МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН ТА СТРАТЕГІЧНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
Ніна РЖЕВСЬКА
«07» 06 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «ІНФОРМАЦІЙНІ ВІЙНИ В СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИНАХ»

Виконавець: здобувач вищої освіти 4 курсу, 409 групи, Половко Анна Сергіївна

Керівник: кандидат історичних наук, доцент, професор кафедри соціології та політичних наук Сальнікова Наталія Валеріївна

Нормоконтролер: Наталія САЛЬНІКОВА

КИЇВ 2024

ЗМІСТ

ВСТУП

Актуальність теми. Специфіка сучасних міжнародних відносин у багатьох аспектах зазнала значних змін. Створення атомної бомби в середині XX століття унеможливило прямі військові конфлікти між провідними державами, а з розвитком наприкінці XX – на початку XXI століття інформаційних технологій та постіндустріального устрою в економіці головним знаряддям боротьби став вплив у засобах масової інформації (ЗМІ) населення країни-об'єкта з його дестабілізації та досягнення своїх намірів.

Вибрана тема є в даний час особливо актуальною, так як, по-перше, методи інформаційного впливу на соціум активно розвиваються і вимагають їх ретельного аналізу та осмислення. По-друге, в виду геополітичної ситуації, що склалася, і неможливості піти на прямий військовий конфлікт країни залучені до інформаційного протистояння з боку зацікавлених сил.

Інформаційні війни стають все більш важливим елементом гібридної війни, що використовується для досягнення політичних цілей, включаючи дестабілізацію суспільства, підірвання довіри до влади та маніпуляцію громадською думкою. Розуміння механізмів цих процесів дозволить розробляти ефективні стратегії протидії та захисту від негативного впливу. Це може мати серйозні наслідки не лише для політичних систем країн, а й для міжнародної безпеки та стабільності. Вони можуть спровокувати міжнародні конфлікти, загострити відносини між державами та загрожувати міжнародному порядку. Тому дослідження інформаційних війн має важливе значення для забезпечення міжнародної безпеки та збереження миру.

Так як інформаційні технології швидко розвиваються, що призводить до зростання можливостей для проведення інформаційних війн. Зростає значення кібербезпеки та захисту інформаційних систем від кібератак та інших форм цифрового впливу. Таким чином, дослідження інформаційних війн є надзвичайно важливим для розробки стратегій захисту від цих загроз у сучасному цифровому світі.

Грамотний аналіз та розуміння ситуації дозволить нам виробити заходи щодо захисту інформаційного простору від зовнішнього втручання та цим звести до

мінімуму можливі загрози цьому напрямі. Дане дослідження покликане допомогти таким фахівцям, як філологи, лінгвісти, перекладачі, політологи та журналісти, розібратися в термінології та мовних технологіях сучасних інформаційних воєн.

Мета – дослідити феномен інформаційних війн у сучасних міжнародних відносинах та роль соціальних мереж як методу поширення дезінформації.

Для досягнення поставленої мети необхідно вирішити такі **завдання:**

1. Пошук та знайомство з літературою, що стосується проблеми інформаційних воєн та психологічного впливу в соціальних мережах.

2. Визначення понять «інформаційна війна», «гібридна війна».

3. Виявлення сформованих методів інформаційного протистояння.

4. Вивчення причин, що послужили формуванню такого явища як інформаційна війна з прикладу світової історії.

5. Аналіз міжнародного права як методу регулювання інформаційних війн.

6. Досліджено діяльність міжнародних організацій у врегулюванні міжнародних війн.

Об’єкт дослідження – інформаційні війни у міжнародному середовищі.

Предмет дослідження – соціальні мережі як сучасний метод ведення інформаційної війни.

Методи дослідження. В процесі написання роботи було застосовано такі методи: термінологічний (визначення термінів «міжнародні відносини», «інформаційна війна», «гібридна війна»); спостереження (дослідження становлення історичних воєн у різних країнах); аналізу та синтезу (характеристика причин та факторів формування інформаційних воєн); структурно-функціональний (дослідження основних напрямків боротьби з простором інформаційних війн у сучасних міжнародних відносинах); узагальнення (написання висновків).

Наукова новизна отриманих результатів полягає в аналізі інформаційних воєн в контексті сучасних міжнародних відносин та їх впливу на політичні, економічні та соціокультурні процеси. У роботі висвітлюється роль соціальних мереж, медіа та інших інформаційних платформ у формуванні думок громадськості та маніпулюванні інформацією для досягнення політичних цілей. Крім того,

надається акцент на важливість розвитку критичного мислення та медіаосвіти як інструментів для забезпечення інформаційної безпеки та захисту від маніпуляцій.

Практичне значення роботи полягає у тому, що матеріал дослідження може використовуватись під час навчально-виховного процесу в закладах вищої освіти, а також у наукових роботах студентів та під час проходження фахових практик.

Апробація результатів роботи полягає в тому, що основні положення, ідеї та результати дослідження представлено та обговорено на 2 науково-практичних конференціях, у тому числі міжнародній та розміщено 2 публікації:

1. Всеукраїнській науково-практичній конференції «Суспільно-політичні трансформації у XXI столітті: локальні, національні та глобальні контексти» (18.04.2024)

2. XXIV Міжнародній науково-практичній конференції здобувачів вищої освіти і молодих учених «ПОЛІТ. Сучасні проблеми науки» (2-5.04.2024)

3. Публікація в збірнику Всеукраїнської науково-практичної конференції «Суспільно-політичні трансформації у XXI столітті: локальні, національні та глобальні контексти» [42].

4. Публікація в збірнику XXIV Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених «ПОЛІТ. Сучасні проблеми науки» [43].

Структура та обсяг роботи встановлюється відповідно до поставленої мети та конкретних завдань дослідження. Вона складається із вступу, трьох розділів, висновку та списку використаної літератури.

РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНЕ ПІДГРУНТЯ РОБОТИ

1.1. Основні поняття дослідження

Міжнародні відносини – це сукупність економічних, політичних, соціальних, дипломатичних, гуманітарних та правових зв'язків між державами [44, с. 45].

Міжнародні відносини формувалися в локальних та регіональних рамках до середини XIX століття. Після цього вони вийшли на глобальний рівень, що було пов'язано із завершенням процесу перетворення світу на єдине ціле, насамперед, з формуванням світового господарства [44, с. 45].

Сучасна система міжнародних відносин перебуває у перехідному стані, де традиційні сили та закономірності, засновані на силовій взаємодії, «зіткненні» національних держав та балансі сил, взаємодіють з новими факторами та тенденціями, що розвиваються на наших очах.

Починаючи з часу Вестфальського миру, який закріпив майже на 350 років міжнародну систему, нові дійові особи та глобальні тенденції виступають у світовій політиці. Міжнародні організації, глобальна комунікаційна система, світова економічна взаємозалежність, зміна ролі військового чинника, поширення єдиної масової культури, взаємопов'язаність внутрішньополітичних та міжнародних проблем, хвилі глобальної демократизації - все це формує новий образ міжнародних відносин. [44, с. 46].

На рубежі XX – XXI століть відбулася масова комп'ютеризація та впровадження нових технологій практично у всі сфери життя. Для країни, яка прагне займати відповідне місце на міжнародній арені, розвиток інформаційно-комунікаційних технологій стає ключовою складовою. Однак, разом із очевидними перевагами науково-технічний прогрес породжує нові загрози для безпеки окремих держав та світової спільноти загалом. Уразливість інформаційного простору стає все більш очевидною, що відображається, зокрема, у з'яві поняття «інформаційна війна» [44, с. 49].

Коли ми чуємо слово «війна», зазвичай виникають асоціації зі зброєю, насильством та протистоянням. Війна – це конфлікт між політичними сутностями, який включає в себе військові (бойові) дії. Інформаційна війна, навпаки, не передбачає прямого використання зброї, але все ж включає в себе протистояння. Це протистояння здійснюється за допомогою інформаційних технологій [37, с. 226].

Термін «інформаційна війна» прийнято ототожнювати з такими поняттями, як «психологічний вплив», «маніпуляція», «інформаційна перевага». Як і будь-яка війна, інформаційна війна має в своєму розпорядженні різні способи та методи.

Поняття інформаційної війни з'явилося багато років тому, але у ЗМІ його стали популяризувати відносно нещодавно. У різних публікаціях йдеться про новий тип воєн, які прийдуть на заміну традиційним бойовим діям між арміями протиборчих сторін.

Під інформаційною війною розуміється стан протиборчих сторін, у якому здійснюється активний інформаційний вплив на інформаційні ресурси одне одного з метою отримання певного виграшу у матеріальній та інтелектуальній сфері. У літературі зустрічаються різні визначення інформаційної війни, що базуються на поняттях «інформаційна зброя», «інформаційна пропаганда», «інформаційна дія», «інформаційна агресія» та ін.[37, с. 230].

Інформація – це універсальна субстанція, яка пронизує всі сфери людської діяльності. Вона служить провідником знань та відомостей, інструментом спілкування, взаєморозуміння та співробітництва, а також впливає на формування стереотипів мислення та поведінки [37, с. 232].

Інформаційний вплив – цілеспрямоване виробництво та поширення спеціальної інформації, що надає безпосередній вплив (позитивний чи негативний) на функціонування та розвиток інформаційно-психологічного середовища держави, психіку та поведінку політичної еліти, населення [37, с. 233].

Інформаційна пропаганда – різновид інформаційного впливу, в якому здійснюється навмисний вплив на об'єкт з метою впливу на його орієнтацію, наміри та дії [37, с. 233]. Застосовується з метою:

- зміни переконань;

- стимулювання елементів поведінки, що сприяють зниженню (підвищенню) морально-психологічного стану;
- ослаблення емоційно-вольової стійкості людини [29, с. 52].

Інформаційна агресія – це дії, спрямовані на завдання противнику конкретної, відчутної шкоди у окремих сферах його діяльності [37, с. 234].

Інформаційна війна – це система відкритих та прихованих цілеспрямованих інформаційних впливів соціальних, політичних, етнічних та інших систем одна на одну. Метою цих впливів є отримання певного виграшу в матеріальній сфері, забезпечення інформаційної переваги над противником, а також завдання йому матеріального, ідеологічного або іншого збитку [37, с. 232].

Інформаційна зброя – метод, що дозволяє втілити у життя цілеспрямоване управління однією інформаційною системою в інших інтересах, що реалізує процес управління системою крізь дані, що надходять або оброблюються цією системою. Інформаційна зброя включає особливі методи, технології та інформацію, що дозволяють реалізувати силовий вплив на інформаційне місце суспільства та намести важливу шкоду політичним, оборонним, фінансовим та іншим актуально необхідним інтересам країни [37, с. 236].

Особливості інформаційної зброї відображають її відмінність від звичних видів озброєнь наступним чином:

- Асиметрія: ця особливість дозволяє окремому елементу виявитися сильнішим за всю систему. Тобто навіть невелика сила може мати значний вплив на загальний стан системи.
- Мімікрія: інформаційна зброя може приймати форму, що є типовою для даної системи, але нести зміст, який відрізняється від загальноприйнятого. Це дозволяє їй приховуватися в середовищі та виконувати свої завдання без виявлення.
- Адаптація: інформаційна зброя може змінювати середовище відповідно до вимог змісту, що вводиться. Вона може швидко адаптуватися до нових умов і змінювати свої методи впливу, щоб залишатися ефективною [29, с. 52].

Наслідком асиметрії є несподіваність, коли інформаційна зброя знаходить незахищені місця у чужій системі, де може виявитися сильнішою, ніж уся система разом.

Наслідком мімікрії є скритність, оскільки інформаційна зброя слабо розпізнається, вона повторює форму елементів, що є типовими для цієї системи, тому її важко виявити.

Наслідком адаптації є трансформація середовища, коли інформаційна зброя може змінювати оточення відповідно до вимог змісту, що вводиться, змінюючи свої методи впливу для забезпечення ефективності.

Інформаційна операція – ансамбль злагоджених та взаємопов'язаних подій з маніпулювання інформацією, що здійснюються за сукупного проекту з метою досягнення та утримання переваги через вплив на інформаційні процеси в системах ворога [36, с. 488].

Директор інформаційних військ Міністерства оборони США В. Лакер визначає інформаційну війну як сукупність заходів, спрямованих на досягнення інформаційної переваги для забезпечення національної військової стратегії. Це включає вплив на інформацію та інформаційні системи супротивника, а також зміцнення та захист власної інформації та інформаційних систем.

Ознаки інформаційної війни включають:

- Діяльність з метою завдання шкоди державним інтересам.
- Використання таємних інформаційно-психологічних операцій як організаційної форми такої діяльності.
- Застосування інформаційної зброї [21, с. 155].

Головною метою інформаційної війни є отримання політичного, військового, економічного та соціального виграшу за рахунок примусу протилежної сторони ухвалити рішення, яке відповідає намірам іншої сторони [21, с. 156].

Для досягнення своїх цілей протиборчі сторони використовують широкий арсенал засобів, що можуть впливати на інформаційні та інтелектуальні ресурси протилежної сторони. Ці засоби дозволяють маніпулювати даними та знаннями,

зокрема шляхом дезінформації, маніпуляції інформацією, та іншими способами впливу на інформаційне середовище..

При цьому організатори інформаційної війни, як правило, вирішують наступні основні завдання:

- забезпечення власної безпеки;
- порушення процесу функціонування системи органів державної влади та управління супротивника;
- вербування громадян;
- завдання шкоди різним об'єктам стратегічної інфраструктури держави противника, а також його національним інтересам;
- нав'язування власних цінностей, інтересів та пріоритетів;
- підрив національної безпеки [21, с. 156].

Однак ці завдання у своїй предметній та змістовній частинах коригуються безпосередньо в залежності від обраних ініціатором цілей та способів проведення інформаційної війни. Методами ж ведення інформаційної війни є:

- приховування важливої інформації;
- зміщення або заміна понять;
- маніпулювання суспільною свідомістю;
- використання «порожньої» інформації;
- загострення політичної боротьби, політична дестабілізація та ініціювання криз;
- створення напруженості в суспільно-політичній атмосфері;
- заподіяння шкоди у різних сферах життя держави та суспільства [21, с. 158].

Щодо об'єктів інформаційної війни, то ними можуть бути як індивідуальна та масова свідомість, так і інформаційна інфраструктура, інформаційні та психологічні ресурси, соціально-політичні системи та процеси. Особливо потужних інформаційних атак зазнають духовно-моральна і ціннісна сфера, патріотична свідомість і виховання молоді, сфера освіти.

Суб'єктами ж інформаційної війни можуть виступати [12, с. 33]:

- держави, їх союзи та коаліції;
- міжнародні організації;
- недержавні незаконні збройні формування та організації терористичної, екстремістської, радикальної політичної, радикальної релігійної спрямованості;
- транснаціональні корпорації;
- віртуальні соціальні спільноти;
- засоби масової інформації та масової комунікації;
- віртуальні коаліції.

При цьому кожен із зазначених суб'єктів в інформаційній війні переслідує свої власні інтереси. В умовах інформаційної війни її учасники:

- використовують технології маніпулювання інформацією для здійснення атак;
- використовують військові інформаційні функції підвищення загальної ефективності збройних сил;
- використовують інформаційні методи впливу на противника та інформаційні технології задля забезпечення власної безпеки [12, с. 35].

Основні сфери ведення інформаційно-психологічного протистояння – політична, дипломатична фінансово-економічна, військова [12, с. 36]

Геополітичне інформаційне протиборство - це одна з сучасних форм конкуренції між державами, а також система заходів, спрямованих на порушення інформаційної безпеки іншої держави, з метою досягнення власних геополітичних цілей. Це включає в себе проведення різноманітних інформаційних операцій та маніпуляцій, а також захисні заходи, спрямовані на відвернення подібних дій з боку інших держав [36, с. 337].

Головною метою геополітичного інформаційного протиборства є порушення інформаційної безпеки іншої держави. У ряді випадків таке протиборство спрямоване на підрив цілісності та стійкості системи державного та військового управління інших держав. Ефективний інформаційний вплив на керівництво, політичну еліту, системи

формування громадської думки та прийняття рішень, а також забезпечення інформаційної безпеки є важливими аспектами такого протиборства [15, с. 82].

Інформаційна війна є всеосяжною та цілісною стратегією, спрямованою на надання належної значущості та цінності інформації в контексті командування, управління та виконання наказів збройними силами, а також на реалізацію національної політики. Інформаційна війна охоплює всі можливості та фактори вразливості, що виникають у зростаючій залежності від інформації, а також використовується у різних конфліктах. Об'єктом уваги стають інформаційні системи, включаючи відповідні лінії передач, обробні центри та людські фактори цих систем, а також інформаційні технології, використовувані у системах озброєнь [15, с. 83].

Інформаційна війна включає наступальні та оборонні складові, проте починається з цільового проектування та розробки власної «архітектури командування, управління, комунікацій, комп'ютерів та розвідки, яка забезпечує особам, що приймають рішення, відчутну інформаційну перевагу у різних конфліктах». Це визначення, насамперед, зорієнтоване на технічне забезпечення інформаційної складової армії, а не на її змістовні аспекти [15, с. 83].

Інтернет, спочатку сприйнятий як потенційний плацдарм, надає всі умови для проведення війни, що призводить до зосередження зусиль на захисті інформаційних мереж від несанкціонованого проникнення. Зростання могутності інформаційних механізмів сучасного суспільства підсилює його залежність саме від цієї складової. Проте важливо зазначити, що інформаційна війна велася у світі і до настання епохи комп'ютерів.

1.2. Аналіз джерельної бази дослідження та методологічне підґрунтя дослідження

Зрозуміло, з огляду на колосальну значимість поняття інформаційної війни для європейської і світової історії, все так чи інакше пов'язані з її вивченням професійні історики різних країн, прихильники різних наукових шкіл і різних політичних поглядів, присвятили ряд цікавих праць.

Значну частину літератури, використаної при підготовці, склали монографії та колективні праці, випущені відомими видавництвами, серед них – Австрія, Великобританія, Німеччина, Італія, Польща, Україна, Франція, США.

Однією з найважливіших праць на тему нашого дослідження є книга «Теорія інформаційної зброї» американського військового аналітика Річарда Шафранскі. У цій книзі розглядається інформаційна війна у контексті збройних дій, спрямованих проти будь-якої частини системи знань чи припущень ворога. Тут «противник» може включати будь-кого, чиї дії суперечать цілям лідера. Поза державною структурою це може бути «образ ворога» чи «не ми». У межах держави «ворогом» може бути зрадник або мандрівник, будь-хто, хто протистоїть або недостатньо підтримує лідера, який керує засобами інформаційної війни. Якщо члени групи не підтримують цілі лідера під час бойових дій, внутрішня інформаційна війна (включаючи такі речі, як пропаганда, брехня, терористичні акти та чутки) може бути використана в спробі змусити їх бути більш лояльними до цілей лідерів [71].

Річард Шафранскі писав про те, що системи знань не так схильні до ірраціональності, вони більш загальні для всіх, у той же час системи уявлень індивідуальні. Оскільки йдеться про війну знань, то метою інформаційної війни називалася атака на епістемологію супротивника.

У своїй статті 1995 року «Інформаційна війна», Дж.Стейн розглядає інформаційну війну як засіб досягнення національних цілей через вплив на інформацію. Він підкреслює, що інформаційна війна має корені в ідеях та епістемології, оскільки вона займається тим, як люди мислять і приймають рішення. Це визначає сферу інтересів військових, зокрема сферу прийняття стратегічних рішень. Отже, визначення цілей інформаційної війни стає зрозумілим – це вплив на розум людей, зокрема на тих, хто має ключовий вплив у процесі ухвалення рішень [70].

Дж. Стейн, обговорюючи питання революції у військовій справі, каже, що багато нових технологій випадково набувають військового застосування, хоча й ілюструє це протилежним прикладом: «Інтернет став результатом потреби у безпечній комунікації. Далі він розширився до університетів, деяких університетів. А

потім він поширився до кожного. Ніхто не контролює інтернет сьогодні». До речі, на той час він очолював департамент досліджень майбутніх конфліктів у рамках Коледжу авіації ВМС США.

У Стейна 1995 р. визначення інформаційної війни звучало як досягнення національних цілей за допомогою інформації. І в нього знову звучить констатація того, що інформаційна війна має справу з ідеями та епістемологією.

Якщо розглянути ще одну розробку з давніших часів, то помітно важливу різницю між прямою та непрямою інформаційною війною. Пряма війна, згідно з сучасним визначенням Мартіна Лібікі у праці «Завоювання в кіберпросторі» (Conquest in Cyberspace), полягає у нападі інформації на інформацію. Іншими словами, це вплив на інформацію противника, який не впливає безпосередньо на його сприйняття та аналіз. У свою чергу, непряма інформаційна війна полягає у створенні феномену, який противник мусить самостійно помітити та проаналізувати, щоб досягти потрібних для комунікатора результатів [31].

З Лібіківської першої узагальнюючої роботи 1995 року випливає думка, що інформаційне середовище не обов'язково є сферою простої війни: «Інформація не є медіумом війни, за винятком вузьких аспектів, таких як електронне глушення». У ті роки він узагальнив усі види інформаційних конфліктів, включаючи електронну війну і психологічну війну. Він дотримувався погляду, що інформаційне середовище не є лише місцем проведення бойових дій, і в 2012 році він підкреслив: «Однією з відмінностей інформаційного середовища від інших сфер бойових дій (земля, вода, повітря, космос) є те, що це середовище штучно створене». Він стверджував, що розглядання інформаційного середовища як простору війни утруднює розробку адекватних заходів захисту та методів атаки мережевих систем.

Приміром, у чотирьох інших просторах сила може змусити «замовчати» іншу силу, але це складно зробити в кіберпросторі, оскільки там є принаймні одразу три різні простори: «мій», «чужий» та «загальний». Також непрацюючими виявляються методи, запозичені з наземної війни, наприклад захоплення ключової позиції або маневр. Цей та інші приклади Лібіки наводить для того, щоб показати, що ухвалення такого розуміння заважає здійснювати як оборону, так і атаку.

М. Лібіки, який з 1998 р. працює в корпорації РЕНД, у своїй книзі «Завоювання в кіберпросторі» виділяє два типи структур: «площі», які не бояться чужих інтервенцій, та «замки», що захищаються від чужих інтервенцій.

Мартін Лібіки у роботі «Що таке інформаційна війна?» («What is Information warfare») розглядає інформаційну війну як інформаційні впливи, що включають захист, маніпулювання, спотворення та спростування інформації. Мартін Лібікі описує сім форм інформаційної протидії: командно-управлінську (Commandand-Control Warfare), розвідувальну (Intelligence-Based Warfare), електронну (Electronic Warfare), психологічну (Psychological Warfare), хакерську (Hacker Warfare), економіко-інформаційну (Economic Informa), Кібервійну (Cyber Warfare) [28].

Д. Деннінг, працюючи в Джорджтаунському університеті та у військових, у своїй книзі «Інформаційна війна та безпека» 1999 р., будучи професором комп'ютерних наук, направила свої зусилля в технічну складову та трактує інформаційну війну як спрямовану на інформаційні ресурси. Д. Деннінг чітко ділить у своїй книзі «Інформаційна війна та безпека» наступальну інформаційну війну та оборонну (захисну) [69].

Ще одним джерелом нових концепцій став РЕНД, де на той момент працювали Джон Аркілла та його співавтор Девід Ронфельдт. Аркіла залучали до консультацій Пентагону під час усіх великих операцій. Він практично першим привернув увагу всіх як до кібервійни, так і до мережевої війни. Відповідно, він зміг реінтерпретувати входження цих нових феноменів під потреби військових.

І ще 1999 р. Аркілла з Ронфельдтом виступили з дослідженням з американської військової стратегії «The emergence of noopolitik. Toward an American information strategy». Дж. Аркілла, який багато в чому сформував американські уявлення про інформаційну війну, у своїї праці аналізує війну у Сирії, вивчає іррегулярні війни США є поширеною формою аналізу [72].

У своїй праці «Поява мережевої війни» Аркілл розглядає сучасний конфлікт як суперництво між двома полюсами: кібервійною та мережевою війною. Кібервійна характеризується конфліктами високої та середньої інтенсивності, тоді як мережева війна відноситься до конфліктів низької інтенсивності та операцій, які відрізняються

від традиційних форм війни. В останній не застосовуються ієрархічні форми організації, стратегії та комунікації. Мережева війна повністю перетворює характер загроз, ролі та місії [72].

Н. Марута і М. Маркова підкреслюють важливий етап історії, який слід враховувати у розгляді інформаційної війни – це міжвоєнний період 1918-1939 років. Під час цього періоду формувалися дві потужні тоталітарні держави – СРСР і нацистський Третій Рейх, які стали своєрідними «полігонами» для випробування та вдосконалення нових методів і технік інформаційно-психологічної війни [30].

О. Дубас у статті «Інформаційна війна: нові можливості політичного протистояння» вказує на активне зацікавлення наукової спільноти, переважно за кордоном, питаннями інформаційних протистоянь, що почалося в 80-90-х роках XX століття. Він зазначає: «Термін «інформаційна війна» має свою сучасну історію, з'явившись в середині 80-х років XX століття в контексті нових завдань Збройних сил США після завершення «холодної війни»« [14].

О.С. Зозуля [14], О. В. Курбан [26], П. М. Олещук [33] вказують, що війна вже відбувається, але це не оголошується офіційно і залишається прихованим від пересічних громадян, хоча вона направляє країни на глобальні зміни у міжнародній арені. Така «прихована» війна можлива завдяки розвитку інноваційних інформаційно-комунікаційних технологій.

Горбулін В. П., Додонов О. Г., Ланде Д. В. в контексті психологічних теорій досліджують інформаційну війну, вказуючи, що об'єктом є когнітивно-емоційна сфера індивідів, а головною метою є управління інтелектуально-психологічними та соціокультурними процесами. Основним елементом такого управління є неусвідомленість впливу на особи, схильні до прихованого впливу, і легко програмована їх поведінка [6].

Жарков Я. М. та Присяжнюк М. М. також розглядають психологічний вплив зазначеного феномена, поєднуючи в одному понятті інформаційне та психологічне протиборство. М. Присяжнюк розглядає інформаційну війну як систему підривних ідеологічних впливів імперіалізму, спрямованих на свідомість людей, переважно через сферу соціальної психології [11, с. 42].

Я. Жарков переконаний, що мова йде про інформаційно-психологічні акції, які здійснюються на міждержавному, стратегічному, оперативному й тактичному рівнях. Ці акції можуть мати місце як у мирний, так і у воєнний час, а також в інформаційній та духовній сферах. Вони можуть бути спрямовані як на власних військовослужбовців, так і на війська противника [11, с. 43].

В. Карпенко, досліджуючи український інформаційний простір, розкриває деталі інформаційної експансії Росії. Він зазначає, що Росія поширює неоімперіалістичні ідеї та форми російської експансії через українські засоби масової інформації [22, с. 182].

Означеною проблемою цікавляться П. Шпига та Р. Рудник у книзі «Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин», в якій науковці виділяють 4 підходи до визначення концепції інформаційних війн. Перший підхід трактує їх як комплекс політико-правових, соціально-економічних, психологічних дії, пов’язаних з захопленням інформаційного простору, витіснення ворога з інформаційної сфери, ліквідація його комунікацій, позбавлення засобів передачі повідомлень та також інші подібні цілі [63].

Другий пояснює інформаційну війну як найгострішу форму протистояння в інформаційному просторі, де воно має першочергове значення набувають значення безкомпромісність, висока конфліктність та коротка тривалість гострого суперництва.

Третій підхід трактує інформаційну війну як форму примусу та проведення військових дій з використанням найсучаснішої електронної техніки (цифрові випромінювачі, супутники та інші інноваційні технології), які використовуються для виконання військових завдань.

Четвертий підхід розглядає інформаційні війни у контексті кібернетичних битв (протистояння між технічними системами). Також важливим є конфліктологічний підхід, який дозволяє аналізувати ці війни з точки зору військового та політичного протистояння [63, с. 328].

Отже, наведені підходи надають можливість зрозуміти різні аспекти інформаційної війни. Психологічна парадигма дозволяє детально вивчити вплив на

внутрішньо-особистісні процеси людей, що призводить до змін у їх психічній сфері, коригує логіку світосприйняття та впливає на політичну поведінку. Геополітичний підхід дозволяє розглянути методи сучасної світової політики для досягнення політичного та економічного панування в мирний період. Конфліктологічний напрям орієнтується на адекватну оцінку стратегічного значення інформації в боротьбі за владу, ресурси та політичний статус. Системний підхід передбачає комплексне дослідження інформаційної війни з урахуванням взаємозв'язку окремих елементів, їх впливу на дестабілізуючі фактори та тактику в рамках стратегій.

1.3. Історія становлення загрози інформаційних війн для міжнародних відносин

Сучасні глобальні тенденції у сфері комунікації принесли нові результати, які практично були недоступні у минулому. Обсяг інформації, яку громадяни отримують поза контролем своїх національних урядів, різко збільшився. Американський дослідник Пол Кеннеді відзначає: «Урядам авторитарних держав стає дедалі важче тримати своїх народів у незнанні. Наприклад, Чорнобиль був швидко сфотографований французьким комерційним супутником, а знімки швидко передані на весь світ, включаючи сам Радянський Союз. Придушення китайським урядом виступу студентів на площі Тяньаньмень і шок, випробуваний усім світом цієї події, відразу ж потрясли і Китай завдяки радіо, телебаченню і телефаксу. Коли наприкінці 1989 року впали комуністичні режими у Східній Європі, повідомлення та відеосюжети про падіння одного з них стимулювали подібні процеси у сусідніх державах».

Термін «інформаційна війна» був вперше використаний американським експертом Томасом Роном у звіті, який він підготував у 1976 році для компанії Boeing, під назвою «Системи зброї та інформаційна війна». У своєму звіті Рон зауважив, що інформаційна інфраструктура стає ключовим компонентом американської економіки, але водночас стає і вразливою метою, як у військовий, так і в мирний час. Цей звіт можна вважати першою згадкою терміна «інформаційна війна» [16].

Історично інформаційне протистояння виникло як складова частина збройної боротьби. Причинами його виникнення стало прагнення нападаючої сторони підняти моральний дух своїх воїнів та послабити волю ворога. Таким чином, вона позбавляла останнього здатності до активного опору, сприяла його швидшому знищенню, зменшувала власні матеріальні та фізичні втрати, у тому числі втрати завойовуваних трудових і матеріальних ресурсів.

Найперша з відомих форм на противника не бойовими засобами – залякування його своєю (іноді уявною) бойовою міццю, – виникла досить рано. Її сліди ми бачимо у озброєних зіткненнях племен в епоху розкладання первіснообщинного ладу, війнах рабовласницьких держав. Під впливом страху, особливо у бою, коли немає часу для обмірковування своєї поведінки, противник приймає рішення про здачу або втечу практично рефлекторно.

Ще в давнину протиборчі сторони використовували засоби духовного впливу, щоб послабити моральний дух та бойову міць противника, а також підняти бойовий дух своїх військ. Це була історично перша форма інформаційного протиборства – інформаційно-психологічного забезпечення бойових та повстанських дій.

Як основний носій та засоби доведення інформації на першому, вербальному етапі виступала людина, як об’єкт впливу – психіка людини, її визначальна спрямованість. Аристотель ще IV ст. до н.е. виділив ті складові психіки людини, які на сьогодні є основними об’єктами інформаційного впливу – свідомість, волю та почуття людини. (Є три сили душі, головні для вчинку та для істини: почуття, розум, прагнення).

Способи ведення інформаційного протистояння у той історичний період були обмежені вербальними технологіями (виступи ораторів, релігійних проповідників, поширення чуток, дезінформації тощо), наочними засобами залякування (демонстрація військової переваги, страхітливі знаки,пропагандистські письмена на каменях, деревах і будовах тощо) та фізичної протидії (арешти, вбивства ораторів тощо). Найважливішими суб’єктами інформаційного протиборства того часу були священнослужителі якнайбільш освічені люди, які мали значний вплив на всі соціальні шари населення. При цьому поява перших друкованих засобів не відіграла

помітної ролі у здійсненні інформаційного протистояння, оскільки на той період основна маса солдатів та цивільного населення були неписьменні.

Витоками ідей інформаційно-психологічного впливу на протилежний бік вважається початкове осмислення правителями Стародавнього світу фізично ненасильницького управління масами людей. Про розуміння важливості психологічного протистояння у той період свідчать погляди єгипетських та ассирійських воєначальників, що прямо пов'язують розвиток ходу битви з психічним станом бійців. Не випадково основним завданням виховання вважалося вироблення психічної стійкості у бійця, готовності загинути, його обличчя, а не спина, має бути завжди бути повернено до ворога. З виховною метою воєначальники широко спиралися на релігію, обряди, традиції та ритуали. Цьому сприяв і народний епос. Разом з тим уже тоді воєначальники розуміли, що на хід битви впливає як настрій своїх воїнів, так й психічний стан ворожих бійців. Тому задум битви, як правило, будувався на основі маневру,що вносив сум'яття до лав противника. Найбільш поширеними способами внесення сум'яття було поширення чуток про переважну чисельність та потужність свого війська (особливо часто цей спосіб застосовував Олександр Македонський – IV ст. н.е.), використання жахливих стандартів, масок, звукового супроводу військових дій тощо. Важливим способом була також дезінформація супротивника з метою забезпечення раптовості нападу.

Класичним прикладом дезінформації є «троянський кінь», який зіграв вирішальну роль у троянській війні за розділ сфер впливу в Малій Азії між грецькими племенами у XIII ст. до н.е. Завдяки троянському коневі, якого, нібито подарувала місту богиня Афіна, спартанці захопили Трою і зруйнували її вщент.

Одним із найкращих фахівців античного світу з дезінформації військового супротивника вважався Ганнібал (III-II ст. до н.е.). Так, давньогрецький історик Полібій залишив свідчення того, як Ганнібал майстерно проводив операції з дезінформації супротивника. Він тривалий час розпускав чутки про те, що у його війську з'явилася якась хвороба, щоб римляни не дивувалися, почувши, що він давно стоїть своїм військом на одному місці, коли сам знаходився всього за три дні шляху від Тарента.

Цей маневр дозволив Ганнібалу швидко захопити місто. Іншим прикладом може служити підготовка Ганнібала до битви з римськими легіонерами при річці Треббін, в ході якої він активно розпускав чутки про незламну силу нової зброї карфагенян, чим сприяв формуванню психологічної готовності римлян до поразки.

Засобами інформаційного протистояння у давнину вирішувалися відповідні завдання не тільки у військовий, ай у мирний час. В історії відомі випадки успішного проведення, по суті, перших інформаційно-психологічних операцій у мирний час Наприклад, у Шумерських пам'ятниках (IV тисячоліття до н.е.) наводиться приклад ведення «війни нервів»: правитель шумерського міста Руку навмисно систематично страшними чутками залякував жителів та правителя міста Аратта, багатого благородним металом, внаслідок чого останні без жодного фізичного примусу платили Шумеру велику данину.

У міру накопичення досвіду практичного здійснення інформаційного протиборства виникла потреба у його теоретичному осмисленні. З документально зафіксованих розробок у галузі теорії інформаційного протиборства історично першими вважатимуться праці китайських дослідників.

У Китаї з давніх-давен з великою увагою ставилися до інформаційних форм і способів боротьби з противником, віддаючи перевагу їх кровопролитним сутичкам на полі бою. Перші наукові обґрунтування інформаційного протиборства пов'язують і з іменами давньокитайських філософів – Конфуція та Сунь-Цзи (VI-V ст. до н.е.), їх теорії використані в сучасних теоретичних та практичних підходах китайських та американських фахівців в інформаційному впливі, а також у діяльності спецслужб Китаю та США.

Сунь-Цзи надавав перевагу психологічному впливу на супротивника у військовому протиборстві. У своєму «Трактаті про військове мистецтво» він писав: «У будь-якій війні, як правило, найкраща політика зводиться до захоплення держави цілим; зруйнувати його значно легше. Взяти в полон армію супротивника краще, ніж її знищити... Здобути сотню перемог у битвах – це не межа мистецтва. Підкорити супротивника без бою – ось вінець мистецтва». Він вважав, що «війна – це шлях обману», і виграє той, хто вміє вести війну, не борючись.

У трактаті висвітлено основні прийоми маніпуляції супротивником шляхом психологічного впливу та дезінформації, у певному поєднанні механізму примусу обраного об’єкта до спрямованих дій.

Так в італійських та австрійських компаніях у 1804–1807 роках Наполеон Бонапарт вміло використовував газети та кореспондентів нейтральних держав (Швейцарія, Англія) для поширення дезінформації для розташування своїх військ.

У ХХ столітті інформаційні війни стали частиною військової політики держав [2, с. 59-78]. Наприклад, у Першу світову війну у Великій Британії було створено так зване Бюро військової пропаганди (1914 р.), яке пізніше перейменовано в Управління військової інформації.

У 1915 році в Франції було створено відділ Служби військової пропаганди в межах другого відділу генерального штабу Міністерства оборони. Ці установи займалися розповсюдженням пропаганди серед військових та цивільних осіб інших країн. У 1917 році США створили психологічну секцію під час розвідувальної служби штабу експедиційних військ. Основними засобами інформаційної війни на той час були листівки, газети; російська армія використовувала гучномовці як технічний засіб [2, с. 120].

Після Першої світової війни зросло зацікавлення цим явищем. У багатьох країнах почали з’являтися роботи з психологічних методів ведення війни. Англійський дослідник психологічної війни П. Г. Ворбертон писав: «У наш час основним завданням у війні є не знищення озброєних сил противника, як це було раніше, а підрив морального стану населення ворожої країни загалом до такого рівня, щоб воно змусило свій уряд піти на мир. Збройні зіткнення армій - це лише один із засобів досягнення цієї мети» [8, с. 132-133].

Таким чином, теорія інформаційної та психологічної війни почала розроблятися вже під час і після Першої світової війни. До Другої світової війни існувала активна пропаганда режимів: у Німеччині у період 1933–1941 років – нацистська пропаганда, в СРСР – комуністична та антикапіталістична, у США та Великобританії – капіталістична та антикомуністична. Під час Великої Вітчизняної війни акценти швидко зрушили в бік антинацистської пропаганди. [2, с. 201-214].

У цей період вже діяли органи державної пропаганди [5, с. 520]. У СРСР це були Бюро військово-політичної пропаганди та 7-е управління ГПУР РККА. У нацистській Німеччині функціонували Міністерство народної освіти та пропаганди та Верховне головнокомандування Вермахту. Свої органи пропаганди мали також США та Велика Британія.

Під час війни методи психологічного впливу, що використовувалися, часто були дуже ефективними. Незважаючи на розвиток інформаційних технологій того часу, більшість пропаганди продовжувала поширюватися у формі листівок та плакатів. Активно використовувалося радіомовлення на мові супротивника [4, с. 69-84].

Після Другої світової війни теорія психологічної війни стала більш складною. У контексті протистояння між СРСР та США під час Холодної війни, а також у локальних конфліктах того періоду, інформаційні війни отримали нові риси. Наприклад, у 1950 році в США було створено Управління психологічної війни, яке здійснювало пропагандистську діяльність, у тому числі за допомогою «агітаційних снарядів», під час Корейської війни [6, с. 149-151]. У свою чергу, пропагандистські органи Корейської народної армії та Народно-визвольної армії Китаю, з підтримкою апарату пропаганди Збройних сил СРСР, здійснювали масштабний психологічний вплив на військових Південної Кореї та США, що виявився дещо успішнішим [6, с. 98-109].

Після Корейської війни результати були критично переосмислені у США, і вже у 1955 році було прийнято нове положення «Ведення психологічної війни», в якому було зазначено: «Психологічна війна включає заходи, що передають ідеї та інформацію для впливу на свідомість, почуття та дії противника. Вони проводяться командуванням у поєднанні з бойовими операціями з метою підриву морального духу супротивника відповідно до політики, проголошеної керівними інстанціями». Управління психологічної війни було перейменовано на Управління спеціальних методів війни, призначення якого обґрунтував генерал У. Троскел: «Спеціальні методи війни – це поєднання прийомів, форм та методів психологічної війни з іншими засобами, спрямованими на підрив супротивника зсередини. Вони розширюють поле

бою і перетворюються з тимчасово чинного тактичного засобу обмеженого впливу на потужну стратегічну зброю, що має великі потенційні можливості» [6, с. 151-152].

Під час війни у В'єтнамі, американські пропагандисти впроваджували нові методи для психологічного впливу на ворога та місцеве населення. Окрім насильства, що супроводжувалося американськими операціями в сільських та міських населених пунктах, вони активно застосовували стратегії, спрямовані на індукцію страху серед місцевого населення та військових, використовуючи знання про культуру та вірування в'єтнамців. Ця інформаційно-психологічна обробка призводила до деморалізації армії противника та сприяла її подальшому фізичному ослабленню.

Важливим аспектом були також експерименти з використанням телебачення як засобу пропаганди. Крім того, проводилися спроби створення комп'ютерних баз даних для збору та аналізу інформації, а також розробки інформаційних систем, наприклад, системи PAMIS.

Проте поразка США у В'єтнамській війні змусила американський військовий апарат переглянути свої підходи до інформаційно-психологічної війни. Цей досвід викликав необхідність в подальшому перегляді тактики та стратегії цієї форми боротьби [8, с. 137-138].

У війні в Афганістані, яка тривала з 1979 по 1989 рік, США використовували свої технології, але вони не брали активної участі в військових діях. Замість цього американські агенти спонсорували моджахедів, надаючи їм зброю та тренування, а також розповсюджували пропагандистські матеріали, які мали на меті дискредитувати радянських військових, накладаючи на них вигадані звинувачення, включаючи вчинення злочинів проти афганських дітей.

У той час радянська пропаганда в Афганістані була організована і зосереджена на поширенні політичних анекдотів про опозиційних лідерів та критиці уряду. Така пропаганда несла в собі більш «гуманні» елементи порівняно з американською, але все ж намагалася дискредитувати опозицію та підтримувати ідею військового втручання [6, с. 301-304].

У XX столітті інформаційна війна часто впліталася в реальні військові конфлікти, стаючи необхідною складовою їх стратегій. У XXI столітті виникає

поняття «інформаційного протистояння», яке стає невід'ємною частиною політичних протиріч як у мирний час, так і в умовах війни.

С. Лем у романі «Фіаско», опублікованому вперше у 1986 році, відобразив розвиток інформаційних воєн наступним чином:

- Розвиток засобів зброї на планеті призвів до ситуації, коли використання бойових арсеналів неодмінно призводить до загибелі біосфери. Обидві ворогуючі сторони мають потужну зброю, і продовження змагання за подальшим нарощуванням безглуздо.

- Виникає проблема контролю за застосуванням сили, тобто проблема контролю над діями противника в таких сферах, як зв'язок і управління.

- Позбавлення противника можливості застосовувати силу означає позбавлення його здатності ефективно керувати ситуацією та своєчасно передавати керівні сигнали.

С. Лем пише: «Ніхто не блокує сам собі канали розпізнавання та командування. Це відбувається через так званий ефект дзеркала. Кожен завдає шкоди іншому, розриваючи його зв'язок, і отримує аналогічну відповідь. Замість змагання за точність і потужність балістичних снарядів, на передній план виходить боротьба за збереження зв'язку. Якщо перше було лише накопиченням засобів руйнування та загрозою їх застосування, то друге — це справжня «війна зв'язку». Битви за руйнування та збереження зв'язку цілком реальні, хоча не призводять до руйнувань чи кривавих жертв. Поступово заповнюючи радіоканали шумом, супротивники втрачають контроль над власними озброєннями, а також контроль над озброєннями та оперативною готовністю ворога».

Сучасна інформаційна війна може тривати безперервно, анонімно та непомітно, в будь-якій точці інформаційного простору, включаючи інші території. Об'єктом атаки виступає культурний простір противника, його свідомість, причому ці атаки можуть протікати довгий час, не викликаючи свідомого реагування з його боку. Все це забезпечує значну ефективність методів впливу при мінімізації втрат для «агресора», тим самим дозволяючи йому зберігати свій образ як мирної та цивілізованої держави.

Характеристика нової «зброї» в контексті сучасних технологій та створення єдиного інформаційного простору дозволяє здійснювати інформаційні операції у глобальному масштабі. Тотальний інформаційний контроль забезпечується спеціальною міжнародною організацією BSA (Business Software Association).

Прийоми інформаційних воєн до XXI століття стали набагато витонченішими і, відповідно, небезпечнішими. Сьогодні ті, хто планує та здійснює інформаційні атаки, мають сучасні знання у галузі психології. Це дозволяє їм впливати на підсвідомість та керувати нашими вчинками. Замість прямолінійної пропаганди використовується масовий гіпноз, якому піддаються цілі країни та народи. Методи, що призводять до подібних результатів, виникали й вдосконалювалися протягом історії людства, стаючи все більш ефективними. Так, від шаманських танців ми перейшли до психотехнологій, які здійснюють прихований вплив на поведінку людини. Піддавшись подібному впливу, ви навіть не усвідомлюєте, що він має мету та відбувається.

Основна відмінність сучасних психо-технологій полягає в їхній здатності впливати на психіку, обминаючи свідомість. Це призводить до втрати можливості приймати обґрунтовані та виважені рішення, а отже, до втрати свободи волі. В результаті наше життя, включаючи поведінку, бажання, емоції та навіть здоров’я, опиняється під чужим контролем.

У випадках, коли інформаційна зброя використовується проти психіки людини (або соціальної групи), мова йде про інформаційно-психологічну боротьбу. На початку XXI століття широкого поширення набули психо-технології, ґрунтовані на сучасних досягненнях психолінгвістики, еріксоніанського гіпнозу та нейролінгвістичного програмування (НЛП). Усі вони відрізняються високою ефективністю впливу на підсвідомість людини.

Отже, у доісторичні та давні часи виник один із способів деморалізації супротивника – бойовий клич, який виступив способом демонстрації своєї рішучості здобути перемогу, способом демонстрації своєї чисельної переваги (або імітації цього перевага за рахунок гучності). З часом інформаційне протиборство ставало більш різноманітним та витонченим, що враховує особливості об’єкта впливу – людської

психіки. Крім того, змінювалися і способи інформаційного впливу від примітивно-вербального спочатку, до складно організованого, комплексного впливу із застосуванням усіх основних комунікативних каналів.

РОЗДІЛ 2 СУЧАСНИЙ СТАН ІНФОРМАЦІЙНИХ ВІЙН В МІЖНАРОДНИХ ВІДНОСИНАХ

2.1. Напрями та методи ведення сучасних інформаційних війн у глобалізованому світі

Як відомо, основний інструмент ведення інформаційної війни є інформаційна зброя, що складається з сукупності засобів, методів та технологій інформаційно-психологічного впливу,створених з метою таємного управління сферою інформації супротивника,системами та процесами, що працюють на основі інформації, а також – для завдання їм шкоди.

Інформаційно-психологічна війна передбачає використання механізмів, які безпосередньо впливають на процес мислення людини. Філософи-»ідеалісти», такі як О.Ф. Лосєв, Г. Фреге, Г. Лебон та Е. Кассірер працювали над функціональним підходом до свідомості людини. Суть цього підходу полягала у відповідності, співвідношенні, певних розмежуваннях, постійних елементах та зв’язках, а не в самому матеріальному предметі.

Ці дослідження призвели до появи такого поняття, як символічний простір. Під символічним простором теоретики мають на увазі абстрактне мислення, яке здійснюється за допомогою символів, завдяки чому людина здатна опосередковано аналізувати зовнішній світ. Це говорить нам про те, що людина живе як у фізичному, так і у символічному універсумі. Сьогодні швидкими темпами зростає символічна активність людини, але водночас відбувається віддалення фізичної реальності, що полегшує процес управління та маніпулювання людьми. Символічне мислення призвело не лише до небаченого прориву людства до нових технологій та знань, а й відкрила нові можливості для керування свідомістю людини. Крім окремих напрямків використання символів існує загальний підхід, що полягає в розробці комп’ютерної карти взаємозв’язків у просторі символів.

Сучасне інформаційне суспільство має могутній засіб реалізації методів та прийомів психологічної війни – засоби масової інформації. На думку М. Паренті, ЗМІ «відбирають більшу частину інформації та дезінформації, якими ми

користуємося з метою оцінки соціально-політичної дійсності. Наше ставлення до проблем та явища, навіть сам підхід до того, що вважати проблемою або явищем, багато в чому визначені тими, хто контролює світ комунікацій».

Сучасна інформаційна війна – це міждержавний конфлікт, що виникає на етапі усвідомлення та загострення політичних протиріч між майбутніми антагоністами (в ролі яких можуть виступати держави та політичні еліти), що формує майбутню структуру конфліктних відносин і, що створює умови для застосування одним із антагоністів прямої збройної сили. Інформаційна війна – це стадія, що охоплює попередню та підготовчу фазу розвитку збройного конфлікту; після переходу конфліктних відносин у фазу прямого (лобового) зіткнення інформаційна війна втрачає своє самостійне значення і стає сервісною функцією війни традиційної.

Структурно-інформаційна війна може поділятися на наступні складові частини [8]:

- психологічні операції (операції прямої дії);
- дезінформація;
- радіоелектронна війна;
- захист власної інформації;
- фізичне руйнування елементів інформаційних систем противника;
- інформаційна атака (або інформаційний «вкидання»).

Далі розглянемо такі засоби ведення інформаційної війни, як: міф, дезінформація, пропаганда, психологічна операція, чутки, переконання, психологічний тиск та диверсифікація суспільної свідомості.

Міф – це інформація (вид інформації), яка роз’яснює походження та подальше перебудова тих чи інших явищ на ґрунтах вигаданих заходів. Осмислення людиною навколишньої реальності за допомогою легенд ґрунтується не на наукових пізнаннях, а на вірі та поглядах адептів певної культури, етносу, суспільної групи. Легенди сприяють передачі соціальної навички з покоління до покоління.

За допомогою послідовного дослідження легенд (переказів) людина долучається до витоків ситуації певного суспільства. Таким чином інтуїтивно протікала і її самоідентифікація по відношенню до сім’ї, держави, цивілізації.

Принцип побудови сюжету традиційного міфу – поєднання знайомих реалій життя із фантастичними вчинками героїв емоційно посилював сприйняття інформації. З удосконаленням суспільних відносин правителі стали більше застосовувати методики міфотворчості у своїх цілях. Для зміцнення особистої сили вони використовували способи поширення такої інформації про свою діяльність, в якій їм приписувалися надприродні ймовірності, завдяки яким вони долали неприємності та забезпечували благоденство своїх країн та народів.

У процесі «міфологізації» зникають реальні людські риси і на сцені соціального життя бувають помічені герої, які перемагають не політичних ворогів або конкурентів у конкурентній боротьбі, а «жахи». Для створення та зміцнення міфологічних образів застосовуються розробки в галузі психолінгвістики, сугестивної лінгвістики, нейролінгвістичного програмування, еріксоніанського гіпнозу, психології сприйняття. Всі вони виділяються найвищою ефективністю впливу.

Пропаганда (від латинського propaganda - «що підлягає поширенню») – це процес популяризації та розповсюдження ідей у глобальній свідомості через усні виступи або за допомогою ЗМІ.

Політична пропаганда означає постійні зусилля впливати на розуміння індивідів, груп та суспільства для досягнення певного, заздалегідь запланованого політичного результату.

Термін «пропаганда» часто має негативне відтінення. Більшість дослідників визнають, що пропаганда є засобом маніпуляції, інформаційно-психологічного тиску на особистість та контролю її поведінки. Зокрема, англійський теоретик Л. Фрезер описав пропаганду як мистецтво примусу людей робити те, чого вони не зробили б, якби мали всю доступну інформацію.

Суть пропаганди в тому, що під її впливом кожен індивід поводиться так, як у випадку якщо б його поведінка випливало з його особистих висновків. Буквально, наприклад, можна маніпулювати поведінкою групи людей, при цьому будь-який член подібної групи стане вважати, що діє за власним розумінням.

Пропаганда часто умовно поділяється на «білу», «сіру» та «чорну». «Біла» пропаганда зазвичай походить від офіційного джерела або одного з його

представників. Вона відкрита, використовує перевірені факти та не приховує своїх цілей. «Сіра» пропаганда не вказує конкретного джерела інформації, користується неперевіреними даними та намагається ввести людей у хибні уявлення. «Чорна» пропаганда завжди приховує своє справжнє джерело, використовується для розповсюдження обману та маніпуляцій.

Основні принципи ведення пропаганди:

- пропаганда повинна бути прихованою і не називатися прямо, щоб уникнути невдачі.
- вона базується на розвідувальній інформації, знаннях про політичні, духовні, військові, економічні, соціальні особливості країн та народів, до яких вона звертається.
- пропаганда не ставить за мету обговорення тем, а висуває питання та проблеми, що існують насправді.
- вона має бути гнучкою і динамічною, постійно адаптуватися до подій і готово змінювати свою інтерпретацію явища для ефективного використання в зміненій обстановці.
- необхідно надавати вільність управління пропагандою на місцях; хоча центр може висувати директиви і інструкції, конкретні дії повинні здійснюватися на місцях відповідно до обставин.
- необхідно використовувати всі існуючі можливості для поширення пропаганди, і особливо використовувати громадян тих країн, які є її об’єктом, перетворюючи їх на мимовільних розповсюджувачів.

Чутки – своєрідна картина інформації, що з’являється раптово, потужність інформаційного вакууму між конкретними верствами населення або навмисне кимось поширюваний вплив на соціальне розуміння.

Впровадження чуток у зацікавленнях в інформаційній війні – це поширення інформації, вигідної джерелу. Чутки мають усі шанси ставати раптово, внаслідок неправильного сприйняття інформації, поширюватись зацікавленою стороною.

Щоб інформація стала об’єктом слуху, важливо:

- Інформація повинна мати значення для особи, що піддається впливу, тобто прямо стосуватися її інтересів.
- Інформація має бути зрозумілою всім учасникам процесу передачі слуху.
- Володіння інформацією сприяє підвищенню престижу транслятора слуху.

Переконання – це метод впливу на свідомість людей, спрямований на їх особисте критичне сприйняття.

Переконання полягає в комунікаційному впливі на свідомість особистості шляхом звернення до її особистого критичного міркування.

Під переконанням розуміється досягнення одноголосності індивіда або групи з певною точкою зору за допомогою логічного обґрунтування, що призводить до зміни їхньої свідомості порівняно з минулим. Особи, які переконані, стають готовими захищати цю точку зору і діяти відповідно до неї.

Основу методу переконання становить відбір, логічне упорядкування фактів та висновків. Переконання часто ускладнене низкою причин, які вкрай потрібні враховувати задля забезпечення ефективності впливу. Цими причинами може бути прийнятність, у яких здійснюється протидія.

Метод переконання передбачає логічно аргументований вплив на раціональну сферу свідомості людей. Переконання спрямоване на інтелектуально-пізнавальну сферу психіки людей та їх груп. Його суть полягає в тому, щоб спочатку за допомогою логічних аргументів досягти в людини внутрішньої згоди з певними умовиводами, а потім на цій основі сформувати та закріпити нові установки (або трансформувати старі), що відповідають поставленій цілі.

Правила переконання:

- Логіка переконання повинна бути зрозумілою та доступною для інтелекту об’єкта дії.
- Переконувати слід доказово, опираючись на факти, відомі об’єкту.

- Крім конкретних фактів та прикладів, інформація повинна містити узагальнені положення та ідеї, особливо для тих, кому бракує широти кругозору або розвиненого абстрактного мислення.
- Переконлива інформація має виглядати максимально правдоподібною.
- Сполучені факти та загальні положення повинні викликати емоційну реакцію об'єкта дії. Критерієм успішності переконання є впевненість.

Дезінформація – поширення свідомо неправдивої інформації з метою вплинути на думку керівництва та населення країни. Один з прикладів – військова інтервенція США та їх союзників до Іраку 2003 р. Бойові дії велися під приводом боротьби з міжнародним тероризмом та знищення зброї масової поразки. Активно використовувалися засоби масової інформації, які, з одного боку, формували необхідне ставлення світової громадськості, з іншого – призводили до погіршення морально-психологічних настроїв населення Іраку, знижуючи цим його боєздатність.

Види дезінформації включають:

- Введення в оману конкретної особи або групи осіб, включаючи цілі нації.
- Маніпулювання діями однієї людини або групи осіб.
- Створення громадської думки щодо певної проблеми або об'єкта.

Психологічний тиск – це вплив на психіку людей шляхом створення залякування та погроз з метою змусити їх прийняти певну заплановану модель поведінки. Методи психологічного тиску включають:

- Надання інформації про реальні або уявні загрози та небезпеки для об'єкта.
- Передбачення репресій, переслідувань, вбивств тощо.
- Шантаж.
- Здійснення вибухів, підпалів, масових отруєнь, захоплення заручників та інших терористичних або диверсійних акцій.

Ще одним методом впливу на маси є диверсифікація суспільної свідомості - це розпорошення уваги правлячої еліти держави на розв'язання штучно створених проблем з метою відволікання уваги від вирішення справжніх соціально-політичних та економічних завдань.

Методи диверсифікації суспільної свідомості включають:

- Дестабілізація ситуації в державі або окремих її регіонах.
- Посилення кампанії проти політичного курсу правлячої еліти держави та її окремих лідерів у різних міжнародних інституціях.
- Ініціювання антидемпінгових кампаній та інших скандальних процесів, застосування міжнародних санкцій.

Засоби, форми та методи інформаційної війни вдосконалювалися та розвивалися часом швидше, ніж наука та технології. Світ змінюється, і сучасна інформаційна війна також, а саме завдяки Інтернет ресурсам, мережевим платформам, таким як Facebook, YouTube, WhatsApp, Messenger, WeChat, Instagram, QQ, Tumblr, Qzone, TikTok та Твіттер, а також телебаченню.

Серед сучасних методів інформаційної війни з використанням інформаційних технологій можна виділити такі:

- **Ефект первинності.** Людська психіка так улаштована, що люди сприймають за істину первинну (почуту вперше) інформацію, а на вторинну, вже мало хто звертає увагу, навіть якщо вона 100% правдива і йде в розріз із уже озвученою. Тому завжди ефективніша та пропагандистська машина, яка працює швидше.
- **Повторення.** Зазвичай використовують спрощений текст, розрахований на низько інтелектуальну аудиторію (яка завжди у будь-якій країні світу у більшості) і повторюють його стільки разів, що інформація закріплюється у підсвідомості людей і стає для них істиною.
- **Інформаційна блокада (неповна інформація).** Державні ЗМІ висвітлюють події з тієї точки зору, яка зручна владі, надаючи часткову інформацію, але не показуючи всієї картини того, що відбувається. Наприклад, нам демонструють численні проурядові мітинги, куди люди йдуть тисячами без примусу, а потім показують мітинги опозиції, куди, нібито, прийшло всього 100 людей.
- **Напівправда.** До 90% вигадки додають один-два правдиві факти, що йдуть на початку новини або повідомлення.

- **Ілюзія підтримки більшості та образ ворога.** Маніпулятори завжди намагаються піднести свої ідеї так, ніби їх підтримує більшість населення. Правителі часто пояснюють низький рівень життя населення витівками зовнішніх сил, перекладаючи всю відповідальність за свої непрофесійні дії на якогось супротивника.
- **Жертва.** Для консолідації суспільства знаходять небезпечну режиму особистість чи групу осіб і починають її загальне цькування. Таке «жертвопринесення» пов'язує і поєднує низько інтелектуальні верстви населення краще, ніж будь-що інше.
- **Ярлики.** На непідходящого владі громадського діяча починають навішувати різні ярлики: злодій, екстреміст, шпигун тощо. Суспільство, не розібравшись до чого, вірить почутому.
- **Інформаційна хвиля.** Відразу безліч різних ЗМІ починають проштовхувати ту саму ідею, висловлювання і т. д. Потім після первинної інформаційної хвилі, настає вторинна, яка є спілкуванням вже між окремими людьми. Хвилі йдуть один за одним і змушують суспільство сфокусуватися на обговоренні цієї ідеї.
- **Констатація фактів.** Метод полягає в тому, що пропагандисти підносять якусь подію як таке, що вже відбулося. Наприклад, ЗМІ повідомляє, що у першому турі за якогось політика проголосувала більшість. При цьому конкретні цифри тих, хто проголосував, наведено не були, а у людей уже створюється ілюзія того, що даний політик практично переможець. Це, своєю чергою, змушує їх віддати свої голоси.
- **Звичайна розповідь.** ЗМІ спокійно розповідають про страшні вбивства та звірства, наче це буденність, а не справжні жахіття. Згодом глядачі звикають до цього і ставляться до подібних подій як до чогось буденного.
- **Психологічний шок та емоційний резонанс.** Спочатку ЗМІ вводять глядача в психологічний ступор, показуючи йому картини вбитих людей, масових руйнувань, а потім «вливають» у шокований розум людини потрібну інформацію, яку критично в цей момент сприймати, не здатні.

- **Відволікання уваги.** Замість сфокусуватися на власних проблемах, що, звичайно ж, призведе до розкриття їхніх справжніх винуватців, державні ЗМІ переводять «стрілки» на події, що відбуваються найчастіше в інших країнах.
- **Рейтинги.** Часто маніпулюють думками людей брехливими рейтингами. Отримавши таку інформацію люди погоджуються з думкою цієї «віртуальної» більшості та, наприклад, віддають голос за кандидата, чий рейтинг вищий.
- **Сенсація.** Грубий метод, який використовується для того, щоб відвернути увагу від по-справжньому значущих подій. Є різновидом прийому «відволікання уваги».
- **Очевидці.** Метод полягає у використанні істерик, гри на публіку, плачу і недосвідчений глядач починає вірити у сказане, не знаючи часу перевірити інформацію про те, хто перед ним: справжня жертва або хороший актор.
- **Авторитети або ефект ореолу.** Це так зване використання анонімного авторитету. За словами вчених, на нас очікує глобальне потепління. Однак у даному прикладі не наводиться інформація, що за вчені це сказали і на підставі яких досліджень було зроблено такий висновок. З метою пропаганди ще більш переконливим є використання популярної людини, медійної особи [2].

До основних засобів інформаційної війни відносять:

- приховування інформації;
- спотворення інформації;
- кількісне прирощення повідомлень певного типу;
- відволікання уваги від важливого несуттєвим.

Кожен із цих засобів має велику кількість варіантів застосування і використовується по-різному в межах текстових чи відео- і аудіо повідомлень.

Таким чином, в сучасному політичному процесі активно використовуються спеціальні засоби для досягнення важливих політичних цілей. Одними з найефективніших з них є маніпулятивні технології. Перераховані вище методи, які є потужним інструментом політичного маніпулювання, відіграють ключову роль у

формуванні суспільної думки, сприяючи зміні поглядів, установок, політичного мислення та поведінки громадян. Інформаційні війни можуть мати як негативне, так і позитивне значення для суспільства, наприклад, сприяючи залученню мас до політичної участі та активізації громадянства.

2.2. Позитивні та негативні наслідки ведення інформаційних війн

Результатом «боїв» інформаційної війни має, на думку фахівців, стати зміна розстановки сил у суспільстві, зниження готовності населення країни-противника активно чинити опір ворогові. Набагато дешевше не вбивати солдатів ворога, ризикуючи своїм життям та військовослужбовців, а переконати ворогів здатися без опору. У сучасних умовах це «війна за знання – за те, кому відомі відповіді на запитання: що, коли, де і чому і наскільки надійними вважає окремо взяте суспільство чи армія свої знання про себе та своїх супротивників» [7] з метою використовувати це знання для досягнення своєї перемоги . Отже, в ході інформаційної війни треба мати здатність збирати, обробляти та розподіляти безперервний потік інформації про ситуацію, перешкоджаючи противнику робити те саме [8].

Тим самим війна виводиться зі сфери прямих силових зіткнень і переводиться головним чином у сферу протиборства інформаційних систем, здатних як отримувати «чужу» інформацію, і захищати «свою».

За думкою фахівців, поразка у інформаційній війні має низку ознак, які схожі на ті, що характеризують поразку у звичайній війні:

- Масова загибель або еміграція частини населення.
- Руйнування промислової бази та сплата контрибуцій.
- Втрата певної частини території.
- Встановлення політичної залежності від переможця.
- Повний розпад або повторне скорочення армії, або навіть заборона існування власних військових сил.
- Вивезення з країни найбільш перспективних і наукомістких технологій.

Проте, не завжди інформаційні війни несуть негативні наслідки. Позитивна інформаційна війна спрямована на те, щоб передати споживачеві певні переконання у зрозумілій формі та сприяти соціальній гармонії та злагоді. Вона сприяє вихованню людей відповідно до загальноприйнятих цінностей. Цей тип інформаційної війни здійснюється на користь тих, кому вона адресована, і не обмежується вузьким колом зацікавлених осіб. Крім того, вона не переслідує маніпулятивних цілей і не допускає використання брехні чи приховування фактів.

Інформаційна війна відрізняється від інших форм конфліктів декількома важливими аспектами:

- Глобальний охоплення: Інформаційні атаки можуть проникати навіть у найзабороненіші схованки психіки, вражаючи розум противника, оскільки не мають кордонів або моральних обмежень.

- Безслідність: Інформаційна війна не залишає по собі слідів, тому важко виявити її вплив та заздалегідь до неї підготуватися.

- Економічна ефективність: Для ведення інформаційної війни не потрібно великих матеріальних та людських ресурсів. Грамотна подача мінімального обсягу інформації може досягти чудових результатів.

- Гнучкість методів: Інформаційна війна може використовувати як «жорсткі» тактики, так і «м’які» підходи, в залежності від об’єкту впливу.

- Мімікрія: Подання інформації різним способом для різних аудиторій дозволяє «маскувати» цілеспрямований вплив, ускладнюючи виявлення його.

- Різноманітність сприйняття: Ті самі факти та явища можуть сприйматися різними групами по-різному, що дозволяє маніпулювати думками та переконаннями.

- Зміна світогляду: Метою інформаційної війни є зміна світогляду великих соціальних груп або цілого суспільства, що вимагає вміння «вникнути у голову» супротивника та змінити його сприйняття світу.

Позитивним прикладом застосування інформаційної зброї може бути операція «Буря в пустелі», проведена США на Близькому Сході. Ця операція вважається успішним прикладом психологічного впливу, оскільки американські військові, використовуючи «м’яку цензуру», фактично виключили з інформаційного простору

повідомлення, які виправдовували протилежну сторону конфлікту. Крім того, ця операція стала першою в історії війни, яку транслювали в прямому ефірі. У даному випадку психологічний вплив здійснювався шляхом ретельного висвітлення необхідної інформації в ЗМІ, що сприяло формуванню певного образу подій у свідомості суспільства [15].

У XXI столітті інформаційна війна є однією з найважливіших проблем міжнародних відносин. Масштаби її впливу постійно зростають. Однією з головних загроз є відсутність у міжнародному праві будь-яких заборон та обмежень щодо ведення інформаційної війни. Крім того, необхідно звернути увагу на те, що в локальних конфліктах це поєднується зі збройною агресією, що підкреслює необхідність врегулювання цього явища на міжнародному законодавчому рівні [17].

Проте, інформаційні війни несуть більше негативні наслідки. Яскравим прикладом можемо навести інформаційні війни Росії проти України у 2014-2021 рр., мета якої полягає у «забруднені» інформаційного поля, а не у переконанні ворога, схилити на свою сторону. Метою російської інформаційної війни є забезпечення інформаційного поля, перенаситити його різноманітною, заплутаною інформацією і, таким чином, дати зрозуміти, що насправді відбувається, для пересічного громадянина стало надзвичайно складним завданням. Російські агенти роблять все, щоб українці, що проживають на Сході Україна не змогли знайти адекватні аргументи на захист української влади, знайти раціональні перспективи тощо [1].

Ключова мета російської інформаційної війни – створити повну недовіру серед Українці на Сході до української влади, армії і, звісно, до будь-яких представників європейського світу. Коли інформаційне поле знищено, працює лише людський страх, розчарування, паніка, відчуття соціального колапсу. Російська пропаганда підриває довіру жителів Східної України українській владі і прагне донести до них свою думку про рятувальну місію Росії для українців, які проживають на сході України [1].

У сучасній Росії основна мета інформаційної війни з формування єдиної національної ідеї, що згуртовує багатонаціональне, поліконфесійне суспільство на основі спільних цінностей, залишається актуальною та першочерговою. Вона

становить метаструктуру пропагандистських повідомлень у мас-медіа. Її змістовне наповнення у вигляді ідей про героїчне історичне минуле (освоєння космосу, перемога у Великій вітчизняній війні) також визначають та заповнюють мезоструктури інформаційного простору. Влада розглядає свою пропагандистську діяльність як виховну, спрямовану популяризацію «цінностей російського суспільства». Відповідно до низки офіційних державних програм, до них відносяться насамперед «здоров'я, праця, сім'я, любов до Батьківщини, активна життєва та громадянська позиція та відповідальність» [4].

Варто відзначити, що елементи російської інформаційної війни активно використовуються для розпалювання паніки та поширення насильства у Східній Європі. Одним із найпотужніших інструментів впливу не лише на українців та жителів європейського континенту, а й на людей по всьому світу, є телеканал «Russia Today». «Russia Today» – це мультимедійне міжнародне інформаційне агентство, метою якого є оперативне, збалансоване та, головне, «по російському» висвітлення подій у світі, тобто розповідь міжнародній аудиторії про російський погляд на ситуацію. Росія є провідним гравцем на політичній мапі світу, і тому її «голос» має бути чутним, як стверджує позиція «Russia Today», яку очолює журналіст-міжнародник Дмитро Кисельов [5].

Ось 7 ключових повідомлень, які вони намагаються донести:

- Євромайдан був зорганізований нацистськими радикалами із Західної України. Це було насильство, а не мирний протест. Всі, хто брав участь або підтримував його, є нацистами.
- Януковича незаконно зняла влада озброєних радикалів. Революція «Євромайдан» – це державний переворот. Більшість українців не підтримувала його. Україна не має легітимного уряду, парламенту або президента.
- Націоналістичні лідери контролюють Україну, дискримінують російськомовних громадян та вбивають їх на Донбасі. Росія має право захищати своїх громадян від фашистів.

- Не було жодної анексії Криму. Жителі Криму вирішили приєднатися до Росії на референдумі. Крим завжди був частиною Росії.
- Українська армія воює проти власного народу на Донбасі. Жителі Донбасу захищаються від неї, хочуть незалежності або більших прав.
- Немає російських солдатів на Донбасі. Росія надсилає гуманітарну допомогу, а не зброю. Малайзійський Боїнг-777 був збитий українською армією.
- Україна – держава, яка не виправдала своїх сподівань. [6].

Основною метою інформаційних кампаній Росії є дискредитація інтеграції України в ЄС та НАТО, підживлення недовіри до влади та спотворення нормальних переговорів щодо врегулювання ситуації на Сході України. Москва все ще намагається створити негативне ставлення до українців в ЄС і погрожує їм уявними погрозами.

Українські проросійські ЗМІ ретранслюють своїй цільовій аудиторії наративи про розкол і неспроможність ЄС. При цьому наголошують на позитивному досвіді співпраці Німеччини та Франції та Росії.

Інформація про співпрацю Москви з Берліном та Парижем подається в Україні таким чином, щоб продемонструвати явну неспроможність української влади. Таким чином Росія намагається показати, що рішення щодо України будуть прийматися без її участі.

Для досягнення цих цілей пропагандисти зосередилися на популяризації в Україні таких наративів:

- Незважаючи на значне погіршення відносин Росії з Європейським Союзом, Брюссель веде переговори з Москвою, в тому числі щодо України та Білорусі;
- Переговори з українського питання ведуться без участі офіційного Києва;
- Деякі країни ЄС, зокрема Німеччина та Франція, готові до діалогу з Росією і виступають за співпрацю з Кремлем;
- Україна є ненадійним партнером для Європейського Союзу через постійне порушення зобов’язань;

- Підписання та реалізація Угоди про асоціацію з ЄС призводить лише до підвищення тарифів на комунальні послуги та зубожіння населення;
- До українців в ЄС ставляться як до людей другого сорту [3].

Численні публікації в проросійських ЗМІ представляють Україну як ненадійного міжнародного партнера, який не дотримується досягнутих домовленостей. Основні приклади – загострення лінії розмежування в Донецькій та Луганській областях та спроби звинуватити Україну у недотриманні Мінських домовленостей. *«Провокації з боку Збройних сил України відбуваються, вони не поодинокі, а численні»*, – заявив 2 квітня 2021 р. речник Путіна Дмитро Пєсков [4].

Останніми днями до цього списку поповнилася трагедія п'ятирічного хлопчика, який загинув унаслідок вибуху на непідконтрольній території Донецької області. З 2 квітня по спіралі триває інформаційна операція щодо притягнення до цієї справи безпілотника Збройних сил України. І хоча кремлівський фейк швидко спростували, пропагандисти продовжують поширювати дезінформацію. Тепер його передали на державні російські телеканали.

Росія використовує ще одну групу антиєвропейських наративів, щоб залякати Україну війною на її території. Пропагандисти припускають, що в разі конфлікту між НАТО і Росією Україна буде змушена вступити у війну, а на її території, ймовірно, відбуватимуться військові дії.

Росія прагне переконати Україну, що НАТО розглядається як полігон для військових дій проти Росії. Особливого поширення ця теза набула після ухвалення в березні нової стратегії військової безпеки України. У відповідь Росія почала погрожувати, що НАТО використає українську територію для боротьби з Росією. Прокремлівські ЗМІ запевняють, що в бойових діях братиме участь все населення України. У той же час вони пропагують очевидну перевагу російської армії. Це можна розглядати як демонстрацію готовності Росії вступити у військовий конфлікт з країнами НАТО. Таким чином Росія залякує населення європейських країн, намагаючись посилити протиріччя в Євросоюзі.

У той же час Росія нав'язує Європі необхідність розглядати Білорусь як супротивника і очікувати військового вторгнення зі своєї території. Таким чином,

спільні військові навчання «Захід 2021» можуть бути використані Росією, щоб продемонструвати Європі свій контроль над Білоруссю [4].

У Росії, стверджує політолог А. Ковальов, *«...обороти державної пропагандистської машини десь з кінця 2013 року, після заміни керівництва найбільшої інформаційної агенції країни РІА «Новини», і за кілька місяців до Криму та подій на сході України, досягли такої інтенсивності, що «російська пропаганда» сьогодні займає цілу категорію. В Інтернеті з'явилася маса аматорських сайтів на кшталт «Stopfake.org», які ретельно спростовують пропагандистські фальшивки, що розповсюджуються російським телебаченням та соцмережами»* [6].

Загалом російські ЗМІ намагаються зобразити зневагу ЄС до українців, а економічні негаразди представити як результат розвитку співпраці Києва з Брюсселем. У цьому ж контексті запровадження паспортів ЄС COVID називають утиском прав громадян України на відвідування ЄС.

Так, інформаційна війна є деструктивним явищем, що негативно впливає на розвиток інформаційних суспільств. Проте, вона також сприяє розвитку пріоритетних сфер життєдіяльності, в тому числі за рахунок впливу маніпулятивних технологій на світову політику. Сучасні тенденції у державно-правових явищах вимагають нових стратегій забезпечення національної інформаційної безпеки.

Одним із важливих завдань є удосконалення правових основ протидії та попередження інформаційних війн і негативного інформаційно-психологічного впливу на національному рівні в Україні. Для цього необхідно вивчати зарубіжний досвід та аналізувати доктринальні та нормативні джерела, щоб знайти оптимальні шляхи реагування на складні ситуації, що виникають у вітчизняному суспільстві в останні роки.

2.3. Міжнародне право та інформаційні війни. Пропозиції щодо регулювання інформаційної війни

У науковій спільноті відсутнє однозначне розуміння предмета міжнародного інформаційного права, і термін сам по собі не є стилізованим. Однак це не зменшує

значення його теоретичного розгляду, а також практичного значення дискусії щодо цього питання у контексті навчання його як навчальної дисципліни.

Кодифікація міжнародного інформаційного права вважається менш ймовірною у найближчому майбутньому через динамічний характер цієї сфери міжнародного права.

Питання про можливість визнання міжнародно-правових норм у цій галузі як окремої галузі має скоріше теоретичне, ніж практичне значення. Донедавна інформаційне право не вважалося самостійною галуззю права в межах внутрішньодержавного правового порядку.

Історія питання сягає своїм корінням в дискусію про систематизацію права та, так званої, «комплексної галузі» права, яка досить активно велася ще в радянській правовій науці. Вперше запропонований в роботах В. К. Райхер [25, с. 120] поділ галузей права на основні та комплексні був загалом позитивно сприйняття радянською правовою наукою, незважаючи на критику прихильників протилежного підходу.

Подальший розвиток ця теорія отримала на роботах А. А. Красавчикова [17, с. 64] та В. Ф. Антипенко [2, с. 9]. На думку Пазюк А. В., «інформаційне право як комплексна галузь, що об’єднує в предметній галузі регулювання однорідну групу суспільних відносин, тісно взаємодіє з профільними галузями права, і насамперед, конституційним, цивільним та адміністративним правом» [22, с. 31].

Аналогічної думки дотримується О. І. Марущак: «комплексний характер цієї галузі обумовлюється, насамперед, законодавчою практикою, згідно з якою інформаційні норми залучаються до традиційних галузей права, насамперед, конституційного, адміністративного та цивільного» [18, с. 88].

Українські автори підручника з інформаційного права, такі як В. С. Цимбалюк, В. Д. Павловський і В. В. Грищенко, висловлюють іншу точку зору. Вони розглядають концептуальні підходи до формування змісту інформаційного права, вказуючи, що це не окрема галузь, а складний міжгалузевий інститут.

Ці автори вважають, що в кожній провідній галузі права існує умовно визначений галузевий інститут, який на міжгалузевому рівні формує нове явище -

міжгалузевий комплексний інститут права. Інформаційне право, на їхню думку, тісно переплітається з іншими міжгалузевими комплексними інститутами, такими як право власності, право інтелектуальної власності, патентне право на інтелектуальну промислову власність та авторське право [21, с. 56]. У зазначеному дослідженні не вказується, яка ж галузь права, на думку його авторів, є для інформаційного права провідною.

Відсутність єдиних підходів визначається також неоднорідністю структури міжнародного інформаційного права, фрагментарністю правового регулювання та відсутністю одноманітної термінології. Серед безлічі назв, поряд із «міжнародним інформаційним правом» [48, с. 12] можна також зустріти вже згадане «міжнародне право масової інформації» [48, с. 12], «міжнародне право Інтернету» (International Internet Law) [48, с. 12], «міжнародне телекомунікаційне право» (International Telecommunications Law) [48, с. 13]; «Міжнародне медійне право» (International Media Law) [48, с. 13]; а також «міжнародні режими інформаційно-комунікаційних технологій» (International Regimes for Information and Communication Technologies) [48, с. 13] та «міжнародні режими та інформаційна інфраструктура» (International Regimes and Information Infrastructure) [48, с. 13] і т.д.

Суб'єктами міжнародного інформаційного права можуть бути як держави, суб'єкти федерації, органи державної влади та місцевого самоврядування, так і фізичні та юридичні особи [27, с. 355].

Актуальність міжнародного співробітництва у сфері поширення масової інформації диктується необхідністю заборони одних та заохочення інших ЗМІ, координації використання радіочастот для запобігання взаємним радіоперешкодам, ідеологічними інтересами держав, комерційними інтересами виробників продукції масової інформації. У 1978 р. створено Комітет ООН з інформації [27, с. 355].

Джерелами міжнародного інформаційного права є численні міжнародні конвенції та не менш численні резолюції-рекомендації міжнародних організацій [27, с. 357].

- Женевська конвенція про використання радіомовлення на користь миру 1936 р. закріплює обов'язок держав припиняти мовлення зі своїх

територій, яке б спонукати іноземне населення до дій проти внутрішнього порядку своїх держав.

- Міжнародна конвенція про ліквідацію всіх форм расової дискримінації 1965 р. передбачає обов'язок держав заборонити на своїй території будь-яку пропаганду, засновану на теоріях расової переваги.
- Міжнародний пакт про громадянські та політичні права 1966 р. зобов'язує держави прийняти національні закони, що забороняють будь-яку пропаганду війни.
- Декларація ООН про поширення серед молоді ідеалів світу, взаємоповаги та взаєморозуміння 1965 р. містить положення, спеціально присвячені впливу ЗМІ на виховання молоді.
- Декларація ЮНЕСКО про основні принципи, що стосуються у ЗМІ для зміцнення миру та взаєморозуміння, у розвиток прав людини та у боротьбу проти расизму, апартеїду та підбурювання до війни 1978 р. присвячена використанню ЗМІ з метою підтримання миру та нормальних міжнародних відносин.
- Декларація ООН про неприпустимість інтервенції та втручання у внутрішні справи держав 1982 р. закріплює зобов'язання держав утримуватися від наклепницьких кампаній, ворожої чи образливої пропаганди з метою втручання у внутрішні справи інших держав [27, с. 358-359].

У міжнародному праві діє ціла низка угод, що регламентують технічні та комерційні аспекти транскордонного використання ЗМІ:

- Міжнародна конвенція електрозв'язку (діє у Женевській редакції 1991 р.);
- Статут Міжнародного союзу електрозв'язку (МСЕ) 1994 р.;
- Угода про полегшення міжнародного обміну візуальними та звуковими матеріалами освітнього, наукового та культурного характеру 1949 р.;
- Конвенція про міжнародний обмін виданнями 1958 р.;
- Конвенція про обмін офіційними виданнями та урядовими документами між державами 1958 р.;

- Брюссельська конвенція про поширення несучих програм і сигналів, переданих через супутники, 1974 р. (забороняє несанкціоноване розповсюдження телепрограм через супутники, які можуть прийматися у державах, населенню яких ці передачі не поширюються) [32, с. 478].

Конвенція про доступ до інформації, участь громадськості у процесі прийняття рішень та доступ до правосуддя з питань, що стосуються навколишнього середовища, 1998 р. (Орхуська конвенція про інформацію) стала першою міжнародною угодою, що забезпечує права громадськості на доступ до екологічної інформації та участь у прийнятті рішень. Одночасно вона зобов'язує держави передбачити правові та організаційні гарантії для реалізації таких прав [35, с. 46].

У 2003 р. до Конвенції 1998 р. було прийнято Додатковий протокол про регістри викидів та перенесення забруднювачів (РВПЗ). Мета Протоколу – розширення доступу громадськості до інформації шляхом створення загальнонаціональних РВПЗ, що сприятиме скороченню забруднення навколишнього середовища [35, с. 47].

Документи, прийняті в рамках НБСЄ/ОБСЄ, забезпечують свободу доступу до інформації на основі укладених міжнародних угод. У Європі діє регіональна міжнародна організація – Європейський Союз електрозв'язку. У 1989 р. між Радою Європи та Європейською Радою було укладено Європейську конвенцію про транскордонне телебачення [35, с. 48].

Інформаційні права та свободи людини становлять фундаментальні засади міжнародного інформаційного правопорядку. Міжнародне право захисту прав людини несе у собі антропоцентристську фундаментальну основу, концентрує регуляторний вплив на людину, її права та свободи. При цьому інформаційні права та свободи проголошуються в документах з прав людини загалом, декларативному вигляді [35, с. 49].

Міжнародне інформаційне право спрямоване на реалізацію людиною інформаційних прав, та виступає інструментом реалізації інформаційних відносин на міжнародному рівні.

Серед відносно «нових» прав людини серед розвинених країн світу отримало своє визнання право на доступ до Інтернету. Наприклад, парламент Естонії у законодавстві, прийнятому у 2000 році, проголосив доступ до Інтернету як право людини. Конституційна рада Франції визнала доступ до Інтернету як фундаментальне право людини в 2009 року, а Конституційний суд Коста-Ріки дійшов такого ж висновку 2010 [35, с. 50].

У науковій спільноті не врегульовано дискусію щодо статусу інформаційної війни та інформаційної зброї. Проте існує концепція «Конвенція про забезпечення міжнародної інформаційної безпеки» [3], яка не є чинною, держави-учасниці ООН досі не можуть дійти ухвали про її прийняття. У концепції визначено, що інформаційна війна – протистояння двох чи більше держав в інформаційному просторі з метою заподіяння шкоди інформаційним системам, критично необхідним та іншим структурам, підриву політичної, фінансової та суспільної систем, масованої психічної обробки населення для дестабілізації суспільства та країни [3].

Спектр дій, віднесених до інформаційної війни, визначений широко, виходячи з цього визначення, до дій, що «дестабілізують суспільство», можна віднести події й у рамках соц. мереж, та ЗМІ.

На нашу думку, помилково настільки широко трактувати цей інститут та виділяти його як самостійну категорію в міжнародному праві, але категорію інформаційної зброї має бути визначено. По-перше, інформаційна війна не відноситься до категорії війни, не є її різновидом, тому що поняття агресії визначено в резолюції Генеральної Асамблеї так [2]: «Агресією є застосування збройної сили державою проти суверенітету, територіальної недоторканності чи політичної незалежності іншої держави, або іншим чином, несумісним зі Статутом ООН, як це встановлено в цьому визначенні» [2].

По-друге, інформаційна війна не може існувати самостійно від військових дій, тому що є одним із засобів досягнення стратегічно важливої мети в ході проведення певних операцій, пов’язаних із втручанням в інформаційну систему держави. Тому необхідно ввести до норм міжнародного гуманітарного права категорію зброї – інформаційну.

Додатковий протокол до Женевських конвенцій [1] щодо захисту жертв міжнародних збройних конфліктів ст. 36 «Нові види зброї» встановлює, що при розробці або прийнятті нових видів зброї необхідно визначити, чи підпадає їх застосування під заборони, що містяться в цьому Протоколі або в нормах міжнародного права [1].

На відміну від інформаційної війни, зброя – це способи та засоби, які націлені на втручання в інформаційну систему, порушення інформаційної безпеки держави, тому, правової регламентації та забезпечення вимагає саме зброя. До категорії інформаційної зброї необхідно відносити ті засоби, які можуть завдати прямої шкоди, але не непрямої. Відповідно до загальноприйнятих підходів під зброєю прийнято розуміти пристрої, спрямовані на об'єкт противника, з метою повної або часткової втрати здатності до виконання бойового завдання [6].

У статті Воробйової І. В. [5] пропонується відносити до інформаційної зброї тільки ту, яка призначена для поразки інформаційних систем військової дії (засоби радіоперешкод, зброя електромагнітного імпульсу та спрямованої енергії) та спеціальних програмних систем (комп'ютерні віруси, комп'ютерні черв'яки, троянські програми, утиліти прихованого адміністрування) [5].

Під ситуацією поширення хибної інформації запроваджується поняття «дезінформація». Як приклад, можна навести дезінформацію, пов'язану з пандемією COVID-19 у 2019–2020 роках. Основна хибна ідея, яка отримала широке охоплення у ЗМІ по всьому світу полягала в тому, що вірус є біологічною зброєю, тобто створеною штучно, яка має на меті регуляцію населення планети, наводилася також хибна статистика.

Така інформація підпадає під категорію дезінформації, оскільки внаслідок її поширення постраждали багато людей (підвищився відсоток нервових захворювань), паніка, а також розпочався «травлення» багатьох держав. Таким чином, інформаційна зброя несе низку загроз щодо держави та мирного населення: поширення шкідливих інформаційних систем, спрямованих на заволодіння стратегічно важливими даними та порушення суверенітету держави, порушення прав людини, дестабілізація

суспільства та розпалювання міжнаціональної ворожнечі, а також у терористичних цілях.

Зростаюча актуальність і обговореність питань правового регулювання аспектів інформаційних війн у державах стає неодмінною. Це пояснюється швидким розвитком інформаційних технологій та поширенням мережі Інтернет. Потреба в правовому регулюванні цієї сфери наростає через те, що Інтернет використовується не лише для комунікації та обміну інформацією, але й може бути інструментом зловмисників для завдання шкоди приватним особам, корпораціям та державам. У зв'язку з цим загострюється питання впровадження кібербезпекових заходів для захисту інформаційних мереж держави та її громадян [34, с. 36].

На думку А. Капто, під «інформаційною безпекою» розуміє властивість інформаційного простору, кіберсистем тощо протистояти умисним і неумисним загрозам, а також реагувати на них і відновлюватися в разі реалізації цих загроз, яка включає також розвиток 60 наступальних можливостей» [14].

Інформаційну безпеку можна визначити як стан захищеності інформаційного простору держави в цілому або окремих об'єктів її інфраструктури від ризику зовнішнього впливу на інформацію. Забезпечення цієї безпеки передбачає стійкий розвиток системи захисту, а також своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз, кібернетичних втручань та інших форм ворожих дій, які можуть завдати шкоду особистим, корпоративним або національним інтересам.

Створена ще у 1967 році Асоціація аудиту і контролю інформаційних систем (ISACA) у своєму виданні глосарію 2014 року визначає інформаційну безпеку як «захист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, що взаємодіють у мережах». Аналітичне видання «Трансформація інформаційної безпеки» розширює це визначення, наголошуючи, що інформаційна безпека охоплює всі заходи, спрямовані на захист організацій та фізичних осіб від умисних атак, порушень, інцидентів та їхніх наслідків. Особлива увага приділяється високотехнологічним та складним загрозам, таким як атаки з використанням

комплексних технік, кібервійни, а також спрямованим та постійним загрозам (APT), що можуть мати серйозний вплив на організації та індивідуальних користувачів [4].

Основні проблеми, що виникають у забезпеченні інформаційної безпеки, обумовлені наступними факторами:

- Недостатнє усвідомлення ролі та значення інформаційно-безпечної складової в системі національної безпеки держави.
- Відсутність чітких визначень, термінологічної узгодженості та нормативно-правового регулювання у галузі інформаційної безпеки.
- Залежність держави від програмного і технічного обладнання іноземного виробництва.
- Відсутність ефективної координації дій між відповідними відомствами, що призводить до неузгодженості заходів зі створення окремих елементів системи інформаційної безпеки.
- Недостатність методичного забезпечення та недостатня кваліфікація кадрів у відповідних структурних підрозділах [4].

Обґрунтування ототожнення культури інформаційної безпеки як складової інформаційної культури у вузькому розумінні видається виправданим, оскільки аспект безпеки є невід'ємною частиною інформаційних відносин, які передбачають використання сучасних IT-технологій та мережі Інтернет [23, с. 144].

Поняття культури інформаційної безпеки, спрямованого на захист інформації, поширилося у світі після прийняття у 2003 році Резолюції Генеральної Асамблеї ООН «Створення глобальної культури інформаційної безпеки». Згідно з звітом Європейського агентства з питань мережевої та інформаційної безпеки (ENISA) 2017 року, «Культура інформаційної безпеки організації», запропоновано таке визначення культури інформаційної безпеки: знання, переконання, уявлення, норми і цінності людей щодо інформаційної безпеки та використання інформаційних технологій. Формування культури інформаційної безпеки в організації спрямоване на зміну мислення співробітників, сприйняття ризику та спільної відповідальності за забезпечення інформаційної безпеки організації, а також на усвідомлення заходів забезпечення особистої інформаційної безпеки як побутової звички [23, с. 145].

Важливим фактором, який підкреслює потребу виокремлення інформаційної безпеки, є розробка деякими країнами доктрин ведення спеціальних операцій у інформаційному просторі. Ці стратегії використовуються для проведення операцій проти окремих країн або об'єктів за допомогою спеціалізованих органів і структур.

З визначених напрямів випливає один важливий висновок: інформаційна безпека є справою всіх суб'єктів – від самої людини до приватного сектору, від суспільства до держави. Тільки у такому симбіозі можливе побудова суспільства, де індивіди відчувають себе безпечно в кіберпросторі. Для досягнення цього необхідно:

- Тісна співпраця між державою, приватним сектором та громадянами: Ця співпраця передбачає взаємний обмін інформацією та взаємодію між відповідальними за інформаційну безпеку органами та приватним сектором.

- Розвиток і впровадження понять «екологія інформації», «інформаційна гігієна», «критичне мислення»: Це включає розвиток інформаційної культури та свідоме усвідомлення необхідності навчання дітей та молоді інформаційній культурі та гігієні [48].

Міжнародний Союз Зв'язку (МСЕ) активно звертається до теми безпеки інформаційного простору, особливо після проведення «женевського» й «туніського» форумів Всесвітнього Саміту з Інформаційного Суспільства (WSIS) та Повноважної конференції МСЕ у 2006 році. Керівники МСЕ вважають, що ключова роль організації полягає в зміцненні довіри та безпеки при використанні інформаційно-комунікаційних технологій.

У 2008 році в Йоханнесбурзі асамблея МСЕ-Т прийняла Резолюцію – 50 «Інформаційна безпека» [49], яка привернула увагу до необхідності більш інтенсивної співпраці членів МСЕ задля вироблення узгоджених стандартів у боротьбі з кіберзлочинами, а також збільшення масштабів інформування про такі злочини та відповідні механізми протидії.

Поміж важливих кроків МСЕ, спрямованих на подальше убезпечення інформаційного простору, варто виокремити створення фахівцями цієї структури такого важливого документа, як «Розуміння кіберзлочинності: Керівництво для країн, що розвиваються» (Understanding Cybercraime: A Guaide for Developing Counries) [49].

У Керівництві викладено ключові погляди МСЕ на ситуацію у сфері інформаційної безпеки, запропоновано ключові визначення та універсальна модель взаємодії основних суб'єктів забезпечення інформаційної безпеки на національному рівні. Досі цей документ залишається достатньо актуальним і виваженим. Факт надзвичайної важливості проблематики інформаційної безпеки для МСЕ засвідчило те, що саме це питання було центральним на порядку денному П'ятого Всесвітнього форуму з політики у сфері електрозв'язку, який відбувся в червні 2013 року в Женеві [49].

Крім ООН та пов'язаних з нею спеціалізованих організацій, проблемами інформаційної безпеки, як зазначалося, опікуються інші міжнародні структури, зокрема G7, яка вперше звернулася до проблем протидії «високотехнологічним злочинам» ще у 1997 році. Тоді, під час зустрічі міністрів внутрішніх справ та юстиції було ухвалено спільне комюніке, додатком до якого стали «Принципи та План дій щодо боротьби з високотехнологічними злочинами» (Principles and Action Plan to Combat High-tech Crime) [13].

У тому ж 1997 році G8 створила Підкомітет з високотехнологічних злочинів (Група Рим–Ліон), який працює й досі.

У європейській практиці адміністративно-правового регулювання у сфері забезпечення інформаційної безпеки великий акцент робиться на тому, що безконтрольне використання можливостей інформаційного простору надає можливість різним деструктивним силам поширювати кіберзагрози та небезпеки. Одним з основних обмежень, щодо ефективності національного законодавства у цій сфері, є неспроможність ефективно протистояти загрозам у кіберпросторі.

Для вирішення цієї проблеми було розроблено Європейську конвенцію про кіберзлочинність, яку прийняв Комітет міністрів Ради Європи 23 листопада 2001 року. Конвенцію підписали 46 країн, у тому числі 38 країн – членів Ради ЄС, а також Канада, Японія, Південна Африканська Республіка і США. На даний момент її ратифікували 24 країни, зокрема Україна.

До числа країн, які не підписали конвенцію, входять Китай, кілька латиноамериканських держав і Росія. Нормами зазначеної конвенції охоплено широке коло питань, включаючи різні аспекти кіберзагроз та кіберзлочинності, такі

як незаконний доступ до комп'ютерних систем та перехоплення даних, вплив на дані та роботу системи, протизаконне використання пристроїв, підроблення та шахрайство з використанням комп'ютерних технологій, а також правопорушення, пов'язані з дитячою порнографією і тероризмом [50].

При підготовці Конвенції про кіберзлочинність переслідувалася мета формування загальної правоохоронної системи для забезпечення інформаційної безпеки та створення умов для обміну інформацією між усіма країнами, що підписали конвенцію. Нормами Конвенції про кіберзлочинність також обумовлено загальні для всіх Інтернет-провайдерів правила зберігання особистої інформації клієнтів на випадок, якщо подібні відомості будуть затребувані при розслідуванні кіберзлочинів [50].

Ще одним міжнародним документом є Директива ЄС, що стала першим у своєму роді юридично обов'язковим документом горизонтальної прямої дії у сфері інформаційної безпеки. Метою Директиви є захист критичної інфраструктури (постачальників життєво важливих та цифрових послуг) від кібератак, які можуть мати «істотний руйнівний ефект» [16].

Європейський Парламент та Рада ЄС прийняв Директиву 6 липня 2016 р. з терміном імплементації країнами-членами до 9 травня 2018 р. Мета Директиви була сформульована таким чином: «...забезпечити високий середній рівень мережної та інформаційної безпеки» [16].

Далі ми переходимо до Закону про інформаційну безпеку ЄС, прийнятого Постановою 2019/881 Європейського парламенту та Ради ЄС від 17 квітня 2019 р. про Європейське агентство з інформаційної безпеки (ENISA) та про сертифікацію технологій у галузі інформаційної та комунікаційної безпеки [16].

Ухвалення закону про інформаційну безпеку було обумовлено низкою факторів, зокрема, прагненням ЄС зайняти лідируючу позицію на міжнародному ринку технологій безпеки поряд з усвідомленням того, що існуюча система не може забезпечити своєчасну протидію певним загрозам, про що свідчать нещодавні кібератаки [16]. По суті, цей закон уперше представив систему сертифікування технологій цифрової безпеки на всьому просторі ЄС. Подібна система покликана

знизити ризик фрагментації єдиного ринку та підвищити конкурентоспроможність ЄС на глобальному рівні [16]. Наявність сертифіката свідчить про те, що продукт чи послуга відповідають заданим критеріям та забезпечують певний рівень захищеності від кіберзагроз.
[16].

У листопаді 2016 року Європейський парламент прийняв Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» (EU strategic communication to counteract propaganda against it by third parties). Цей документ ґрунтується на нормативних актах Європейського Союзу, прийнятих раніше, зокрема на Плані дій щодо стратегічних комунікацій (Action Plan on Strategic Communication) [12].

У зазначеній Резолюції основний акцент робиться на аспектах інформаційного впливу Росії, зокрема через мультимедійні сервіси та інформаційний простір. Цікавим є також те, що вона висвітлює необхідність заходів наступального характеру, а не лише оборонного. В офіційних документах Європейського Союзу Російська Федерація все частіше зазначається як суб'єкт, що продукує гібридні загрози, у тому числі й у кіберпросторі. Крім того, зроблено акцент на впливі дезінформації у сфері забезпечення інформаційної безпеки Європейського Союзу [6, с. 67].

У березні 2015 року Європейська Рада наказала Верховному Представнику ЄС у співпраці з інституціями ЄС та країнами-членами ЄС розробити план дій зі стратегічних комунікацій. Це призвело до створення оперативної робочої групи для протидії кампаніям дезінформації, що проводить Росія [6, с. 67].

У контексті досвіду адміністративно-правового регулювання забезпечення та організації інформаційної безпеки в країнах Азії слід відзначити, що одним із найпотужніших механізмів правового та організаційного забезпечення інформаційної безпеки є система контролю Інтернету в Китаї. На сьогодні китайська система адміністративно-правового регулювання забезпечення інформаційної безпеки є складною, комплексною і дуже ефективною.

У 2004 році було утворено Європейське агентство з мережевої та інформаційної безпеки (ENISA) з метою підвищення ефективності внутрішнього ринку. Агентство

діє як консультативний та центр передових технологій у сфері мережевої та інформаційної безпеки для країн-членів та інститутів Європейського Союзу. Крім того, ENISA сприяє розвитку зв'язків між країнами-членами ЄС, їхніми інститутами, господарюючими суб'єктами та приватним сектором [13].

Талліннський центр кіберзахисту НАТО (CCD COE) є міжнародною військовою організацією, що була створена у 2008 році з фінансовою та організаційною підтримкою держав-учасниць. Операційно незалежний, він спеціалізується на дослідженнях, розробках, навчанні та освіті в галузі кіберзахисту, охоплюючи як технічні, так і нетехнічні аспекти.

Ідея створення Центру виникла під час інциденту з пам'ятником «Бронзовий солдат» у Таллінні, коли Естонія стала жертвою кібератак. У травні 2008 року Естонія, разом з Німеччиною, Італією, Латвією, Литвою, Словенією та Іспанією, підписала Меморандум про порозуміння щодо створення Центру. Це рішення було реакцією на кіберзагрози та потребу підвищення кіберзахисту.

28 жовтня 2008 року Північноатлантична Рада надала Центру акредитацію при НАТО і статус міжнародної військової організації. Першим кроком у лінії співпраці були естонсько-шведські кібернавчання, проведені 9 грудня 2008 року, що відзначили як перший крок у підготовці нових спеціалістів з кіберзахисту.

У січні 2013 р. у Гаазі було відкрито Європейський центр боротьби з кіберзлочинністю (ЕС3) [23, с. 354], завданням якого є присікання дій організованих злочинних мереж. На даний момент об'єктами уваги ЕС3 є кібератаки на ключові інфраструктури і інформаційні системи, онлайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії [23, с. 354]. Найбільше уваги приділяється протидії в трьох напрямках – онлайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи [23, с. 354].

У 2013 році було опубліковано «Таллінське керівництво з міжнародного права, що застосовується в випадку кібервійни» (Tallinn Manualon The International Law Applicableto Cyber Warfare). Талліннське керівництво є підсумком трирічної роботи

міжнародної групи експертів, запрошених Центром передового досвіду НАТО із спільного захисту від кіберзагроз (The NATO Cooperative Cyber Defence Center of Excellence), м. Таллінн (Естонія). У цьому документі було зазначено, що жодна держава не може здійснювати суверенітет над кіберпростором, держави володіють суверенітетом над кіберінфраструктурою, розташованою на їхніх територіях і діяльністю, пов'язаною з такою інфраструктурою [3, с. 11].

У вересні 2015 року була запущена оперативна робоча група зі стратегічних комунікацій Європейського Союзу, відома як East StratCom Task Force. Метою цієї групи є роз'яснення ключових аспектів політики Європейського Союзу, підсилення його позитивного іміджу та протидія дезінформації [23, с. 357].

Відзначаючи високий рівень активності та співпраці міжнародного співтовариства у вирішенні стратегічно важливих проблем розвитку інформаційного простору та загроз його використання у якості гібридного інструменту воєнної агресії, а також досвід провідних країн у сфері адміністративно-правового та організаційного забезпечення інформаційної безпеки, обґрунтованим є висновок щодо реально сформованого міжнародного консенсусу розвинених країн світу на основі визнання його об'єктивної необхідності в умовах стрімкого зростання кіберзагроз як на національному, так і міжнародному рівнях.

РОЗДІЛ 3 РОЛЬ СОЦІАЛЬНИХ МЕРЕЖ У ПОШИРЕННІ ДЕЗІНФОРМАЦІЇ

3.1. Механізми поширення дезінформації в соціальних мережах

Зі зростанням популярності Інтернету неухильно зростає його роль у повсякденному житті людини. Масштабне впровадження швидких і безкоштовних онлайн-сервісів формує основи комунікації значної частини суспільства, надаючи доступ до інформації, актуалізуючи економічні інтереси і політичну позицію громадян.

Інтернет-технології радикально змінили індустрію спілкування та медіа, спосіб споживання і створення новин. Онлайн-платформи, зокрема соціальні мережі, поступово стають домінантним джерелом новин та інформації для сотень людей. Простота створення й розповсюдження новин через Інтернет, а також фізична неможливість перевірити величезні обсяги інформації, що циркулює у всесвітній мережі, різко збільшила поширення дезінформації та фейкових новин.

Під терміном «дезінформація» розуміється процес маніпулювання інформацією: введення будь-кого в оману шляхом надання неповної інформації або повної, але вже не потрібної інформації, спотворення контексту, спотворення частини інформації.

Концепція дезінформації, згідно з ЮНЕСКО, розглядається у взаємозв’язку з іншими двома категоріями:

- Недостовірна інформація (Misinformation): Це тип інформації, яка є невірною або неточною, але не має наміру вводити в оману. Наприклад, це може бути помилкове розуміння події або невірна інтерпретація фактів.

- Шкідлива інформація (Malinformation): Це інформація, яка має намір вводити в оману, шкодити чи ображати людей, а також спричиняти збиток. Наприклад, це може включати матеріали наклепу, образливі висловлювання чи розповсюдження особистої інформації без згоди.

У контексті концепції ЮНЕСКО дезінформація розглядається як частина ширшого спектру проблем з інформаційною безпекою, який включає в себе різні типи неправдивої або шкідливої інформації, що можуть впливати на суспільство. (рис. 3.1)

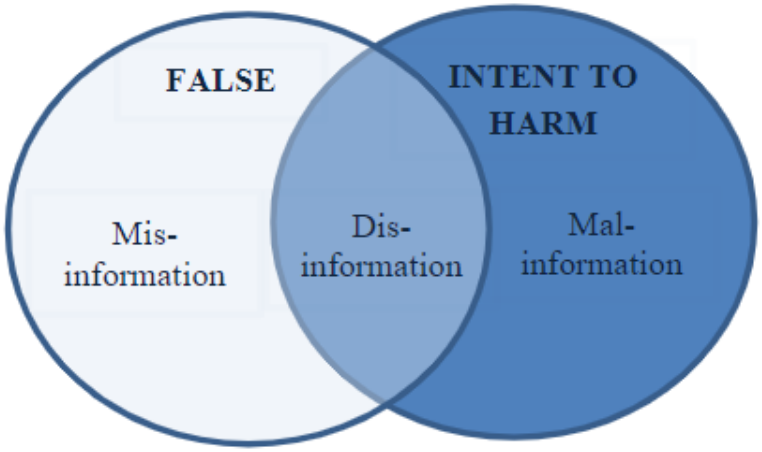

Рис.3.1.Співвідношення понять дезінформація, недостовірна та шкідлива інформація

Дезінформація може включати в себе різні типи неправдивої або шкідливої інформації, кожен з яких має свої характеристики:

- Усвідомлена дезінформація. Особа, яка поширює цю інформацію, знає, що вона неправдива і свідомо вводить людей в оману. Це є свідомою, навмисною брехнею з метою досягнення певних цілей.

- Хибна інформація. Це інформація, яка є неправдивою, але особа, яка її поширює, вірить у її правдивість. Вона може бути недбалою або неправильною інтерпретацією фактів.

- Шкідлива інформація. Ця інформація базується на реальності, але використовується для заподіяння шкоди особі, організації чи країні. Вона може включати матеріали наклепу або образливі висловлювання.

Одним з важливих аспектів дезінформації є те, що вона має ряд характеристик, вітчизняний дослідник Г. Почепцов виділив такі:

- Високий емоційний рівень, що дозволяє ефективно охоплювати велику кількість людей.

- Просування вигаданого віртуального об’єкту, який активно руйнує звичну картину світу.

- Слабка схильність до спростування, оскільки важко довести неправдивість вигаданих об’єктів.

- Направлення на вразливі точки масової свідомості.

Існують різноманітні форми дезінформації, які включають текстовий контент, відеоконтент і аудіальний контент. У свою чергу, методи поширення дезінформації включають координовану неавтентичну поведінку, таргетинг, діпфейки, а також фейкові новини. (рис.3.2)

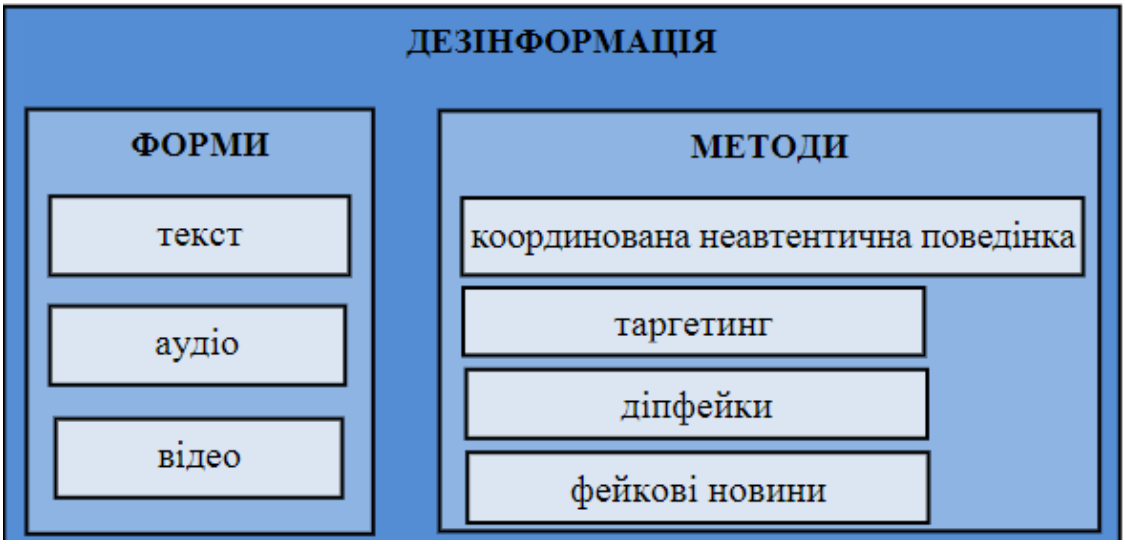

Рис. 3.2. Форми й методи дезінформації

Дезінформація у формі тексту є однією з найпростіших у створенні, оскільки майже будь-хто може написати текст і поширити його. Для цього не потрібно мати спеціальних навичок монтажу чи дизайну, як для створення відеоконтенту. Більшість публікацій на платформах, таких як Facebook, Telegram, інтернет-виданнях, а також у друкованих матеріалах є текстовими.

Відеоконтент тепер також доступний у простіших форматах, ніж раніше. Якщо раніше створення відео вимагало великих витрат часу і зусиль, то зараз відеоблогінг на найпростіших рівнях може відбуватися, просто використовуючи смартфон і доступ до Інтернету. Аудіоконтент застосовується у виступах, радіопередачах, подкастах і в особистій комунікації.

Одним з поширених методів поширення дезінформації є координована неавтентична поведінка. Цей спосіб полягає у створенні багатьох фейкових акаунтів, які залучають користувачів і в один і той же період часу поширюють ідентичні

повідомлення, посилаючись один на одного або на одне джерело. Така діяльність має на меті створити для читачів інформаційне полотно, в якому вони отримують лише те, що потрібно автору дезінформації, а інша інформація відсутня.

Однак у останні роки з'явилося і стало предметом особливого інтересу явище, відоме як *«fake news»* або фейкові новини, тобто інформаційна містифікація або намірене поширення дезінформації в соціальних медіа та традиційних ЗМІ з метою введення в оману для отримання фінансової або політичної вигоди. Важливо враховувати, що з розвитком Інтернет-технологій суспільний запит на отримання інформації про світ навколо все частіше задовольняється в мережі Інтернет, зокрема в соціальних мережах.

Deepfake – це одна з найсучасніших форм дезінформації, яка полягає у створенні підроблених аудіовізуальних записів за допомогою штучного інтелекту з метою створення ілюзії реальності. Ці фальшиві записи можуть бути використані для дискредитації відомих осіб, шантажу або приписування їм висловів, яких вони насправді не висловлювали.

У січні 2020 року Facebook оголосив про початок блокування відеозаписів із політичними deepfake, розглядаючи такий контент як дезінформацію.

Поняття «фейкові новини» стало широко відомим у 2016 році і поки що не має чіткого визначення. Наприклад, за Кембриджським словником, фейкова новина – це неправдива історія, що представлена як новина, зазвичай поширюється в Інтернеті або іншими медіа з метою вплинути на політичні переконання людей або як жарт.

На основі аналізу різних підходів до сутності поняття «фейкові новини» було визначено основні їх риси, які можуть проявлятися повністю або частково:

- Навмисне створення нового цілком неправдивого контенту або представлення суперечливої або неповної «правди», однобоке висвітлення подій.

- Відсутність фактичної бази повідомлення, але подання його як новини.

- Подання правдивої інформації у хибному контексті.

- Спрямованість на навмисне введення в оману, дезорієнтацію споживача новин.

- Подання новини від імені самозванця, тобто джерела, яке видає себе за справжнє, або посилання на анонімне джерело.

- Невідповідність заголовка чи підписів (зазвичай сенсаційних або приголомшливих) змісту повідомлення.

- Спорідненість з такими явищами, як чутки, розіграші, сучасні міфи.

- Використання гумору, сатири та перебільшення, представлення жартів як правди.

- Спрямованість на критику соціальних та політичних питань.

- Формулювання інформації у спосіб, який використовують легітимні журналістські організації.

- Використання мережі Інтернет для оприлюднення фейкових новин і їх подальшого масштабного поширення.

Соціальні мережі в Інтернеті – це зовсім інше середовище: тут порівняно з традиційними ЗМІ відсутні строгі принципи і правила поширення інформації, існує значний інформаційний плюралізм, а охоплення деяких, ні від кого не залежних, медіа персон налічує аудиторії, що рівні провідним новинним стрічкам. Недавні дослідження, проведені Центром контент-аналізу, показали, що 62% українців регулярно слідкують за новинами в соціальних мережах, і для 14% з них соціальні медіа – пріоритетне джерело новин, при цьому їх кількість зростає з кожним роком.

У 2023 році активні користувачі Facebook склали 1,8 мільярда, а Twitter – 400 мільйонів. Проте Інтернет-технології часто не є нейтральними щодо достовірності інформації: вони можуть сприяти поширенню як правдивої, так і неправдивої інформації. А замах цілеспрямованого поширення неправдоподібних новин зовсім не є безпечним, як може здатися на перший погляд.

Отже, Інтернет стає надзвичайно зручним середовищем для поширення дезінформації. Достатньо лише одного номера телефону, щоб дати можливість інформації в лічені секунди розлетітися по всьому світу. Крім відсутності будь-яких юридичних правил входу на інформаційні площадки соціальних мереж, гучні, клішові заголовки фальшивих новин викликають великий інтерес користувачів, тим самим забезпечуючи значний дохід від рекламних платформ. У зв’язку з цим, окрім

політико-ідеологічної функції фейкові новини є засобом збагачення. Саме подвійна вигода замовника і поширювача робить такий маніпулятивний інструмент, як фейкові новини, надзвичайно популярним і доступним засобом досягнення економічних і політичних цілей. Однак просто виразні заголовки недостатні для того, щоб фейк розповсюдився.

Модель споживання та пропозиції інформаційних ресурсів передбачає, що типовий споживач новин має дві характеристичні риси: по-перше, він бажає отримувати достовірну інформацію, знати об'єктивну правду про світ; по-друге, він схильний працювати з інформацією, яка відповідає його власним уподобанням. Отже, споживачі стикаються з компромісом: вони мають стимул для споживання точних новин, але також отримують задоволення від новин, які підтверджують їх звичне уявлення. При цьому інформаційне агентство отримує користь, головним чином, від реклами, яка безпосередньо залежить від чисельності аудиторії.

В цій моделі існують два стимули, що підштовхують новинні канали говорити неправду: по-перше, коли зворотний зв'язок про істинний стан навколишнього світу неможливий; по-друге, бажання відповідати вподобанням аудиторії. Агрегати фейкових новин знаходяться поза цією моделлю: вони не мають мети ні відповідати вподобанням аудиторії, ні поширювати достовірну інформацію. Вони не намагаються побудувати довгострокову репутацію, а скоріше максимізують короткостроковий прибуток від кліків у початковий період. Крім того, фальшиві новини є низько авторитетним типом інформації, тому джерелами поширення чуток є блоги з малою аудиторією. Дослідження показали, що потік фейкових новин йде від користувачів з невеликою аудиторією до більшої.

На відміну від традиційних засобів масової інформації, основний канал поширення фейкових новин – це лайки та репости. Сьогодні репост та лайк – це далеко не лише показник соціального схвалення, це специфічний та дуже важливий канал комунікації, який, крім привертання найширших та різноманітних груп суспільства, слугує психологічним інструментом, що дозволяє формувати певне ціннісно-емоційне сприйняття об'єкта.

Поведінка друзів та авторитетів у мережах суттєво впливає на споживача інформації: ймовірність того, що окрема особа репостне або лайкне певний рекламний пост, різко зростає у разі, якщо хоча б один друг проявив інтерес до цього поста, і поступово збільшується по мірі того, як багато друзів взаємодіяло з цим постом. Але лайк та репост не завжди означають схвалення контенту окремою особою. Сьогодні на ринку присутня величезна кількість сервісів, що пропонують послуги з просування блогів, окремих постів, акаунтів і т.д. Наприклад, китайська компанія «Boryou Public Opinion Influencing System» пропонує своїм клієнтам метод обробки великих обсягів даних, використовуючи колишні коментарі, пости, зображення та фотографії, а також інформацію, розміщену на їхній сторінці, для знаходження цільової аудиторії.

Для накручування голосів, лайків, репостів та поширення записів організації використовують як ботів (акаунти неіснуючих осіб), так і віруси. У другому випадку активні (реальні) користувачі можуть навіть не підозрювати, що їх сторінка була використана для поширення певної ідеї. Навіть якщо лайк був встановлений вірусним шляхом, друзі використаного аккаунта бачать оголошення «Ваш друг лайкнув цей пост», що статистично збільшує зацікавленість та надихає на поширення новини.

Пропагандисти фейкових новин активно та успішно використовують кожен з цих прийомів, незважаючи на те, що політика всіх поширених соціальних мереж в основному спрямована на придушення нечесної активності.

3.2. Приклади використання соціальних мереж для поширення дезінформації

Яскравим прикладом можемо навести інформаційні війни Росії проти України починаючи з 2014 року, мета яких полягає у «забруднені» інформаційного поля, а не у переконанні ворога, схилити на свою сторону. Метою російської інформаційної війни є забезпечення інформаційного поля, перенаситити його різноманітною, заплутаною інформацією і, таким чином, дати зрозуміти, що насправді відбувається, для пересічного громадянина стало надзвичайно складним завданням. Російські агенти роблять все, щоб українці, що проживають на Сході Україна не змогли знайти

адекватні аргументи на захист української влади, знайти раціональні перспективи тощо [1].

Ключова мета російської інформаційної війни – створити повну недовіру серед українців на Сході до української влади, армії і, звісно, до будь-яких представників європейського світу. Коли інформаційне поле знищено, працює лише людський страх, розчарування, паніка, відчуття соціального колапсу. Російська пропаганда підриває довіру жителів Східної України українській владі і прагне донести до них свою думку про рятувальну місію Росії для українців, які проживають на сході України [1].

У сучасній Росії основна мета інформаційної війни з формування єдиної національної ідеї, що згуртовує багатонаціональне, поліконфесійне суспільство на основі спільних цінностей, залишається актуальною та першочерговою. Вона становить метаструктуру пропагандистських повідомлень у мас-медіа. Її змістовне наповнення у вигляді ідей про героїчне історичне минуле (освоєння космосу, перемога у Великій вітчизняній війні) також визначають та заповнюють мезоструктури інформаційного простору. Влада розглядає свою пропагандистську діяльність як виховну, спрямовану популяризацію «цінностей російського суспільства». Відповідно до низки офіційних державних програм, до них відносяться насамперед «здоров'я, праця, сім'я, любов до Батьківщини, активна життєва та громадянська позиція та відповідальність» [4].

Соціальні медіа породили велику кількість пропаганди та дезінформації навколо російсько-української війни та стали справжнім полем інформаційної битви, оскільки обидві країни використовують соціальні медіа, щоб дискредитувати одна одну та впливати на світову громадську думку. Більше людей, особливо молоді, використовують соціальні мережі, щоб отримати доступ до того, що вони вважають більш надійними новинами. Доступ до соціальних мереж також легший і швидший, і, що найважливіше, користувачі високо цінують їх інтерактивність.

У міру розгортання російсько-українського конфлікту стало зрозуміло, що обидві використовують соціальні медіа для маніпулювання правдою, і тому багато прикладів.

25 лютого 2022 року, наступного дня після того, як Росія вперше розпочала атаку на українську територію, соціальні мережі, пов'язані з російським урядом, поширили чутки, що президент України Володимир Зеленський втік за кордон. Після того, як новина поширилася, президент В. Зеленський завантажив у соцмережі коротке відео, на якому він зображений у столиці України Києві.

Іншим прикладом інструменту пропаганди є використання історичних фактів (у даному випадку загарбницьких воєн) для співвіднесення з подіями сучасності. У своєму Twitter український уряд поширив карикатуру. Це прямо пов'язує Путіна з одним із найбільш ненависних розпалювачів війни в історії та вказує на жахи спільного кордону з агресивним російським урядом. (рис. 3.3)

Рис.3.3. Публікація в Twitter

Проте дезінформація не обмежується лише зображеннями президентів Росії та України. Фейкові новини про війну на землі відіграють певну роль у впливі на результат конфлікту та можуть легко ввести в оману громадськість, яка відчайдушно хоче знати, що відбувається. Наприклад, у лютому 2022 року обліковий запис під назвою «CNN Україна» стверджував, що активіст на ім'я Берні Горс став «першою американською жертвою війни в Україні», оскільки він загинув від «міни, встановленої підтримуваними Росією сепаратистами». Твіти про цю передбачувану подію розповсюдили сотні тисяч людей у соціальних мережах. Однак ще в серпні 2021 року в Twitter з облікового запису, який називає себе «CNN Афганістан», стверджувалося, що журналіст на ім'я Берні Горес був страчений талібами в Кабулі. У двох твітах використано одну фотографію Берні Горса. Численні користувачі

соціальних мереж були введені в оману фейковими акаунтами та критикували CNN за нібито повідомлення про те, що одна людина загинула в двох різних війнах.

Ще один метод дезінформації використовує емоційні кадри, щоб викликати підозру. Наприклад, відео переглянули понад 1,3 мільйона разів у різних дописах у Facebook, де стверджується, що на ньому зображені бої російських і українських солдатів 26 лютого 2022 року. У відео йдеться: «Бій між Україною та Росією розпалюється». Заява виявилася неправдивою. Відео циркулює принаймні з 2019 року в публікаціях про війська Французького іноземного легіону в битві в Малі.

Ще одним методом дезінформації є використання Deepfake під час російсько-української війни. Російські хакери маніпулювали українським веб-сайтом, де показали відео, на якому нібито зображений президент В. Зеленський. На відео Президент В. Зеленський просить українських військових скласти зброю. Цей випадок підкреслив потенційне використання deepfake у поєднанні з скомпрометованими медіа-сервісами для поширення оманливих повідомлень. Наслідком цього інциденту стало поширення неправдивої інформації з начебто надійного джерела. Це відео розкриває багато ознак використання технології deepfake: розмиті контури, мерехтіння обличчя (одна з очевидних речей, оскільки деякі з цих відео все ще виглядають неприродно – це стосується переходів між обличчям, шиєю та волоссям, які не завжди органічно поєднані один з одним), неприродні вирази обличчя, особливо під час моргання та низька якість відео, яка часто використовується для приховування некоректної роботи нейронної мережі.

Однак приклади використання синтетично відтвореного медіаконтенту під час війни були не лише з метою дезінформації. Наприклад, 15 січня офіційний канал Верховної Ради опублікував генероване штучним інтелектом зображення на тему теракту в Дніпрі 14 січня. На фото зображений маленький плачучий хлопчик з подряпинами на обличчі на тлі зруйнованої багатоповерхівки. Зображення дуже реалістичне: спочатку його можна сплутати з фотографією із занадто сильною ретушшю. Саме ця правдоподібність вразила публіку. Після десятка коментарів акаунт видалив пост. Коли українські медіа та дипломати докладають максимум зусиль, щоб донести до західної аудиторії наслідки російської агресії, реалістичний

образ війни, згенерований штучним інтелектом, може стати простором для маніпуляцій, тож можна з упевненістю припустити, що активний розвиток штучного інтелекту може спричинити новий вид фейкових образів, а отже, і новий рівень інформаційної війни [4].

Зауважимо, що з початком повномасштабного вторгнення Росії 24 лютого 2022 року в українському сегменті Facebook та Telegram, а також загалом в Україні, відбулося значне зростання патріотизму та проукраїнських настроїв, що відповідно призвело до збільшення антиросійських настроїв. У зв'язку з цим, грубі та очевидні інфовкиди, такі як фотошоп-фейки, якими пропагандисти щедро наповнювали власний та світовий інформаційний простір, рідко потрапляли до соціальних мереж та telegram-каналів одеського регіону. На прикладі декількох фейкових зображень, створених з метою переконати глядачів у тому, що в Україні владу захопили нацисти, можна відзначити наступне:

- Полк «Азов» з прапором із свастикою.

- Президент України, який тримає футболку із своїм прізвищем та свастикою.

- Ополонка у формі свастики, в якій нібито купається боєць полку «Азов» та інші.

Ще одним прикладом є, для переконання користувачів Інтернету у сильному впливі США на політичне і військове керівництво України, у соціальних мережах було поширено фотографію, датовану нібито 25 травня 2014 року. На цьому зображенні український генерал, стоячи на одному коліні, вручає шаблю послу США в Україні. Автор повідомлення описує цю сцену як ілюстрацію покірності українських політиків перед США, зазначаючи, що вручення особистої зброї з колін – це стандартний звичай капітуляції.

Насправді ця фотографія була зроблена рік тому в місті Херсон. У ній зображено вручення шаблі у рамках нагородження Теффту за заслуги родоначальника військово-морського флоту США Джона Поля Джонса, який у 1788 році допоміг українським козакам перемогти турків і прийняв козацьку присягу. Шабля була піднесена не як бойова зброя, а як подарунок і витвір мистецтва.

На сайті «antimaydan.com», який вважає себе форпостом антифашизму, розміщені пропагандистські плакати, серед яких є плакат під назвою «Сірі конячки Держдепу США». На зображенні представлений Дядько Сем, що уособлює США, та українські політики, які підтримали Євромайдан, зокрема П. Порошенко, А. Яценюк, Ю. Тимошенко, О. Турчинов, В. Кличко, О. Тягнибок та інші. Крім того, на цьому сайті опубліковано повідомлення про створення нового підрозділу української армії – сил спеціальних операцій (СС), яке порівнюється з гітлерівськими військовими формуваннями, що брали участь у військових злочинах Другої світової війни.

У цьому ж контексті у групі «АнтиМайдан» у соціальних мережах було розміщено повідомлення «Апартеїд по-українськи». В ньому йдеться про лист жінки з Донецька (ім'я не вказано), яка переїхала до Дніпропетровської області та потрапила під фільтрацію. У паспортному столі їй заявили, що донецьким жителям заборонено отримувати право на проживання у будь-яких областях України. Щоб отримати таке право, їм треба пройти «принизливу процедуру» та довести відсутність співпраці з сепаратистами. Після відмови у паспорті їй поставили штамп «Відмовлено у в'їзді в Україну». У Донецьку їй сказали, що програму етнічної чистки затвердив Державний Департамент США і новий президент України. Згідно з цією програмою, всі жителі Донбасу визнаються винними у сепаратизмі та позбавляються цивільних прав. Ті, хто не пройде процедуру чистки, будуть примусово вислані у сільські райони без права поселення у великих містах.

У травні 2014 року в мережі Інтернет з'явився відеозапис, що показує, як українські солдати грубо скидають мертві тіла з бойової машини під містом Краматорськ. Проте насправді цей запис був зроблений в Дагестані та опублікований у листопаді 2012 року під назвою «Публічні звірства кафірів над тілами шахідів».

Таким чином, соціальні мережі створюють нові можливості для проведення інформаційної війни. Це ідеальний простір для ведення високоефективних пропагандистських кампаній, що створюють інформаційне павутиння, яке постійно розширюється і забезпечує оперативне розповсюдження дезінформаційних повідомлень для різних цільових аудиторій.

3.3. Інструменти виявлення та боротьби з дезінформацією. Заходи регулювання та законодавчі ініціативи

З урахуванням величезного масштабу дезінформації у глобальному Інтернет-просторі та постійного зростання поширення фейкових новин перед суспільством, виникає проблема запобігання та протидії дезінформації як інструменту маніпулювання громадською думкою і свідомістю. Оскільки забезпечення порядку та інформаційної безпеки в Інтернеті на сьогодні є проблематичним, а держави не володіють ефективними інструментами для запобігання та протидії дезінформації, вирішальну роль у розв'язанні цих проблем відіграють соціальні мережі, мотивація, інструменти та сервіси, а також користувачі Інтернету. Саме останні завдяки свідомому сприйняттю та відповідальному підходу до розповсюдження інформації можуть знизити ефективність дезінформації й поширення фейкових новин.

Насамперед варто відзначити, що перевіреним методом уникнути фейкових новин є отримання інформації з надійних джерел: інформаційних організацій, які мають професійних журналістів та працюють відповідно до суворих етичних принципів.

До списку основних закордонних засобів масової інформації входять такі видання, як Reuters, Bloomberg, BBC, Financial Times, Deutsche Welle, The Washington Post. Вітчизняний Інститут масової інформації (IMI) сформував так званий «білий список» українських ЗМІ, що відзначені найвищим рівнем дотримання журналістських стандартів (у середньому 96%). До списку входять: Суспільне, Громадське, Ліга, Українська правда, Укрінформ, Радіо Свобода, Дзеркало тижня, НВ, Еспресо, Бабель.

Водночас нерідко може виникати ситуація, коли інформація ще не представлена на сайтах офіційних організацій чи ЗМІ, або на їх акаунтах у соцмережах. У таких випадках користувачу варто дотримуватися низки рекомендацій щодо методів виявлення фейкових новин, розроблених на основі дослідження.

– Перевірка джерела новин. Це включає аналіз законності і надійності джерела, дотримання стандартів точності, збалансованості та справедливості. Належить звернути увагу на такі аспекти:

- Перевірка легітимності джерела: важливо визначити, чи не є сайт «одноденним» і уникати дивних або незнайомих URL-адрес.

- Аналіз розділу «Про нас»: перевірте інформацію, що надається власниками сайту.

- Пошук підказок про законність та дотримання редакційних стандартів: деякі фальшиві видання можуть містити хибні поштові адреси або вигадані локації.

- Аналіз змісту і заголовка новини. Ознаки фальсифікованого змісту можуть включати:

- Однобічне подання фактів і оцінок.

- Вибір сенсаційних або приголомшливих заголовків.

- Використання неперевірених фото/відео.

- Посилання на соціологічні дані без вказування вибірки, замовника та географії досліджень.

Необхідно бути критичним щодо інформації, представленої у блогах, а також у соцмережах, де часто розповсюджуються чутки та неперевірені факти. Для аналізу новин з соцмереж варто перевірити їх на логічність та перевірити представлені факти в надійних джерелах.

– Для перевірки правдивості новин можна скористатися веб-сайтами перевірки фактів. Серед таких інструментів є:

- PolitiFact – це проєкт Tampa Bay Times, який перевіряє правдивість та точність політичних заяв та новин.

- FactCheck.org – це проєкт Annenberg Public Policy Center, який зосереджується на перевірці фактів у політичних заявах та новинах.

- Snopes.com – це незалежний сайт, який спеціалізується на перевірці правдивості Інтернет-чуток та дезінформації.

- The Washington Post Fact Checker – цей сервіс також спеціалізується на перевірці політичних новин та заяв.

Сьогодні в Україні виникає потреба в розвитку стратегічних підходів до національної інформаційної сфери, а це включає й організацію прогнозно-аналітичної роботи у соціальних мережах. Такий підхід дозволить вчасно реагувати на інформаційні загрози та розробляти необхідні заходи для їх запобігання.

Державі варто активніше входити до сфери мережевої комунікації, надаючи підтримку бюджетним і позабюджетним організаціям. Це означає стимулювання Інтернет-ЗМІ, електронних видань та журналістів для використання всіх можливостей мережевого спілкування. Головна мета – налагодження зв'язку з широкою громадськістю, а також пропаганда національної ідентичності, патріотизму та гуманності.

Важливо відзначити, що недостатнє використання державними установами та організаціями можливостей мережевого спілкування є неприпустимою помилкою, яка значно знижує їх ефективність у сучасному суспільстві з його новими інформаційними вимірами.

Після окупації Криму та початку російської агресії на Донбасі в Україні почалася активна законодавча діяльність, спрямована на зміцнення інформаційної безпеки та захист національних інтересів. У 2014 році Державний комітет телебачення і радіомовлення запропонував стратегію розвитку інформаційного простору України до 2020 року, а також рішення Ради національної безпеки і оборони про заходи в сфері інформаційної безпеки.

Однією зі складових цих заходів стало введення квот на україномовний контент у зусиллях зменшення впливу російської культури на українське суспільство. Такий крок мав на меті просування українських наративів та зміцнення національної ідентичності. У 2017 році, відповідно до указу президента, були заборонені великі російські соцмережі і пошуковики, а також припинено мовлення більшості російських телеканалів.

Одним із результатів цих заходів стало зменшення довіри українців до російських соціальних мереж. Наприклад, відсоток довіри до мережі «Вконтакте» скоротився до 3%. Також, важливу роль у боротьбі з дезінформацією відіграють Центр протидії дезінформації та Центр стратегічних комунікацій та інформаційної

безпеки, які активно використовують свої Telegram-канали для розвінчання фейків та просування українських наративів.

Підвищення медіаграмотності та навичок критичного мислення серед громадськості має важливе значення для формування стійкості проти дезінформації. Завдяки наданню людям можливості виявляти й оцінювати інформацію, що вводить в оману, суспільство може стати більш стійким до маніпуляцій і пропаганди.

Також, співпраця між урядом, промисловістю, академічними колами та громадянським суспільством має вирішальне значення для розробки комплексних стратегій боротьби з дезінформацією, спричиненою соціальними мережами. Об’єднуючи ресурси, досвід і технології, зацікавлені сторони можуть покращувати можливості виявлення, ділитися найкращими практиками та координувати реагування на нові загрози [2].

Крім того, необхідно запровадити заходи прозорості та підзвітності, щоб притягнути осіб, які поширили дезінформацію, до відповідальності за свої дії. Це включає посилення вимог до прозорості для онлайн-платформ, посилення дотримання існуючих законів і нормативних актів, а також міжнародну співпрацю для боротьби з транскордонними кампаніями дезінформації.

Зростання дезінформації, спричиненої соціальними мережами, підкреслює необхідність нових засобів захисту від її шкідливих наслідків. Розробляючи інноваційні інструменти, сприяючи медіаграмотності, сприяючи співпраці та впроваджуючи заходи прозорості, суспільства можуть посилити свою стійкість проти зростаючої загрози дезінформації, спричиненої соціальними мережами, і зберегти цілісність демократичного дискурсу.

ВИСНОВКИ

За результатами проведеного дослідження можемо зробити такі основні висновки:

1. Досліджено поняття «інформаційної війни», її характеристики та місце в міжнародному інформаційному праві. Проблема наукового осмислення та практичного використання інформаційної війни супроводжується суттєвими термінологічними та нормативно-правовими питаннями. Наразі не існує загальноприйнятого визначення навіть базового поняття інформаційної війни, не кажучи про інші, ціла низка яких настільки активно застосовується в публіцистиці, що поступово губиться можливість їх наукового осмислення.

У нашій роботі під поняттям інформаційна війна розуміється відкриті та приховані цілеспрямовані інформаційні впливи соціальних, політичних, етнічних та інших систем одна на одну з метою отримання певного виграшу в матеріальній сфері, спрямовані на забезпечення інформаційної переваги над противником та завдання йому матеріального, ідеологічного або іншого збитку.

В умовах гібридної війни бойові дії є другорядними, а на перший план виходять інформаційні операції та інші важелі впливу. Війна полягає у прагненні однієї держави агресивно діяти на свідомість жителів іншої. Іншими словами – це прагнення не знищити мільйони людей, а залякати й деморалізувати їх.

2. Відповідно до історичних даних, перша згадка про інформаційну війну стосується ще до V ст. до н. е. Згодом відбувалася трансформація інформаційних воєн, але головною їх метою залишалося показати перевагу армії, держави завдяки пропаганді. Слід зазначити, що у XX столітті інформаційні війни стали частиною військової політики держав. Історія показує, що основними засобами ведення цих воєн були листівки, газети; як технічні засоби – гучномовці, тобто всім знайомі ЗМІ у сучасному світі. Розвиватися інформаційні війни починали ще в давнину, потім стали затребувані та необхідні під час проведення військових дій, так теорія інформаційної війни почала розроблятися вже під час та після Першої світової війни. Під час Другої світової війни вже функціонували органи державної пропаганди На

даний момент, через ситуацію, що склалася на світовій арені, змінюються методи та засоби ведення інформаційної війни та з кожним роком вони виходять більш високий рівень.

3. Обґрунтовано, що систему суб'єктів забезпечення інформаційної безпеки держави, людини і суспільства слід розглядати у комплексному взаємозв'язку міжнародних й регіональних організацій, недержавних організацій, галузевих організацій, держави, приватного сектору та безпосередньо громадян. За такого комплексного підходу структуру суб'єктів забезпечення інформаційної безпеки можна відобразити наступним чином: міжнародній регіональні організації, недержавні організації, галузеві організації, держава, приватний сектор, громадяни.

4. Досліджено правову природу процесів формування понятійних категорій у сфері міжнародного права, форми їх закріплення та застосування в українському, зарубіжному та міжнародному праві, правозастосовній практиці та науковій доктрині. Проблеми інформаційної безпеки є предметним полем діяльності кількох міжнародних інституцій, передусім спеціалізованих організацій ООН, зокрема ЮНЕСКО й МСЕ, а також міждержавним форумам, як G7, G20, ОЕСР, ШОС, АТЕС тощо.

5. Проаналізовано, що соціальні мережі відіграють важливу роль у поширенні дезінформації через їхню широку доступність, вплив на громадську думку та здатність до швидкого поширення інформації. Вони створюють ідеальні умови для поширення неперевіреної, маніпулятивної та фальшивої інформації, яка може бути використана для впливу на громадську думку, формування певних поглядів та ставлення до подій і явищ.

Отже, у висновку ми можемо сказати, що феномен інформаційних війн у сучасних міжнародних відносинах представляє собою складний та динамічний процес, де залучаються різноманітні методи та інструменти для впливу на громадську думку, формування поглядів та впливу на прийняття рішень. Соціальні мережі стали одним з найефективніших методів поширення дезінформації у цих війнах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антипенко В. Ф. Проблеми ефективності міжнародного права. Проблеми ефективності міжнародного права: матер. тез. міжн. наук.-практ. конф., м. Київ, 29 бер. 2013 р. Київ, 2013. С. 9-11.
2. Бабенко Ю. Інформаційна війна зброя масового знищення! / Українська правда. URL: http://www.pravda. com.ua/rus/articles/2006/04/20/4399050/ (дата звернення 12.04.2024).
3. Бойченко О. Міжнародна інформаційна безпека: Проблеми і перспективи. URL: http://www.irbis-nbuv.gov.ua/ (дата звернення 9.04.2024).
4. Воробйова І. В. Інформаційно-психологічна зброя як самостійний засіб ведення інформаційно-психологічної війни. Системи озброєння і військова техніка, 2010. №1. С. 141–144.
5. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентові України, 2015. №1. С. 136–141.
6. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ: Інтертехнологія, 2009. 164 с.
7. Даниленко С. Російський народ – це перший народ, що впав під натиском власного телебачення / Дело.UA. URL: http://delo.ua/ukraine/rosijskij-narod-ce-pershij-narod-scho-vpav-pid-natiskom-vlasnog282825 (дата звернення 17.03.2024).
8. Добровольська А. Б. Інформаційний простір: проблеми становлення нової якості національного росту / Наука України у світовому інформаційному просторі. Вип. 3. К.: Академперіодика, 2010. С. 61-70
9. Дорошенко А.С. Гібридна війна в інформаційному суспільстві. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого», 2015. № 2(25). С.21-28.

10. Дубас О. П. Інформаційно-комунікаційний простір: культурно-політичні детермінанти: Монографія. Київ: Генеза, 2011. 256 с.
11. Жарков Я.М., Присяжнюк М.М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування // Вісн. Київ. нац. ун-ту імені Тараса Шевченка. Сер. Військово-спеціальні науки, 2007. №14. 15. Вип. 14. С. 42 – 44.
12. Забара І. М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. URL: http://e-pub.aau.edu.ua/index.php/chasopys/article/view/212 (дата звернення 18.03.2024).
13. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни. Вінниця: Віндрук, 2014. 384 с.
14. Зозуля О. С. Інформаційна зброя як геополітичний чинник та інструмент силової політики / Державне управління: теорія та практика, 2013. № 2. С. 82-89. URL: http://nbuv.gov.ua/UJRN/Dutp_2013_2_12 (дата звернення: 14.04.2024).
15. Зозуля О. Фейк як інструмент інформаційної війни. URL: https://yur-gazeta.com/publications/practice/inshe/feyk-yak-in- strument-informaciynoyi-viyni.html. (дата звернення 8.03.2024).
16. Інформаційні війни та майбутнє України. URL: http://siac.com.ua/index.php?option=com_content&task=view&id=1054& Itemid=44 (дата звернення 14.04.2024).
17. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. К.: Інтертехнологія, 2009. 164 с.
18. Інформаційно-психологічне протиборство (еволюція та сучасність): монографія / Я.М. Жарков, В.М. Петрик, М.М. Присяжнюк та ін. К.: ПАТ «Віпол», 2013. 248 с.
19. Калініченко Б. М. Сучасні ЗМІ як інструмент інформаційної війни. Політикус: Науковий журнал. Південноукраїнський національний педагогічний університет імені К. Д. Ушинського МОН України. Одеса: Вид-во «Гельветика», 2018. Випуск 1. С. 77–82

20. Калініченко Б. М. Форми і засоби інформаційного супроводження воєннополітичних конфліктів. Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін. Збірник наукових праць. Відп. ред. О. В. Бабкіна. Випуск 24. Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. С. 99–103.
21. Конгресмен США Еліот Енґель закликав до негайного застосування адресних санкцій проти низки українців. URL: http://ukrainian.voanews.com/content/article/1855124.html (дата звернення 16.04.2024).
22. Конгресс готов противостоять «информационной войне» Кремля // Голос Америки. URL: http://www.golosameriki.ru/content/us-russia-information-war/2722861.html (дата звернення 15.03.2024).
23. Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах. Вісник Харківської державної академії культури, 2013. Випуск 41. С. 108–113.
24. Курбан О. В. Сучасні інформаційні війни в соціальних онлайн-мережах / О. В. Курбан // Інформаційне суспільство, 2016. Вип. 23. С. 85-90. URL: http://nbuv.gov.ua/UJRN/is_2016_23_15 (дата звернення 10.04.2024).
25. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії: монографія. К.: ВКФ «Сатсанта», 2000. 222 с.
26. Лібікі М. Що таке інформаційна війна? URL: http://viysko.com.ua/texnologiji-voyen/martin-libiki - shho-take-informacijnavijna/ (дата звернення: 20.03.2024)
27. Марута Н. О., Маркова М. В. Інформаційно-психологічна війна як новий виклик сучасності: стан проблеми та напрямки її подолання. Український вісник психоневрології, 2015. Т. 23. Вип. 3. С. 21–28.
28. Медведєв В. К. Сучасна інформаційна війна та її обрис / Системи озброєння і військова техніка, 2008. № 1. С. 52-54. URL: http://nbuv.gov.ua/UJRN/soivt_2008_1_13 (дата звернення: 20.03.2024).

29. Олещук П. М. Новітні політичні технології інформаційного впливу: монографія. Київ: Видавець Вадим Карпенко, 2018. 288 с.
30. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти): дис. ä докт. юрид. наук : 12.00.11. К., 2015. 467 с.
31. Парубій А. Війна Росії проти України і світу / Українська правда, 2014. URL: http://www.pravda.com.ua/articles/2014/08/6/ 7034046/ (дата звернення 10.04.2024).
32. Парфенюк І. М. Стратегічні та стандартні інформаційні війни в Україні (на прикладі інформаційної агресії РФ). Український інформаційний простір, 2014. №2. С. 298–305.
33. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: www.justinian.com.ua/article.php (дата звернення 10.03.2024).
34. Пітер Померанцев: Мета російської пропаганди – щоб ніхто нікому не довіряв / Українська правда. URL: http://www.pravda.com.ua/articles/2015/03/31/7063251/ (дата звернення 17.03.2024).
35. Погрібна В. Л., Герасіна. Л. М. Інформаційна війна як каталізатор геополітичних змін. Європейська інтеграція в контексті сучасної геополітики: зб. наук. статей за матеріалами наук. конф., м. Харків, 24 трав. 2016 р. / редкол.: А. П. Гетьман, І. В. Яковюк, В. І. Самощенко та ін. Харків: Право, 2016. С. 72–75;
36. Політична енциклопедія. Редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. Київ: Парламентське видавництво, 2012. 808 с.
37. Політологічний енциклопедичний словник / Упорядник В.П. Горбатенко; За ред. Ю.С. Шемшученка, В.Д. Бабкіна, В.П. Горбатенка. 2-е вид., доп. і перероб. Київ: Генеза, 2004. 736 с.
38. Половко А.С. Соціальні мережі як інструмент впливу на формування політичної ідентичності молоді. *Політ. Сучасні проблеми науки. Міжнародні відносини: Збірник матеріалів XXIV Міжнародної науково-практичної*

інтернет-конференції здобувачів вищої освіти і молодих учених, Київ, Національний авіаційний університет, 02-05 квітня 2024 року. С.85-86

39. Половко А.С. Пропаганда в медіапросторі: виклики сьогодення. *Суспільно-політичні трансформації у XXI столітті: локальні, національні та глобальні контексти: Збірник матеріалів Всеукраїнської науково-практичної інтернет-конференції, Київ, Маріупольський державний університет, 18 квітня 2024 року. С.138-139*
40. Почепцов Г. (Дез)інформація. Детектор Медіа, 2019. 248 с.
41. Почепцов Г. Г. Информация и дезинформация. Киев: Ника-Центр, 2001. 256 с.
42. Почепцов Г. Г. Новые подходы в теории информационных войн: британская модель. URL: https://psyfactor.org/psyops/infowar26.htm (дата звернення 17.03.2024).
43. Почепцов Г. Г. Пропаганда vs информационные операции: сходства иразличия URL:http://osvita.mediasapiens.ua/trends/1411978127/propaganda_vs_informatsionnye_operatsii_skhodstva_i_razlichiya/ (дата звернення 17.04.2024).
44. Почепцов Г. Г. Пять новых направлений трансформации информационной войны: реализованные подходы. URL: https://ms.detector.media/trends/1411978127/pyat_novykh_napravleniy_transformatsii_informatsionnoy_voyny_realizovannye_podkhody/ (дата звернення: 21.03.2024).
45. Почепцов Г. Г. Смислові та інформаційні війни: Інформаційне суспільство, 2013. Вип. 18. С. 21-27.
46. Почепцов Г. Сучасні інформаційні війни. Вид. 3-є. доповн. та переробл. К.: Видавничий дім «Києво-Могилянська академія», 2016. 504 с.
47. Почепцов Г. Сучасні інформаційні війни. Київ: Києво-Могилянська акад., 2015. 498 с.
48. Прибутько П. С., Лук'янець І. Б. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ: Вид. ПАЛИВОДА А. В., 2007. 252 с.

49. Рижков М. Інформаційна війна. Політична енциклопедія. Редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. Київ: Парламентське видавництво, 2012. С. 298–299.
50. Росія ніколи не зупинить інформаційної війни проти України. URL: http://www.pohlyad.com/news/n/54504 (дата звернення 19.03.2024).
51. Савчук М. М. Захист інформаційних технологій та кібербезпека. Стенограма наукової доповіді на засіданні Президії НАН України 25 вересня 2019 року. Вісн. НАН України, 2019, № 11. С. 23-28
52. Семен Н. Ф. Поняття «інформаційна війна» в контексті соціальних комунікацій . Держава та регіони: серія: соціальні комунікації, 2016. № 1. с. 22-25.
53. Соснін О. В., Олійник О. В. Правові проблеми регулювання інформаційної діяльності / Стратегічна панорама, 2002. № 4. С. 166-174.
54. Требін М. П. Армія та суспільство: соціально-філософський аналіз взаємодії в умовах трансформації. Х.: Видавничий дім «Інжек», 2004. 404 с.
55. Фейки як інструмент впливу на вибори: аналітична доповідь / Дубов Д. В., Корецька І. О., Баровська А. В. та ін. (2020) Київ: Національний інститут стратегічних досліджень: центр безпекових досліджень. Школа політичної аналітики НАУКМА.
56. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. Актуальні проблеми політики : зб. наук. пр. / редкол.: С. В. Ківалов (голов. редкол.), Л. І. Кормич (голов. ред.), А. В. Полухіна (відп. ред.) [та ін.] ; НУ «ОЮА», Південноукр. центр гендер. проблем. Одеса : Фенікс, 2016. Вип. 58. С. 66-76.
57. Фурашев В. Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки // «Інформація і право». № 1(4)/ 2012. С. 46 – 55.
58. Черепанова, Є. А. Міжнародно-правовий статус інформаційної війни та інформаційної зброї / Новий юридичний вісник, 2020. № 6 (20). С. 71-73. URL: https://moluch.ru/th/9/archive/171/5325/ (дата звернення: 20.03.2024).

59. Шевченко М. М. Проблеми теоретичного визначення сутності війни. Військово-науковий вісник. 2007. Вип. 9. С. 184-194.
60. Шлапаченко В.М. Дезінформація як спосіб інформаційно-психологічного впливу. Інформаційна безпека людини, суспільства, держави. 2013. № 2(12). С. 78–86. URL: http://nbuv.gov.ua/UJRN/ iblsd_2013_2_15 (дата звернення: 15.04.2024).
61. Шумка А. В. Досвід локальних війн і збройних конфліктів другої половини XX століття у формуванні концепцій інформаційної війни. Львів : ЛВІ, 2006. – 180 с.
62. Що таке інформаційна війна. URL: my.elvisti.com/sergandr/iv.html (дата звернення 10.04.2024).
63. Bakshy E., Exposure to ideologically diverse news and opinion on Facebook / AAAS; E. Bakshy, S. Messing, L. Adamic. URL: http://science.sciencemag.org . (дата звернення 20.03.2024).
64. Denning D. Information warfare and security. URL: http://isiseurope.wordpress.com/2014/04/10/information-wars-in-thepost-modern-world/ (дата звернення 8.03.2024).
65. Gu L. The fake news machine: how propagandists abuse the internet and manipulate the public. URL: https://www.trendmicro.com, (дата звернення 8.03.2024).
66. Richard Shafransky Theory of Information Weapons. URL: http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm (дата звернення 18.03.2024).
67. The Journal of Information Warfare. URL: https://www.jinfowar.com/ (дата звернення 8.04.2024).