для розуміння сучасних тенденцій інформаційного протиборства.

Внесок Й. Мандіча та Д. Кларича полягає в детальному розборі російської дезінформаційної кампанії під час війни в Україні [9]. Авторами окреслено основні наративи, цілі та наслідки пропаганди.

О. Мельникова-Курганова досліджує наративи пропаганди під час облоги Маріуполя у 2022 році [10]. Її робота дозволяє глибше зрозуміти специфіку інформаційної боротьби у контексті воєнних дій.

Б. Розенфельд та Дж. Воллес розглядають інформаційну політику в авторитарних суспільствах, акцентуючи увагу на використанні пропаганди як інструменту контролю [11].

М. Шульц аналізує цифрові аспекти інформаційної війни, зокрема пропаганду та кіберзагрози [12]. Його робота висвітлює інноваційні підходи до захисту інформаційного простору.

Ю. Тарасюк досліджує російські наративи в медіапросторі Туреччини, наголошуючи на їхніх історичних витоках [13]. Її висновки проливають світло на культурні аспекти інформаційної війни.

М. Вехнер аналізує взаємозв'язок між хакерством, пропагандою та маніпуляцією виборчим процесом [14], тоді як Е. Вільямс і К. Карлі фокусуються на маніпуляціях пошуковими системами для поширення проросійської пропаганди [15].

З урахуванням викладеного вище, зазначені роботи є важливим підґрунтям для розробки комплексних стратегій протидії інформаційним атакам і пропаганді, інтегруючи теоретичні та прикладні підходи до розуміння цього феномену.

Мета і завдання дослідження. Метою статті є всебічне дослідження сучасних стратегій захисту національної безпеки від інформаційних атак і пропаганди, з акцентом на їхніх когнітивних, технологічних і соціально-політичних аспектах. На наше переконання, дана мета обумовлена необхідністю глибокого теоретичного осмислення природи інформаційної загрози та формування дієвих механізмів протидії у глобалізованому цифровому середовищі. На її досягнення поставленої передбачається вирішення таких завдань, як: розкриття концептуальних засад інформаційної війни та пропаганди, зокрема визначення ключових понять, механізмів впливу та їх трансформацію в умовах цифровізації; розкриття специфіки інформаційних атак у контексті сучасних гібридних загроз, враховуючи їхній вплив на суспільну свідомість, політичні процеси та національну безпеку; вивчення міжнародного досвіду у сфері протидії пропаганді та інформаційним атакам, окресливши ефективні практики для їхнього адаптування до українських реалій.

Методи дослідження. У процесі написання статті використано міждисциплінарний підхід, що передбачає поєднання методів різних галузей знань для комплексного аналізу обраної проблематики. Основними методами стали системний аналіз, який дозволив розглянути інформаційну війну та пропаганду як складні соціально-технологічні явища, а також метод порівняльного аналізу, застосований для вивчення міжнародного досвіду протидії інформаційним атакам. Використання історико-генетичного методу забезпечило глибше розуміння еволюції пропагандистських стратегій, тоді як структурно-функціональний підхід дозволив виявити ключові механізми впливу інформаційних атак на суспільні процеси. Додатково застосовано контент-аналіз, спрямований на дослідження сучасних пропагандистських наративів у цифрових медіа, та метод правового аналізу для оцінки нормативно-правових засобів захисту інформаційного простору. На наше переконання, така комбінація методів забезпечує цілісність та багатовимірність дослідження.

Результати дослідження

1. Теоретичні основи інформаційної війни та пропаганди: сучасний контекст. Інформаційна війна та пропаганда як складні феномени сучасного світу заслуговують на глибоке теоретичне осмислення з огляду на їхню трансформацію у цифрову епоху. У контексті гібридних загроз вони перетворилися на ключові інструменти впливу, спрямовані на маніпуляцію суспільною свідомістю, підрив національної безпеки та формування керованої політичної реальності. Зокрема, як зазначає К. Кріллі, інформаційна війна стає «новим полем битви», де терористи й авторитарні режими використовують Інтернет для просування своїх наративів [2]. На наше переконання, це свідчить про глибинну зміну структури комунікаційних стратегій у глобальному середовищі.

Теоретичні підходи до вивчення пропаганди включають низку концептуальних моделей, кожна з яких пропонує власне трактування цього явища. Наприклад, прихильники критичної теорії, такі як М. Вехнер, наголошують на тісному зв'язку між пропагандою, маніпуляцією виборчими процесами та технологіями хакерства, які часто стають основою для поширення дезінформації [14]. Водночас, постмодерністські інтерпретації, що ґрунтуються на працях Ж. Бодрійяра, акцентують увагу на симулятивному характері інформаційного впливу, де реальність заміщується її медійними репрезентаціями.

Значну увагу у сучасних дослідженнях приділяється специфіці інформаційних атак у цифровому середовищі. Як наголошують І. Іфтиме та М. Іфтиме, основними інструментами когнітивного впливу є дезінформація та пропаганда, які інтегруються в соціальні мережі для досягнення максимальної ефективності [5]. На наше переконання, саме це поєднання когнітивного та цифрового впливу створює унікальну динаміку сучасної інформаційної війни, підриваючи традиційні підходи до захисту інформаційного простору.

Окремо варто відзначити роль держави у забезпеченні інформаційної безпеки. Як зазначає В. Денисенко, у випадку Литви, ефективний захист інформаційного простору базується на поєднанні правових, технічних та освітніх заходів [3]. Такий підхід дозволяє створити стійку систему протидії пропаганді, адаптовану до викликів глобалізованого світу.

З урахуванням викладеного вище, важливо враховувати також культурно-історичний контекст інформаційної війни, оскільки пропаганда часто апелює до національних символів, історичних наративів та культурних особливостей. Наприклад, Ю. Тарасюк у своєму дослідженні аналізує, як російські наративи у медіа Туреччини використовують історичні алюзії для зміцнення політичного впливу [13]. Вочевидь, такі аспекти вимагають не лише правового, а й соціокультурного підходу до вирішення проблеми.

На наше переконання, розуміння теоретичних засад інформаційної війни та пропаганди є ключовим для розробки ефективних стратегій протидії цим явищам. Саме тому у подальших розділах дослідження буде приділено увагу як практичним аспектам протидії інформаційним атакам, так і аналізу конкретних пропагандистських наративів, що мають значний вплив на сучасні суспільства.

2. Стратегії захисту національної безпеки від інформаційних атак. На наше переконання, сучасні стратегії захисту національної безпеки в умовах інформаційної війни повинні базуватися на комплексному підході, який поєднує технічні, правові, організаційні та освітні механізми. Інформаційні атаки, що спрямовані на підрив суспільної довіри до державних інституцій, маніпуляцію виборчими процесами чи поширення фейкових наративів, вимагають адаптивних методів протидії. У цьому контексті важливим є не лише виявлення та нейтралізація загроз, а й формування стійкості суспільства до їхнього впливу.

Одним із ключових напрямів захисту є розвиток кібербезпеки, що забезпечує технологічну базу для захисту інформаційного простору. Як зазначають О. Кравченко, В. Веклич, М. Крихівський та Т. Мадрига, кібербезпека в умовах інформаційної війни є критичним компонентом стійкості держави, оскільки інформаційні атаки часто поєднуються з кібернападами [7]. На наше міркування, технічні заходи повинні включати впровадження систем раннього попередження, постійний моніторинг інформаційного середовища та забезпечення безпеки ключових державних інформаційних ресурсів.

Другою важливою складовою є підвищення рівня медіаграмотності населення, що дозволяє мінімізувати ефективність пропагандистських впливів. Як зазначає К. Кіфорчук, аналіз контенту російських Telegram-каналів виявляє високий рівень маніпулятивності, що спрямована на викривлення суспільного сприйняття подій [6]. Медіаграмотність сприяє розпізнаванню таких маніпуляцій, а також формуванню критичного мислення, що є основою для побудови інформаційної стійкості.

Водночас важливим аспектом є правове забезпечення інформаційної безпеки. Держава повинна розробляти й упроваджувати законодавчі акти, що регулюють питання відповідальності за поширення дезінформації та інших форм інформаційних атак. Як зазначає В. Денисенко, ефективна правова база у поєднанні з інституційними механізмами є запорукою забезпечення національної безпеки [3]. На наше переконання, в Україні доцільно розвивати механізми міжнародного співробітництва для обміну досвідом у протидії інформаційним загрозам.

Окремим елементом є інформаційна стратегія, спрямована на створення позитивного порядку денного. Як зазначають Б. Розенфельд і Дж. Воллес, у авторитарних режимах інформаційна політика базується на монополії над медіапростором, що дозволяє контролювати громадську думку через пропаганду [11]. Демократичним державам варто використовувати відкритий підхід, заснований на прозорості, об'єктивності й підтримці довіри громадян до офіційної інформації.

Також значущим фактором є розвиток міжвідомчої координації між державними органами, громадськими організаціями та приватним сектором. Як зазначають І. Іфтиме та М. Іфтиме, такі координаційні механізми є важливими для забезпечення цілісності системи протидії інформаційним загрозам [5]. На наше переконання, взаємодія різних секторів створює умови для швидкої та ефективної відповіді на інформаційні атаки.

З урахуванням викладеного вище, стратегія захисту національної безпеки повинна інтегрувати технічні, соціальні та нормативно-правові інструменти, спрямовані на забезпечення інформаційної стійкості держави. У подальших розділах дослідження буде розглянуто конкретні пропагандистські наративи та методи їх деконструкції.

3. Пропагандистські наративи та їх вплив на суспільство: сучасні виклики. Одним із ключових аспектів інформаційної війни є формування пропагандистських наративів, що активно використовуються для впливу на суспільну свідомість, зокрема з метою дестабілізації політичних систем, маніпуляції громадською думкою та підриву довіри до державних інституцій. Пропагандистські наративи являють собою цілеспрямовано створені змістові конструкції, які мають маніпулятивний характер і використовуються для досягнення стратегічних цілей у гібридних конфліктах.

Як зазначають Й. Мандіч і Д. Кларич, російські дезінформаційні кампанії під час війни в Україні спираються на пропагандистські наративи, які поєднують історичні міфи, антизахідну риторику та апеляцію до культурних символів [9]. На наше переконання, ці наративи спрямовані на формування викривленого образу реальності, який сприяє легітимізації агресивних дій та створенню ілюзії підтримки серед місцевого населення.

Одним із центральних елементів сучасних пропагандистських стратегій є використання соціальних мереж як засобу швидкого та широкомасштабного поширення маніпулятивного контенту. Як свідчить дослідження К. Кіфорчука, аналіз контенту російських Telegram-каналів демонструє систематичне використання емоційно забарвлених меседжів, спрямованих на дискредитацію західних інституцій та розкол у суспільстві [6]. Вочевидь, такі методи дозволяють швидко адаптуватися до змін у політичному чи інформаційному середовищі, посилюючи ефективність пропаганди.

Пропагандистські наративи часто використовують когнітивні вразливості суспільства, зокрема упередження, страхи та стереотипи. І. Іфтиме та М. Іфтиме зазначають, що когнітивні атаки, побудовані на використанні таких вразливостей, стають ключовим інструментом у сучасних інформаційних війнах [5]. Цей підхід включає маніпуляцію історичними фактами, викривлення культурних символів і апеляцію до традиційних цінностей, що сприяє посиленню дезінтеграційних процесів у суспільстві.

Важливою особливістю сучасних інформаційних кампаній є залучення історичних наративів для легітимізації агресивної політики. Як показує аналіз Ю. Тарасюк, у Туреччині російські медіа активно використовують історичні алюзії для створення вигідного геополітичного контексту, що сприяє поширенню проросійських настроїв [13]. На наше переконання, такі методи не лише підсилюють ідеологічний вплив пропаганди, а й ускладнюють процес її деконструкції.

Ефективна протидія пропагандистським наративам вимагає системного підходу, який включає виявлення та деконструкцію маніпулятивних меседжів, розвиток критичного мислення у суспільстві та створення альтернативних позитивних наративів. Як зазначають Б. Розенфельд і Дж. Воллес, у демократичних суспільствах протидія пропаганді має базуватися на прозорості, об'єктивності та підтримці суспільної довіри до офіційних джерел інформації [11].

З урахуванням викладеного вище, сучасні виклики, пов'язані з впливом пропагандистських наративів, вимагають інтеграції різних підходів до їхньої нейтралізації. Це включає технологічні, правові, освітні та культурні заходи, спрямовані на зміцнення інформаційної стійкості суспільства, що є ключовим компонентом національної безпеки в умовах глобалізованого інформаційного простору. Узагальнимо наші міркування у формі таблиці (Таблиця 1).

Висновки. Дослідження проблематики захисту національної безпеки від інформаційних атак і пропаганди підтвердило критичну важливість цієї сфери у контексті сучасних глобальних викликів. Інформаційна війна стала невід'ємною частиною гібридних конфліктів, що значно ускладнює традиційні підходи до забезпечення безпеки держави. Пропаганда, дезінформація та когнітивні атаки дедалі частіше використовуються як стратегічні інструменти для маніпуляції суспільною свідомістю, підриву довіри до державних інституцій і поширення хаосу в інформаційному просторі.

Теоретичний аналіз засвідчив, що феномен інформаційної війни та пропаганди має багатовимірний характер, який потребує інтеграції підходів різних наукових шкіл. На наше переконання, най-

Таблиця 1

Механізми впливу пропаганди та інформаційних атак

Тип інформаційної загрози	Механізм впливу	Приклад
Пропаганда	Формування маніпулятивних наративів	Російські наративи щодо «легітимізації» агресії проти України
Дезінформація	Поширення фальшивої або викривленої інформації	Використання Telegram-каналів для дискредитації західних інституцій
Когнітивні атаки	Використання упереджень і стереотипів	Апеляція до історичних міфів у медіа для посилення проросійських настроїв
Кіберзагрози	Злам та маніпуляція інформаційними ресурсами	Хакерські атаки, спрямовані на викрадення або модифікацію даних виборчих кампаній
Симуляція реальності	Створення альтернативного медіапорядку	Використання медіа для заміщення реальних подій вигаданими або спотвореними

більш продуктивним є міждисциплінарний підхід, що враховує технічні, когнітивні, правові та соціокультурні аспекти цих явищ. Інформаційні атаки сьогодні спираються не лише на технологічну інфраструктуру, але й на складні психологічні механізми, які важливо розуміти для розробки ефективних стратегій протидії.

Практичний аналіз показав, що стратегії захисту національної безпеки повинні включати розвиток кібербезпеки, підвищення рівня медіаграмотності населення, формування правових механізмів протидії дезінформації, а також створення позитивного інформаційного порядку денного. Як свідчить міжнародний досвід, ефективна протидія інформаційним загрозам можлива лише за умов тісної взаємодії державних інституцій, громадянського суспільства та приватного сектору.

Особливої уваги потребує деконструкція пропагандистських наративів, які становлять основну зброю інформаційних атак. Як показали результати дослідження, такі наративи використовуються для зміцнення авторитарних режимів, маніпуляції історичними фактами та викривлення реальності. На наше переконання, протидія цим наративам має ґрунтуватися на прозорості, об'єктивності та розвитку критичного мислення серед населення.

З урахуванням викладеного вище, важливим є формування комплексного підходу до захисту інформаційного простору, що включатиме технологічні, правові, соціальні та освітні заходи. Гадаємо, лише така інтегративна стратегія дозволить забезпечити стійкість суспільства до сучасних інформаційних загроз і зміцнити національну безпеку в умовах глобалізованого цифрового світу.

ЛІТЕРАТУРА:

1. Baranovsky-Dewey A. Determinants Of The Timing And Intensity Of Propaganda Attacks. St Antony's International Review. 2019. Vol. 14. No. 2. P. 120–136.

2. Crilley K. Information warfare: new battle fields. Terrorists, propaganda and the Internet. Aslib Proceedings. 2001. Vol. 53. No. 7. P. 250–264.

3. Denisenko V. Threats of propaganda and the information war on Lithuanian security. Lithuania in the global context: national security and defence policy dilemmas. 2020. P. 235–248.

4. Huang A. Combatting and defeating Chinese propaganda and disinformation: A case study of Taiwan's 2020 elections. State-Sponsored Disinformation Around the Globe. Routledge. 2024. P. 121–136.

5. Iftime I., Iftime M. The main tools of cognitive attacks on contemporary society – disinformation and propaganda. International Scientific Conference "Strategies XXI". "Carol I" National Defence University. 2023. Vol. 19. P. 306–311.

6. Kiforchuk K. Frequency analysis of russian propaganda telegram channels. Theoretical and Applied Cybersecurity. 2023. Vol. 5. No. 1.

7. Kravchenko O., Veklych V., Krykhivskyi M., Madryha T. Cybersecurity in the face of information warfare and cyberattacks. Multidisciplinary Science Journal. 2024. Vol. 6.

8. Macdonald S. Propaganda and Information Warfare in the Twenty-First Century: Altered images and deception operations. Routledge. 2006.

9. Mandić J., Klarić D. Case study of the russian disinformation campaign during the war in Ukraine – propaganda narratives, goals, and impacts. National Security and the Future. 2023. Vol. 24. No. 2. P. 97–140.

10. Melnykova-Kurhanova O. Propaganda Narratives in the Information Space During the Siege of Mariupol in 2022. Societas/Communitas. 2024. No. 37(1). P. 107–118.

11. Rosenfeld B., Wallace J. Information Politics and Propaganda in Authoritarian Societies. Annual Review of Political Science. 2024. Vol. 27.

12. Shults M. I. Information Warfare in the Digital Age – Propaganda, Cyberattacks and the Protection of. Institute for Peace and Prosperity. 2021.

13. Tarasiuk Y. Russian narratives in Turkey: historical background and propaganda in media. European Political Science. 2024. P. 1–11.

14. Wehner M. Hacking, propaganda and electoral manipulation. Europe. 2017.

15. Williams, E. M., & Carley, K. M. Search engine manipulation to spread pro-Kremlin propaganda. (2023). Harvard Kennedy School Misinformation Review.

REFERENCES:

1. Baranovsky-Dewey, A. (2019). Determinants Of The Timing And Intensity Of Propaganda Attacks. St Antony's International Review, 14(2), 120-136. [in English]
2. Crilley, K. (2001, September). Information warfare: new battle fields Terrorists, propaganda and the Internet. In Aslib Proceedings (Vol. 53, No. 7, pp. 250-264). MCB UP Ltd. [in English]
3. Denisenko, V. (2020). Threats of propaganda and the information war on Lithuanian security. Lithuania in the global context: national security and defence policy dilemmas, 235-248. [in English]
4. Huang, A. (2024). Combatting and defeating Chinese propaganda and disinformation: A case study of Taiwan's 2020 elections. In State-Sponsored Disinformation Around the Globe (pp. 121-136). Routledge. [in English]
5. Iftime, I., & Iftime, M. (2023). The main tools of cognitive attacks on contemporary society–disinformation and propaganda. In International Scientific Conference» Strategies XXI» (Vol. 19, pp. 306-311). « Carol I» National Defence University. [in English]
6. Kiforchuk, K. (2023). Frequency analysis of russian propaganda telegram channels. Theoretical and applied cybersecurity, 5(1). [in English]
7. Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. Multidisciplinary Science Journal, 6. [in English]
8. Macdonald, S. (2006). Propaganda and Information Warfare in the Twenty-First Century: Altered images and deception operations. Routledge. [in English]
9. Mandić, J., & Klarić, D. (2023). Case study of the russian disinformation campaign during the war in Ukraine–propaganda narratives, goals, and impacts. National security and the future, 24(2), 97-140. [in English]
10. Melnykova-Kurhanova, O. (2024). Propaganda Narratives in the Information Space During the Siege of Mariupol in 2022. Societas/Communitas, (37 (1)), 107-118. [in English]
11. Rosenfeld, B., & Wallace, J. (2024). Information Politics and Propaganda in Authoritarian Societies. Annual Review of Political Science, 27. [in English]
12. Shults, M. I. (2021). Information Warfare in the Digital Age–Propaganda, Cyberattacks and the Protection of. Institute for Peace and Prosperity. [in English]
13. Tarasiuk, Y. (2024). Russian narratives in Turkey: historical background and propaganda in media. European Political Science, 1-11. [in English]
14. Wehner, M. (2017). Hacking, propaganda and electoral manipulation. Europe.
15. Williams, E. M., & Carley, K. M. (2023). Search engine manipulation to spread pro-Kremlin propaganda. Harvard Kennedy School Misinformation Review. [in English]

Strategies for protecting national security against information attacks and propaganda

Krap Andriy Pavlovych

PhD in Political Sciences,
Associate Professor at the Department
of Social and Humanitarian
and Fundamental Disciplines
Interregional Academy of Personnel
Management
Frometovskaya str., 2, Kyiv, Ukraine
ORCID: 0000-0002-4443-3364

The article examines modern strategies for protecting national security against information attacks and propaganda, which have become an integral part of hybrid threats in the globalized digital world. The study aims to comprehensively conceptualize the nature of information threats and develop effective mechanisms to counteract them. Key aspects of information warfare, the mechanisms of propaganda influence, and the role of digital technologies in its dissemination are analyzed.

To achieve this goal, an interdisciplinary approach was applied, including systems analysis, comparative analysis, historical-genetic methods, structural-functional methods, and content analysis of contemporary propaganda narratives. This ensured a multidimensional perspective on phenomena associated with information warfare.

As a result of the study, the main types of information attacks and propaganda narratives were identified, particularly those targeting the manipulation of public consciousness, distortion of historical facts, and undermining trust in state institutions. It was established that effective counter-strategies should encompass the development of cybersecurity, the enhancement of media literacy, the creation of a positive informational agenda, and the improvement of the regulatory framework.

The scientific novelty of the article lies in synthesizing theoretical and practical approaches to safeguarding the information space, considering cognitive, technological, and sociocultural aspects. The theoretical significance of the work is in systematizing knowledge about the mechanisms of information warfare, while its practical relevance lies in developing recommendations for state institutions, civil society, and international organizations.

Key words: *information warfare, propaganda, national security, disinformation, social networks, cybersecurity, cognitive attacks.*