

УДК 355.1

DOI <https://doi.org/10.32782/1992-5786.2025.98.13>**Є. В. Денисенко**

кандидат педагогічних наук,
начальник відділу організації заочного та дистанційного навчання
Національної академії Національної гвардії України
<https://orcid.org/0000-0003-3776-0823>

ТЕОРЕТИЧНІ ЗАСАДИ ВПЛИВУ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ НА КУРСАНТІВ ВІЙСЬКОВИХ ЗАКЛАДІВ ОСВІТИ: СПОСОБИ БОРОТЬБИ

Інформаційний тероризм у сучасному світі став одним із найнебезпечніших інструментів гібридної війни, що активно використовується для підризу морально-психологічного стану цивільного населення та військових. Війна Росії проти України яскраво демонструє масштаби та ефективність застосування дезінформації, пропаганди та маніпуляцій у інформаційному просторі. Особливо вразливою до таких впливів групою є курсанти військових закладів освіти, які тільки розпочинають свою професійну підготовку і формують основи своєї особистої стійкості до зовнішніх викликів. Відповідно, важливо на початку навчання курсантів пояснити їм, що існує багато дезінформації, яку необхідно вміти розпізнати та застосовувати певні методи протидії цьому явищу. Інформаційний тероризм є складовою частиною гібридної війни та часто використовується як інструмент пропаганди, дезінформації та психологічного тиску. Його основні характеристики складаються з багатьох пунктів, які необхідно розуміти для власного захисту від маніпуляцій.

У статті проаналізовано теоретичні засади впливу інформаційного тероризму на курсантів військових закладів освіти, що використовуються в умовах війни та способи боротьби з ним. Окрему увагу приділено досвіду України, яка зіткнулася з масованими інформаційними атаками, спрямованими на дискредитацію армії, деморалізацію населення та руйнування єдності суспільства. Описано вплив дезінформації та пропаганди на морально-психологічний стан курсантів, вказуючи на загрози, пов'язані зі зниженням їхньої боєздатності та загальною вразливістю до інформаційних атак. Наведено ключові аспекти інформаційних атак, які застосовуються Росією проти України. Зазначено, що військові заклади освіти повинні приділити достатню кількість часу підготовці курсантів до можливих атак інформаційного тероризму та боротьби з ним, що є великим завданням забезпечення моральної стійкості. Представлено способи боротьби з інформаційним тероризмом у військових закладах освіти, які підкріплені реальними прикладами та демонструють комплексний підхід. Визначено, що найефективнішими способами протидії інформаційному тероризму є підвищення інформаційної грамотності, розвиток критичного мислення, запровадження програм психологічної стійкості, а також використання сучасних технологій для моніторингу та нейтралізації інформаційних загроз.

Ключові слова: інформаційний тероризм, гібридна війна, боротьба з пропагандою, підготовка курсантів, інформаційна війна, морально-психологічний стан курсантів.

Постановка проблеми. Сьогодення представлено вираженою жорстокістю реальності, в якій нині приходится жити українському населенню, це пов'язано з активними бойовими діями на її території. Окрім фізичного насилля та матеріальних втрат, проблема також значно виражена у психологічному аспекті, від якого залежить моральний дух українців. Великого значення набуває налаштованість українських військових, в руках яких знаходиться можливість перемоги України у плинному військовому конфлікті. Згадуючи психологічний аспект, мова йде про наступні його складові: рівень мотивації, впевненість в собі та в своїх діях, зберігання ефективності у виконанні завдань, установки та принципи, які визначають поведінку військового, його лояльність до держави, команди та служби, сприйнятливості до маніпуляцій, дезінформації або пропаганди

та здатність їм протистояти. Останній, вищеведений пункт психологічних аспектів військового постає проблемою в середовищі сучасного інформаційного простору, який характеризується швидким поширенням даних – вони зі свого боку можуть мати як позитивний, так і деструктивний вплив. У питанні ефекту поширення політичної інформації зі сторони країни-агресора, здебільшого вона постає у вигляді інформаційного тероризму – одна з форм сучасної гібридної війни, що стає потужним інструментом психологічного тиску.

Аналіз останніх досліджень і публікацій. Аналіз останніх літературних джерел, пов'язаних із питанням інформаційного тероризму, виокремив наступних вітчизняних науковців: Саган О. В., в роботах якої висвітлено аналіз політики протидії медіа-інформаційному тероризму у системі політики національної безпеки України [10]. В свою

чергу, Бех В. П. та Лепський М. А. розглядають концепцію гібридної війни як комбінацію конвенційних, іррегулярних й асиметричних засобів, які включають постійну маніпуляцію політичним та ідеологічним конфліктом [2]. Зокрема, Додонов Р. розглядає поняття схізмогенезу, як опис подій на Сході України, що можна зіставити із результатом виконаного плану російської пропаганди на формування депресивної думки «свій-чужий» [6]. Разом із попереднім автором це питання також піднімають у своїх роботах Фадаєв В. та Кобалія Д. [13], та Скворець В. [11]. Наступним чином, у виділені важливості інформаційних технологій як руйнівного фактору при боротьбі з тероризмом, розглядає Мамчин М. М. [8].

Віддаючи належне українським науковцям, також не можна забути про іноземних авторів, які проводили аналіз та дослідження ефекту інформаційного тероризму в межах гібридних війн: Фраєр Н. [19]; Роберт А. Ньюсон [20]; Франк Хофман [18]; Рассел Гленн [17] та інші.

Незважаючи на зростання кількості досліджень у сфері інформаційної безпеки, питання впливу інформаційного тероризму на особистість курсантів та ефективні методи протидії цьому явищу залишаються недостатньо вивченими. Важливість дослідження зумовлена необхідністю розробки дієвих методик та підходів, спрямованих на захист курсантів від негативного впливу інформаційного тероризму, підвищення їхньої стійкості до дезінформаційних атак т/а формування критичного мислення у мінливому середовищі.

Виділення невирішених раніше частин загальної проблеми. Саме тому важливо приділити значну увагу вивченню питання щодо інформаційного тероризму та способів боротьби з ним, адже військовослужбовці, зокрема курсанти військових закладів освіти, є однією з найбільш уразливих категорій, оскільки вони перебувають у специфічному середовищі, де інформаційна атака може спричинити зниження морально-психологічного стану, порушення єдності колективу та зменшення рівня боєздатності.

Тож, **метою статті є** визначення основних механізмів впливу інформаційного тероризму на курсантів військових закладів освіти та розробка ефективних способів боротьби, на прикладі війни Росії з Україною.

Виклад основного матеріалу. Навмисне використання інформаційних технологій, медіа та інших каналів комунікації з метою поширення страху, хаосу та дестабілізації суспільства, маніпулювання масовою свідомістю або впливу на прийняття рішень з боку державних, військових чи соціальних структур – це те з чим стикаються громадяни та військові країн, які потерпають від озброєних конфліктів. Інформаційний тероризм є складовою частиною гібридної війни та часто

використовується як інструмент пропаганди, дезінформації та психологічного тиску. Його основні характеристики складаються з багатьох пунктів, які необхідно розуміти для власного захисту від маніпуляцій (рис. 1).

Якщо розглядати події пов'язані з повномасштабним вторгненням Росії проти України, нерідко можна спостерігати за наступними прикладами інформаційної пропаганди, яка пов'язана з виправдуванням агресії, публікацією аморального медіа-контенту, розповсюдженням, знищуючих моральний дух військових, новин про ситуацію на фронті.

Інформаційна пропаганда відбувається через такі засоби: масові дезінформаційні кампанії щодо «легітимності» окупації Криму та Донбасу та інших областей країни; використання фейкових новин про ситуацію на фронті для деморалізації населення та військового духу; активне використання ботів і тролів у соціальних мережах для створення паніки та розповсюдження пропаганди (Telegram, Viber, WhatsApp).

Вкиди про нібито злочини української армії для дискредитації Збройних Сил України на міжнародній арені. Виходячи з інформації, зображеної на рисунку 1, формується твердження, що інформаційний тероризм використовує широкий спектр інструментів і методів, спрямованих на дестабілізацію суспільства, підрив морально-психологічного стану та маніпулювання громадською думкою. У контексті війни, зокрема агресії Росії проти України, ці методи стали ключовим елементом гібридної війни. Опишемо основні інструменти інформаційного тероризму:

1) Соціальні мережі: поширення фейкових новин через ботів, тролів та фейкові акаунти; масове поширення панічних повідомлень, спрямованих на створення хаосу; використання алгоритмів для таргетування вразливих груп населення.

2) Мас-медіа: контрольовані медіаресурси, які транслюють пропагандистський контент; підготовка «псевдонovin», які викликають недовіру до військового керівництва та уряду; використання телеканалів і радіо для масового поширення пропаганди.

3) Кіберзагрози: злами сайтів та порталів із метою розміщення фейкових новин; кібератаки на інфраструктурні об'єкти з подальшим поширенням дезінформації про їх наслідки; викрадення даних для шантажу або публікації компромату.

4) Візуальний контент: фальшиві фотографії та відео, які ілюструють нібито катастрофічні події; монтаж відео з метою перекручування реальності; використання графічних матеріалів (меми, плакати) для емоційного впливу.

5) Мобільні платформи: масові SMS-розсилки з погрозами або панічними закликами; викори-

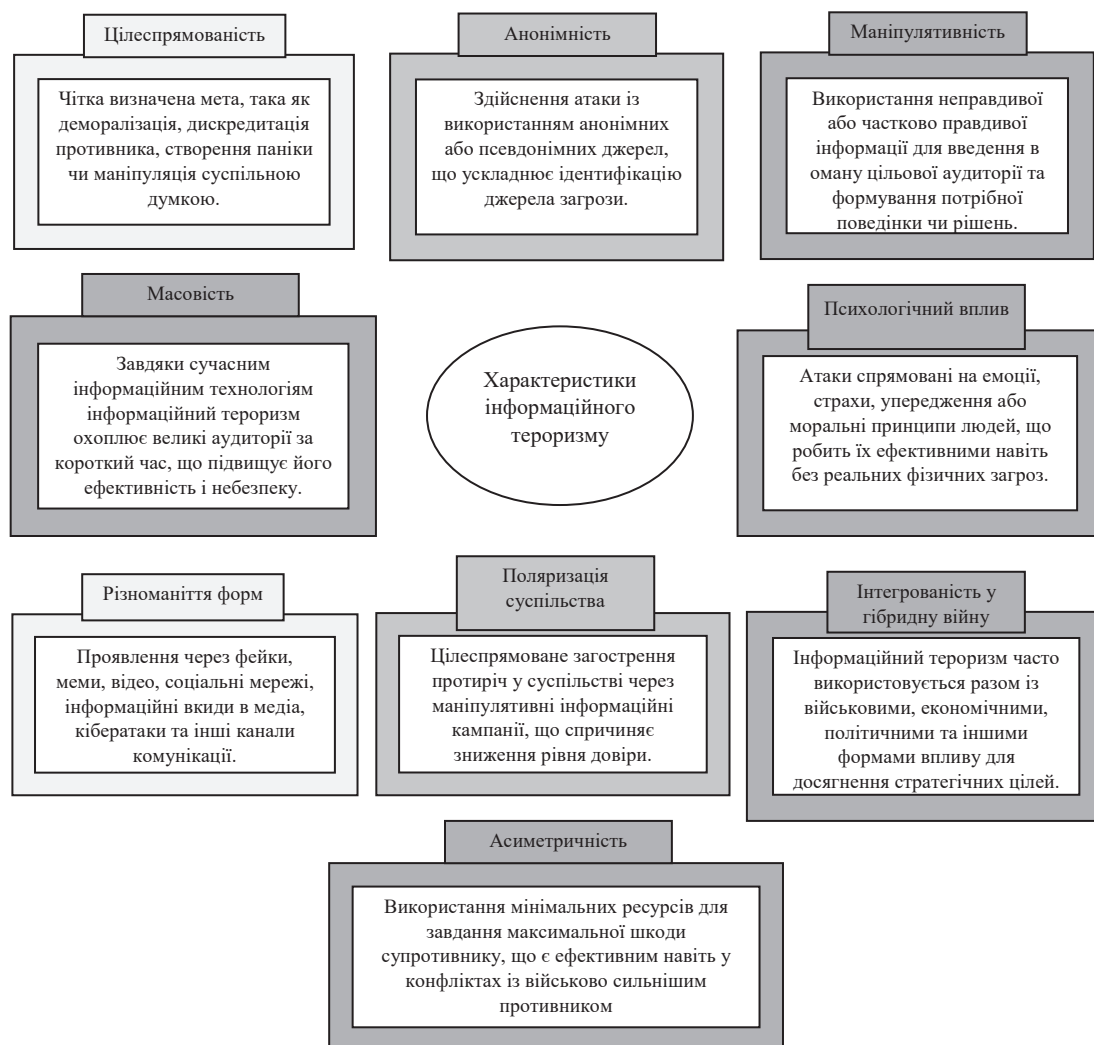


Рис. 1. Основні характеристики інформаційного тероризму

Джерело: сформовано автором згідно [2]

стання месенджерів (Telegram, WhatsApp) для поширення фейків у закритих групах.

6) Псевдоексперти та лідери думок: залучення «експертів», які транслюють дезінформацію у публічному просторі; використання популярних блогерів для підриву довіри до держави чи військових [7].

Надані інструменти широко використовуються для зловмисних цілей інформаційних терористів, ефективно проводячи заплановану «програму» вибираючи один або комбінуючи декілька методів одночасно. Щодо прикладів застосування інформаційного тероризму Росії проти України, увагу слід звернути на відомі події: фейкові новини про «знищення української армії» для деморалізації військових; використання проросійських медіа для виправдання агресії та поширення тези про «громадянську війну»; організація «флешмобів» у соціальних мережах з метою дискредитації Збройних Сил України; маніпуляції навколо гуманітарної ситуації (наприклад, створення фейків про «геноцид російськомовних»).

Таким чином війна Росії проти України стала прикладом масштабного застосування інформаційних атак як одного з основних інструментів гібридної війни. Такі інформаційні атаки спрямовані не лише на українських громадян і військових, а й на міжнародну спільноту, використовуючи багаторівневий підхід до впливу. Основні напрямки інформаційних атак є небажаним досвідом українського суспільства та української армії, який став уроком в навчанні не тільки для українського населення, а й для міжнародної арени (табл. 1).

Виходячи з вищезазначеного у таблиці 1, можна побачити, що застосовується системний підхід Росії до інформаційних атак у війні проти України та підкреслює необхідність комплексної протидії цим загрозам, адже зрозуміло, що дезінформація та пропаганда мають потужний психологічний вплив на суспільство, особливо в умовах війни, коли люди перебувають у стані підвищеної емоційної напруги та вразливості.

Таблиця 1

Досвід війни Росії проти України: ключові аспекти інформаційних атак

№	Категорія	Опис	Приклади війни Росії проти України
1	Основні напрямки інформаційних атак	Зусилля спрямовані на маніпуляцію громадською думкою, деморалізацію населення та армії, підтримку міжнародної підтримки України.	- Створення фейкових новин про «біолабораторії» Україні. - Просування наративу «Україна – держава, що провокує війну».
2	Інструменти інформаційних атак	Засоби та технології, які використовуються для поширення дезінформації, маніпуляції емоціями та формування спотвореної реальності.	- Використання соціальних мереж для розповсюдження фейків. - Deepfake - відео із «заявами» українських лідерів.
3	Ключові аспекти інформаційних атак	Деталі тактик, методів та цілей, які застосовуються для досягнення інформаційного впливу.	
	3.1. Маніпуляція емоціями	Використання страху, ненависті та розгубленості для дестабілізації населення та військових.	- Відео з погрозами населенню окупованих територій. - Фейкові повідомлення про евакуацію через «нові атаки».
	3.2. Створення фейкової реальності	Пропаганда альтернативної картини подій, яка дискредитує Україну та виправдовує дії Росії.	- Твердження про «визвольну місію» Росії. - Фото з інших конфліктів, представлені як кадри з України.
	3.3. Цілеспрямовані кібератаки	Використання технологій для паралізації інфраструктури, викрадення даних та поширення пропаганди.	- Злам українських урядових сайтів із залишенням повідомлень, спрямованих на деморалізацію. - Вірусні атаки (наприклад, WhisperGate).
	3.4. Розкол суспільства	Просування суперечливих тем, які провокують конфлікти серед населення.	- Розпалювання мовного питання. - Фейкові заяви про «відмову західних країн» підтримувати Україну.
	3.5. Дискредитація військових	Підлив довіри до українських збройних сил через поширення фейків про їхню нібито жорстокість, некомпетентність чи зраду.	- Відео, де ЗСУ звинувачують у обстрілі мирного населення. - Висвітлення фейкових «злочинів» українських військових.
	3.6. Деморалізація міжнародної підтримки	Спотворення фактів для зменшення обсягу допомоги Україні з боку союзників.	- Поширення наративу про «виснаження ресурсів» Заходу через підтримку України. - Фейки про корупцію у використанні міжнародної допомоги.

Джерело: сформовано автором згідно [5; 12; 14; 16]

Основним завданням цих інструментів є маніпуляція свідомістю, створення хаосу, паніки та формування певної моделі поведінки, яка вигідна агресору для досягнення своїх цілей.

Звісно, що настрої цивільного населення є важливим для держави, однак не можна забувати про наших захисників, які боронять нашу країну та молодих курсантів, яким необхідно підтримувати їх психологічний стан та захищати від інформаційного тероризму. Важливим у розгляді даного питання є захист курсантів військових підрозділів від інформаційного тероризму з боку країни-агресора, адже від їх готовності, рішучості до перемоги, вмотивованого морального стану залежить не тільки успішність операцій, а й життя окремого військового, команди та загалом українського населення.

Слід відмітити, що курсанти військових навчальних закладів є особливо вразливою категорією до загроз морально-психологічного характеру в умовах гібридної війни. Через специфіку їхньої підготовки, постійний тиск під час навчання

та необхідність формувати стійкість до стресів, інформаційний тероризм може мати на них суттєвий негативний вплив.

Одна з ключових загроз – деморалізація через поширення дезінформації, спрямованої на формування негативного уявлення про військову службу, перспективи в професії або загальну ситуацію в країні. Фейки про «зраду» керівництва, величезні втрати чи неспроможність Збройних Сил України можуть викликати у курсантів сумніви у правильності їхнього професійного вибору, знижувати мотивацію до навчання та служби, що негативно може впливати на їх подальше перебування у військовому закладі освіти.

Також, ще однією важливою складовою та серйозною загрозою є психологічний тиск через соціальні мережі. Курсанти часто використовують ці платформи для комунікації, і через них можуть поширюватися фейкові повідомлення, маніпулятивні відео чи заклики до сумнівних дій. Боти й тролі, створюючи ілюзію масовості певних думок, впливають на емоційний стан курсантів,

викликаючи почуття ізольованості чи розгубленості. Розпалювання внутрішніх конфліктів є ще однією загрозою. Через маніпуляції на темах мовного, етнічного чи регіонального характеру пропаганда намагається посіяти розбрат серед курсантів, що підриває командний дух і ускладнює їхню адаптацію до військового середовища. Не менш небезпечною є моральна дезорієнтація курсантів під час навчання, викликана переконаченням понять про героїзм, патріотизм чи етичні цінності. Наприклад, пропаганда може підносити ворога як жертву, а захисників країни виставляти в негативному світлі. Це спотворює систему цінностей курсантів і знижує їхню здатність адекватно оцінювати ситуацію.

Постійний інформаційний тиск також може спричинити емоційне вигорання та стрес, особливо якщо курсанти не мають достатньо навичок для протидії інформаційним атакам. Це проявляється у вигляді тривожності, зниження впевненості у власних силах, труднощів у концентрації

та загальної втоми. Сукупність цих факторів ставить під загрозу не лише психологічне здоров'я курсантів, але й їхню здатність виконувати майбутні службові обов'язки. Тому критично важливо впроваджувати у навчання додаткові програми з підвищення інформаційної грамотності, тренінги з емоційної стійкості та заходи, які сприяють зміцненню морального духу та командної згуртованості в середовищі курсантів.

Таким чином, військові заклади освіти повинні приділити достатню кількість часу підготовці курсантів до можливих атак інформаційного тероризму та боротьби з ним, що є великим завданням забезпечення моральної стійкості під впливом психологічних маніпуляцій противника, адже зараз це є однією з найнебезпечнішої зброї сучасності (табл. 2).

Отже, запропоновані способи боротьби з інформаційним тероризмом у військових закладах, підкріплені реальними прикладами, демонструють комплексний підхід до протидії цьому

Таблиця 2

Способи боротьби з інформаційним тероризмом у військових закладах освіти

№	Спосіб	Опис	Приклад застосування	Очікуваний результат
1	Підвищення інформаційної грамотності курсантів	Навчання основам аналізу інформації, перевірки джерел та ідентифікації фейків.	Проведення тренінгів з OSINT (Open Source Intelligence) для виявлення маніпулятивних матеріалів.	Зниження впливу маніпуляцій та дезінформації на курсантів.
2	Розробка програм психологічної стійкості	Навчання подоланню стресу та емоційної стійкості до тиску через інформаційні атаки.	Запровадження регулярних занять із військовими психологами, спрямованих на управління стресом.	Покращення емоційної стабільності курсантів.
3	Формування критичного мислення	Розвиток навичок аналізу та логічного мислення для розпізнавання маніпуляцій.	Використання кейсів аналізу фейкових новин під час лекцій з інформаційної безпеки.	Здатність курсантів уникати маніпуляцій і пропаганди.
4	Використання сучасних технологій моніторингу	Впровадження інструментів аналізу даних та виявлення дезінформації.	Використання програмного забезпечення для моніторингу соціальних мереж, таких як CrowdTangle.	Раннє виявлення інформаційних загроз.
5	Організація кіберзахисту	Захист інформаційних систем військових закладів від атак.	Встановлення SIEM-систем для аналізу логів і виявлення аномалій у мережах.	Підвищення рівня кібербезпеки.
6	Практичні тренінги та симуляції	Проведення навчань з моделювання реальних інформаційних атак.	Організація симуляцій кібер- та інформаційних атак з використанням платформи CyberRange.	Підготовка курсантів до реагування на реальні загрози.
7	Формування команд інформаційного реагування	Створення груп для аналізу та протидії інформаційним загрозам.	Запуск проекту «ІнфоВарта» для моніторингу та аналізу ворожої пропаганди у соцмережах.	Швидке реагування на нові виклики та підвищення ефективності протидії інформаційним атакам.
8	Популяризація медіаграмотності у повсякденному житті	Навчання відповідального користування інформаційними ресурсами та соцмережами.	Лекції про безпеку поширення неперевіраних новин і вплив соціальних мереж на формування думок.	Зниження поширення фейків серед курсантів і суспільства.

Продовження таблиці 2

9	Співпраця з інформаційними експертами	Залучення фахівців для навчання та консультування курсантів з питань інформаційної безпеки.	Проведення гостьових лекцій із провідними експертами з інформаційних загроз, наприклад, представниками StopFake.	Розширення знань курсантів та обмін практичним досвідом із фахівцями галузі.
10	Створення бази знань з інформаційних атак	Формування електронної бази даних для вивчення прикладів дезінформації та методів боротьби.	Розробка інтерактивного ресурсу з архівом фейкових новин та способами їхнього спростування.	Забезпечення доступу курсантів до систематизованої інформації про інформаційні загрози.

Джерело: сформовано автором згідно (1; 9; 15; 21)

явищу. Кожен із методів спрямований на різні аспекти захисту курсантів: від підвищення їхньої інформаційної грамотності та формування критичного мислення до впровадження сучасних технологій для моніторингу загроз і організації команд швидкого реагування. Реальні кейси як використання платформ для виявлення фейкових новин або проведення симуляцій інформаційних атак, підкреслюють практичність і ефективність цих заходів.

Важливим також є впровадження програм психологічної стійкості та залучення експертів до навчального процесу, що забезпечує як професійний розвиток курсантів, так і підвищення їхньої готовності до реальних викликів. Системна реалізація цих підходів дозволить створити стійке середовище у військових закладах освіти, яке здатне ефективно протидіяти інформаційному тероризму та інформаційним атакам з боку агресора. Це, у свою чергу, сприятиме підвищенню рівня інформаційної безпеки, збереженню боєздатності майбутніх офіцерів та зміцненню обороноздатності країни в умовах гібридної війни.

Висновок. Інформаційний тероризм у сучасних умовах війни є потужним інструментом впливу, який спрямований на підлив морально-психологічного стану військовослужбовців, зокрема курсантів військових закладів. У процесі війни Росії проти України інформаційні атаки стали складовою гібридної агресії, що включає маніпуляцію фактами, поширення дезінформації та пропаганду, спрямовану на деморалізацію як військових, так і цивільного населення. Для військових закладів освіти особливо важливо впроваджувати системні заходи з протидії цим загрозам. Ключовими напрямками є: підвищення інформаційної грамотності курсантів, розвиток критичного мислення, створення програм психологічної стійкості та використання сучасних технологій для моніторингу й аналізу інформаційних загроз. Важливу роль відіграє також співпраця з інформаційними експертами, організація практичних тренінгів і формування команд швидкого реагування на інформаційні атаки.

Реалізація запропонованих методів дозволить не лише захистити курсантів від негативного впливу інформаційного тероризму, а й підготувати їх до активної протидії таким загрозам у реальних умовах. Формування у курсантів стійкості до дезінформації та навичок ефективного використання інформації є необхідною умовою для забезпечення боєздатності армії та зміцнення інформаційної безпеки держави в цілому.

Список використаної літератури:

- 10 інструментів для відстеження інформаційних впливів онлайн. URL: <https://internews.ua/opportunity/10-tools-for-tracking-information> (дата звернення: 15.12.2024).
- Бех В. П. Лепський М. А. Гібридна війна: in verbo et in praxi : монографія / Донецький національний університет імені Василя Стуса / під. заг. ред. проф. Р.О. Додонова. Вінниця : ТОВ «НіланЛТД», 2017. 412 с. URL: <https://jmonographs.donnu.edu.ua/article/view/3781> (дата звернення: 15.12.2024).
- Війни інформаційної епохи: міждисциплінарний дискурс: монографія/за ред. В.А. Кротюка. Харків: ФОП Федорко М. Ю. 2021. 558 с. URL: <http://library.dnu.dp.ua/vijni.pdf> (дата звернення: 15.12.2024).
- Громадська організація «Центр Медіареформи». URL: <https://www.stopfake.org/uk/pro-nas/> (дата звернення: 15.12.2024).
- Дезінформаційна мережа в Telegram: як працює російська пропаганда на окупованих територіях. URL: <https://euneighbourseast.eu/uk/news/stories/dezinformaczijna-merezha-v-telegram-yak-praczuuye-rosijska-propaganda-na-okupovanyh-terytoriyah/> (дата звернення: 15.12.2024).
- Додонов Р. О. Конфлікт на Сході України у дзеркалі соціально-філософської рефлексії : монографія / Р. О. Додонов, Український інститут стратегій глобального розвитку та адаптації. Вінниця: ГЛОБУС ПРЕСС, 2016. 200 с. URL: <https://uisgda.com/assets/files/monogr-konflikt8.pdf> (дата звернення: 15.12.2024).

7. Малахов Г. Б. Використання кіберпростору як інструменту інформаційного тероризму. *Інформація і право*. № 3 (50). 2024. URL: <http://il.ippi.org.ua/article/view/311671> (дата звернення: 15.12.2024).
8. Мамчин М., Яричевська Я. Маркетинговий погляд на тероризм. *Економіка та суспільство* (45). 2022. URL: <https://doi.org/10.32782/2524-0072/2022-45-15> (дата звернення: 15.12.2024).
9. На базі НАУ створили кіберполігон Cyber Range UA. Тут навчатимуть і студентів, і спеціалістів держустанов. URL: <https://dou.ua/lenta/news/about-cyber-range-ua/> (дата звернення: 15.12.2024).
10. Сеган О. В. Протидія медіа-інформаційному тероризму як питання національної безпеки України. – Рукопис. Дисертація на здобуття наукового ступеня кандидата політичних наук за спеціальністю 21.01.01 – основи національної безпеки держави (політичні науки). Національний інститут стратегічних досліджень, Київ, 2021. URL: <https://niss.gov.ua/sites/default/files/2021-04/06.04.2021-sagan-o.-dis.rab.pdf> (дата звернення: 15.12.2024).
11. Скворець Володимир. Внутрішні передумови формування цивілізаційного конфлікту в Україні. Схід, спецвипуск, лютий 2015. № 2 (134): 104.
12. Субота І. Як і навіщо російська пропаганда шукає біолабораторії США в Україні та світі? *Українська правда*. 2022. URL: <https://www.pravda.com.ua/columns/2022/09/22/7368473/> (дата звернення: 15.12.2024).
13. Фадєєв Володимир та Дмитро Кобалія. Від різниці до схізмогенезу: про соціокультурні передумови української кризи. Звіт з науково-дослідної роботи 3/2 «Витоки і динаміка східноукраїнського конфлікту». Київ, Український інститут стратегій глобального розвитку та адаптації, 2015.
14. Через Telegram та TikTok-блогерів Росія найбільше поширює пропаганду та дезінформацію — Сагайдак. URL: <https://suspilne.media/culture/643506-cerez-telegram-ta-tiktok-blogeriv-rosia-najbilse-rozpovisudzue-propagandu-ta-dezinformaciu-sagajdak/> (дата звернення: 15.12.2024).
15. Що таке SIEM? Інформація про безпеку та управління подіями. URL: <https://gridinsoft.ua/siem> (дата звернення: 15.12.2024).
16. Як війна в Україні викликала революцію в розсекреченні західних розвідданих. URL: <https://www.bbc.com/ukrainian/news-64117433> (дата звернення: 15.12.2024).
17. Dr. Russell W. Glenn Thoughts on “Hybrid” Conflict. *Small Wars Journal*. 2022. URL: <https://smallwars-journal.com/wp-content/uploads/2022/02/188-glenn.pdf> (дата звернення: 15.12.2024).
18. Frank J. Hoffman Conflict in the 21st Century: The Rise of Hybrid Wars. 2007. URL: https://www.potomac-institute.org/images/stories/publications/potomac_hybridwar_0108.pdf (дата звернення: 15.12.2024).
19. Nathan Freier (2018). The Darker Shade of Gray: A New War Unlike Any Other. *Center for Strategic and International Studies*. URL: <https://www.csis.org/analysis/darker-shade-gray-new-war-unlike-any-other> (дата звернення: 15.12.2024).
20. Robert A. Newson Why the US Needs a Strategy To Counter 'Hybrid Warfare'. *Defence One*. 2014. URL: <https://www.defenseone.com/ideas/2014/10/why-us-needs-strategy-counter-hybrid-warfare/97259/?oref=d1-author-river> (дата звернення: 15.12.2024).
21. What is Open-Source Intelligence? URL: <https://www.sans.org/blog/what-is-open-source-intelligence/> (дата звернення: 15.12.2024).

Denysenko Ye. Theoretical foundations of the impact of information terrorism on cadets of military educational institutions: ways to combat

Information terrorism in the modern world has become one of the most dangerous components of hybrid warfare, actively used to undermine the moral and psychological state of the civilian population and the military. Russia's war against Ukraine clearly demonstrates the scale and effectiveness of disinformation, propaganda and manipulation in the information space. The group that is particularly vulnerable to such influences is the cadets of military educational institutions who are just starting their professional training and forming the basis of their personal resilience to external challenges. Accordingly, it is important to explain to cadets at the beginning of their training that there is a lot of disinformation that they need to be able to recognise and apply certain methods to counteract this phenomenon. Information terrorism is an integral part of hybrid warfare and is often used as a tool of propaganda, disinformation and psychological pressure. Its main characteristics consist of many points that need to be understood to protect yourself from manipulation.

The article analyses the theoretical foundations of the impact of information terrorism on cadets of military educational institutions used in wartime and ways to combat it. Particular attention is paid to the experience of Ukraine which faced massive information attacks aimed at discrediting the army, demoralising the population and destroying the unity of society. The author describes the impact of disinformation and propaganda on the moral and psychological state of cadets, pointing out the threats associated with a decrease in their combat capability and overall vulnerability to information attacks. The key aspects of information attacks used by Russia against Ukraine are presented. It is noted that military educational institutions should devote sufficient

time to preparing cadets for possible information terrorism attacks and combating them which is a major task of ensuring moral stability. The article presents ways of combating information terrorism in military educational institutions, which are supported by real-life examples and demonstrate an integrated approach. It is determined that the most effective ways to counteract information terrorism are to increase information literacy, develop critical thinking, introduce psychological resilience programmes, and use modern technologies to monitor and neutralise information threats.

Key words: *information terrorism, hybrid warfare, countering propaganda, training of cadets, information warfare, moral and psychological state of cadets.*