Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий інститут державного управління
Кафедра державного управління і місцевого самоврядування

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Ніколаєнка Владислава Ігоровича*

академічної групи *гр. 281м-21з-2 ІДУ*

спеціальності *281 Публічне управління та адміністрування*

на тему: *«Державна політика протидії інформаційної експансії Росії щодо України»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Овдін О.В.			

Рецензент				

Нормоконтролер	Вишневська О.В.			

Дніпро
2022

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи ступеня магістра на тему *«Державна політика протидії інформаційної експансії Росії щодо України».*

77 стор, 105 джерел.

ПУБЛІЧНЕ УПРАВЛІННЯ, ГІБРИДНА ВІЙНА, ІНФОРМАЦІЙНА ВІЙНА, ГІБРИДНИЙ СВІТОУСТРІЙ, ІНФОРМАЦІЙНА ДЕРЖАВНА ПОЛІТИКА, ЗАСОБИ МАСОВОЇ КОМУНІКАЦІЇ, ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО, ІНТЕРНЕТ-РЕСУРСИ, СТІЙКІСТЬ.

Об’єкт дослідження – гібридна війна як сучасна політико-правова та управлінська реальність.

Предмет дослідження – державна політика протидії інформаційної експансії Росії щодо України

Мета дослідження – проаналізувати особливості введення гібридної війни в інформаційному просторі в умовах агресії Російської Федерації проти України та визначити складові чинники інформаційного протистояння Росії проти України, вдосконалити механізми протидії російській інформаційній експансій в умовах сучасного гібридного світоустрою.

У першому розділі проаналізована сутність поняття «інформаційна експансія», «інформаційна війна». Другий розділ визначає загальну характеристику інформаційної експансії Росії щодо України та окреслено форми застосування, механізми, стилі реалізації комунікаційних маніпулятивних технологій. У третьому розділі розглядається необхідність вдосконалення механізмів протидії російській інформаційній експансій в дискурсі зарубіжного досвіду та вітчизняної практики

Сфера практичного застосування результатів роботи – органи влади та місцевого самоврядування, інститути громадянського суспільства.

ABSTRACT

Explanatory note of the master’s degree qualification thesis on the topic

«State policy of countering Russia's informational expansion in relation to Ukraine».

77 pages, 105 sources.

PUBLIC ADMINISTRATION, HYBRID WARFARE, INFORMATION WARFARE, HYBRID WORLD SYSTEM, INFORMATION PUBLIC POLICY, MASS COMMUNICATION MEDIA, CIVIL SOCIETY, INTERNET RESOURCES, SUSTAINABILITY

The object of research is hybrid war as a modern political, legal and managerial reality.

The subject of the study is the state policy of countering Russia's informational expansion in relation to Ukraine

The purpose of the study is to analyze the features of the introduction of hybrid warfare in the information space in the context of the aggression of the Russian Federation against Ukraine and to determine the constituent factors of the information confrontation between Russia and Ukraine, to improve the mechanisms of counteraction to Russian information expansion in the conditions of the modern hybrid world system.

The first chapter analyzes the essence of the concept of «information expansion», «information war».

The second section defines the general characteristics of Russia's information expansion in relation to Ukraine and outlines the forms of application, mechanisms, styles of implementation of communication manipulative technologies.

The third chapter examines the need to improve the mechanisms of counteraction to Russian information expansion in the discourse of foreign experience and domestic practice

The sphere of practical application of the results of the work - authorities and local self-government, institutions of civil society.

ЗМІСТ

ВСТУП

Актуальність обраної тематики роботи полягає в тому, що проблема гібридної війни потребує особливої уваги та наукового обґрунтування, оскільки це явище не тільки гальмує розвиток інформаційного суспільства, а й зачіпає практично всі пріоритетні сфери життя в усьому світі. Інформаційні технології в сучасному житті є невід'ємною складовою інфраструктури людства. Інформація є базою для прийняття рішень.

Протягом останніх років у світі спостерігається стрімкий розвиток новітніх інформаційно-телекомунікаційних технологій, їх поширення та впровадження серед широких верств населення. Постійний розвиток інформаційно-комунікаційних технологій приводить до таких позитивних змін, як стимулювання конкуренції, розширення виробництва, що забезпечує економічне зростання і зайнятість населення, підвищує ефективність функціонування практично всіх сфер життєдіяльності шляхом переходу на нові засади обробки та передачі інформації. Але, зважаючи на здатність інформації впливати на суб'єктів та повністю змінювати поведінку людини, суспільства або держави в необхідному напрямків, існують випадки, коли позитивні властивості інформації та інформаційних технологій можуть бути використані для досягнення як корисних, так і незаконних цілей. Технічний прогрес суттєво скорегував методи військових, торговельних, економічних конфліктів, унаслідок чого прямі силові методи стали поступатися інформаційним.

Латентність, оперативність, лабільність, доступність, ємність, а найголовніше – інтерактивність і мережева архітектура, відносно низька вартість при значному ефекті, універсальність – усе це визначає інформаційну епоху як епоху інформаційних війн, атак без прямого військового конфлікту. Гібридні війни стають найпоширенішим засобом досягнення цілей у внутрішній та зовнішній політиці. Бурхливі події, які відбуваються в Україні, є наслідком прояву такої війни: потік інформації стає все менш і менш керованим, а управління збройними та не збройними конфліктами

перемістилося з поля бою в інформаційний простір. На наш погляд, вивчення структурних компонентів війни, яку породило інформаційне суспільство, її проявів та тактики ведення, надасть можливість об'єктивно оцінити сучасні реалії, не піддатись впливу шкідливих технологій, що активно застосовуються серед населення нашої держави.

Отже, актуальність теми зумовлена тим, що проведена інформаційно-пропагандистська кампанія із залученням російських спецслужб спричинила потужний деструктивний вплив на свідомість громадян України, місцеве населення Криму та Сходу України, суміжних територій та перетворилася на чинник загрози національній безпеці держави. Гібридна війна складається з комплексу технологій інформаційного та психологічного впливу, який спрямовано на трансформацію стану масової та індивідуальної свідомості та психологічного самоусвідомлення громадян конфліктуючих сторін.

Стан і ступінь розробки проблематики в спеціальній літературі. В процесі роботи використані погляди, узагальнення і висновки з досліджуваної проблеми, викладені в працях вітчизняних та зарубіжних вчених, фахівців з публічного управління, політології, історії, соціології, дослідників з інших галузей знань, які мають принципове значення для осмислення і розв'язання сформульованих завдань дослідження Зарубіжні дослідники Д. Ласіка, М. Маклюєн, Дж. Н. Маттіс, Френк Г. Хоффман уперше розкрили феномен «війни гібридного типу» та проаналізували її складові. Проблематика дослідження гібридної війни та її складових висвітлена в наукових розвідках українських дослідників: В. Горбуліна, Л. Залізняка, Т. Ісакової, С. Козиряцької, М. Лазаровича, Є. Магди, Г. Почепцова, І. Рущенка, В. Тарасюка, І. Тодорова. Окремим аспектам гібридної війни та її інформаційної складової приділено увагу в працях Д. Арабаджиєва, В. Гулая, В. Гусарова, Н. Ніколаєнко, Г. Щедрової.

Дослідивши значну кількість теоретичних джерел, наукових публікацій, автор робить висновок про те, що проблема аналізу державної політика протидії інформаційної експансії Росії щодо України всебічно не досліджена,

залишається багато дискусійних питань, а зазначена проблематика до 2014 року не отримала достатнього вивчення в українській науковій спільноті.

Об'єктом дослідження є гібридна війна як сучасна політико-правова та управлінська реальність.

Предметом дослідження є державна політика протидії інформаційної експансії Росії щодо України

Мета дослідження – проаналізувати особливості введення гібридної війни в інформаційному просторі в умовах агресії Російської Федерації проти України та визначити складові чинники інформаційного протистояння Росії проти України, вдосконалити механізми протидії російській інформаційній експансій в умовах сучасного гібридного світоустрою.

Досягнення поставленої мети передбачає вирішення наступних *дослідницьких завдань:*

- проаналізувати сутність поняття «інформаційна експансія», «інформаційна війна»;
- висвітлити особливості інформаційного протистояння Росії проти України;
- визначити форми застосування, механізми, стилі та сферу реалізації комунікаційних маніпулятивних технологій;
- дослідити особливості застосування технологій маніпуляції свідомістю громадян застосовані під час анексії Криму в контексті інформаційної гібридної війни;
- визначити пріоритети інформаційної державної політики в Україні;
- охарактеризувати складові чинники механізмів протидії інформаційній експансії Росії щодо України;
- обґрунтувати необхідність вдосконалення механізмів протидії російській інформаційній експансій в дискурсі зарубіжного досвіду та вітчизняної практики.

Методи дослідження. Теоретико-методологічною основою магістерської роботи є загальнонаукові методи (історичний, соціологічний, структурно-

функціональний, системний, інституційний, соціально-психологічний, діяльнісний, аксіологічний, а також аналіз і синтез, індукція і дедукція, абстрагування і конкретизація, моделювання, систематизація, класифікація, типологізація тощо), що утворюють інструментальний каркас дослідження. Історично-порівняльний метод дав змогу визначити спільне й відмінне у війнах минулого та сьогодення, до яких належить гібридна війна. Логіко-семантичний підхід дав змогу проаналізувати понятійно-категоріальний апарат гібридної війни. На основі інституційного методу визначено логіку та особливості інформаційного впливу в умовах гібридної війни. Оцінка перспектив впливу гібридної війни на суспільство здійснювалася за допомогою аналітико-прогностичного методу.

Практичне значення одержаних результатів полягає в подальшому використані в подальшій науковій розробці проблеми та формуванні практичних засад при створенні механізмів протидії інформаційній експансії в контексті російсько-української гібридної війни. Крім того, зміст і висновки роботи суттєво розширюють спектр наукових знань з публічного управління.
Триваюча російсько-українська гібридна війна демонструє важливість вироблення механізмів протидії інформаційній експансії країни-агресора. На думку автора, для подолання прорахунків та недоліків потрібно створювати державну дієву програму протистояння деструктивному впливу засобів масової комунікації, а перед українською школою публічного управління стоїть важливе завдання – сформувати дискурс розвитку Української держави, враховуючи реалії гібридної війни.

Обсяг і структура роботи обумовлені метою та дослідницькими завданнями представленої курсової роботи. Дана робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

Загальний обсяг магістерської роботи становить 73 сторінки.

РОЗДІЛ 1.
ІНФОРМАЦІЙНА ЕКСПАНСІЯ РОСІЇ ЯК ЗАГРОЗА ДЕЖАВНОМУ СУВЕРЕНІТЕТУ УКРАЇНИ

1.1.Теоретико-методологічні підходи до аналізу понять «інформаційна експансія», «інформаційна війна».

XXI століття – епоха інформаційних технологій та глобальних інтеграційних процесів. Інформаційні технології застосовуються майже у всіх сферах суспільного життя, що робить суспільство і кожного конкретного індивіда все більш залежним від інформації.

Сьогодні на інформаційному просторі ведуться інформаційно-психологічні війни. Інформація – глобальний ресурс сьогодення, за допомогою якого збільшується ефективність керування в усіх сферах життя. Практично в усіх збройних конфліктах за останні десятиліття ефективно використовувалися методи та засоби інформаційної боротьби, які можуть призвести до таких трагічних наслідків, як: зміна суспільного ладу та політичного устрою; розпад держави; втрата армії; розвал економічної системи в країні; страта національної ідеї та духовних цінностей; загибель людей тощо.

Нині на часі наукове обґрунтування нових форм ведення збройної боротьби. Сьогодні буває складно визначити межу, за якою починається і закінчується власне війна. Наукові досягнення та технології дозволяють вести війну в найрізноманітніших формах та без її оголошення чи навіть дотримання її легітимних стандартів.

Все частіше інформаційні технології використовуються для маніпулювання масовою свідомістю, впливу та управління людьми. Дана тенденція, що є загальносвітовою, на теперішній час набула особливого значення для України у зв’язку з гібридною війною, яку вже майже чотири роки веде проти українського народу сусідня держава.

Гібридні сили успішно використовують технологічно передові системи

таким чином, що вони працюють на межі можливостей. Тому гібридні збройні сили мають перевагу над традиційною армією, яка діє суворо в рамках уставу. Найбільше ж важить контроль за інформаційними потоками.

«Інформаційна експансія» є технологією набагато місткішою, ніж «інформаційна війна» або «інформаційна атака». Власне, ці терміни можна вважати складовими інформаційної експансії. В свою чергу, терміном «інформаційна експансія» позначають систему, що склалася в засобах інформації розвинених держав, і методи, використані для пропагандистського забезпечення певних геополітичних цілей. Інформаційну експансію можуть створювати і поширювати як державні органи (за допомогою державних і приватних інформаційних установ і заходів), так і транснаціональні корпорації для досягнення власної вигоди: забезпечення ринку збуту, участь у великих міжнародних тендерах, доступ до дешевої сировини і робочої сили, політичні та військові цілі тощо. Мета інформаційної експансії: вплив на владу іншої країни для прийняття/скасування певних рішень, дій, інтеграційних намагань, демократизації тощо; контроль в укладенні міжнародних угод, формуванні міжнародних спілок; втручання в геополітичну, військову, економічну концепції країни; — вплив на громадян країни для тиску на владу, а також з рекламно-пропагандистськими мирними цілями (приміром, напередодні сезону відпусток, щоб залучити іноземних громадян до своїх курортів) [67, с. 71].

Ознаками інформаційної експансії на сьогодні можна вважати: монополізацію газет, журналів радіо і телебачення, а також засобів зв'язку спеціалізованими корпораціями; пряме підпорядкування засобів інформації та зв'язку олігархічному капіталу; відкрите втручання державних органів у сферу ЗМІ, заборону або позазаконне обмеження свободи слова; панування порівняно невеликої кількості засобів масової інформації й інформаційних агентств на світовому ринку новин; монополізацію інформаційного простору країни або регіону; поглиблення диспропорцій у забезпеченості засобами інформації та зв'язку між розвиненими державами і країнами, що розвиваються; використання друкованою пресою, радіо, телебаченням та інформаційними

агентствами розвинених країн інформаційного забезпечення власної внутрішньої та зовнішньої політики на теренах інших країн; публікацію низки матеріалів, спрямованих на дискредитування певної політичної сили, заходу, політика; створення негативного іміджу політичної сили, руху, державно[59, с. 10].

Г.Г. Почєпцов визначає інформаційну війну як комунікаційну технологію впливу на масову свідомість з метою зміни когнітивної структури таким чином, аби впливати на зміни в поведінці людей [55, с. 7].

Термін «інформаційна війна» вперше вжив 1967 року колишній директор ЦРУ Ален Далес у книзі «Таємна капітуляція». Наступного разу термін з'явився у аналітичній доповіді американського дослідника Т. Рона для компанії Boeing «Системи озброєння та інформаційна війна». На думку аналітика, інформаційна структура стає найбільш важливим елементом економіки з одного боку, та найбільш вразливою мішенню з іншого.

Одним із перших у відкритому друці, хто написав про феномен інформаційних воєн був М. Маклюєн у 1960 роках. Уже тоді було відомо, що «холодна війна» ведеться за допомогою інформаційних технологій, так як у всі часи війни велися з допомогою передових технологій. Дослідник відмітив, що якщо «гарячі» війни минулого використовували зброю, знищуючи ворогів одного за іншим, то інформаційна зброя за допомогою телебачення та кіно, навпаки, занурює все населення у певний світ уяви: «земна куля тепер – не більше, ніж село» [39, с. 7].

Інформаційна війна є тотальним явищем, де неможливим є визначення його початку та кінця. Зокрема, на думку С. Расторгуєва, інформаційна війна – це наявність боротьби між державами за допомогою інформаційної зброї, тобто це відкриті та приховані цілеспрямовані інформаційні впливи систем (держав) одна на одну, з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи з допомогою таких засобів, використання яких дозволяє досягати задуманих цілей [62, с. 455–456].

П. Шпига та Р. Рудник [66, с. 328] повідомляють, що нині є 4 підходи до

визначення даного поняття:

- перший підхід трактує їх як сукупність політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного простору, витіснення ворога з інформаційної сфери, знищення його комунікацій, позбавлення засобів передачі повідомлень, а також інші подібні цілі;

- за другим підходом інформаційна війна – це найгостріша форма протистояння в інформаційному просторі, де першочергового значення набувають такі якості взаємодії, як безкомпромісність, висока інтенсивність суперечки та коротко тривалість гострого суперництва;

- за третім підходом інформаційна війна інтерпретується як форма забезпечення та ведення військово-силових дій за допомогою найсучасніших електронних засобів (цифрових випромінювачів, супутникових передавачів та інших аналогічних засобів, які застосовуються для виконання військових завдань);

- четвертий підхід ототожнює інформаційні війни з кібернетичними війнами (протистояння між технічними системами).

Українські дослідники Д. Богуш та О. Юдін зазначають, що про ведення інформаційної війни можна говорити лише в тому випадку, коли здійснюється комплексний вплив на інформаційну сферу противника, який передбачає створення умов для ведення бойових дій або виступає як самостійний чинник, який змушує конфронтуючу державу відмовитись від намічених політичних, економічних чи інших цілей [71, с. 145]. При цьому особливостями інформаційної війни в будь-якому випадку є ризик і невизначеність її результатів.

Р. Чирва стверджує, що головне завдання інформаційних воєн полягає в маніпулюванні масами, дезорієнтації та дезінформації громадян, залякуванні супротивника своєю могутністю [78]. Якщо розглядати нові інформаційні технології, як зброю, то ми приходимо до висновку, що вони здатні обернутися для людства катастрофою, адже в якості інструмента політики інформаційна

війна означає панування одного суспільства шляхом обдурення народу іншої країни. Є. Магда вважає, що інформаційна війна проти України спрямована не лише на розхитування ситуації всередині держави, а і на створення негативного іміджу України в світі.

Комбінації інформаційно-психологічного, економічного та військового протиборства використовувались і раніше. Але гібридність сучасного конфлікту в тому, що питома вага факторів принципово інша. Набагато потужнішою також є використання засобів та особливостей інформаційного суспільства. Відтак, нагальною очевидною потребою є формулювання асиметричної, так само гібридної відповіді на гібридну загрозу, ключовим аспектом якої є інформаційна війна.

Події кінця 2013 – початку 2014 року стали драматичними для України. Внаслідок дестабілізації внутрішньої політичної ситуації, експансії Криму та «гібридної війни» на сході України.

Інформаційна війна проти України спрямована не лише на розхитування ситуації всередині держави, а і на створення негативного іміджу України в світі. Стартував цей процес ще 2005 року під час першої газової війни. Тоді Україну успішно представили в якості нечесного, а щонайменше сумнівного транзитера газу, незважаючи на те, що протягом десятиліть Україна ніколи не допускала зриву поставок природного газу до Європи через свою територію. До того ж звинувачення у крадіжках газу не підкріплювалися конкретними фактами [11].

Перші системні ознаки інформаційних утисків з боку російської сторони почали з’являтися після парламентських виборів 2006 року, коли в Криму перемогу одержала Партія регіонів та «Русский блок», які почали перешкоджати діяльності місцевих медіа. Засоби масової комунікації, засновані кримською владою зазнавали цензури, до того ж кримською владою контролювалося і державне республіканське телебачення, яке формально підпорядковувалося Києву. Однією з основних тенденцій українського інформаційного ринку, як Криму так і України в цілому, було те, що він

розвивався не як бізнес, а як ідеологічне поле битви, та використовувався саме для інформаційних війн. Так само реалізувалися у Криму і російські спецпроекти, зокрема через фінансову підтримку окремих видань, через спроби міняти засновників медіа тощо.

Вже майже чотири роки Україна знаходиться в стані неоголошеної війни з РФ. Гібридна війна, яку розв'язано проти України, ведеться одразу на декількох рівнях та напрямах, одним з яких є, безумовно, інформаційний. В цьому плані було застосовано цілий арсенал методів пропаганди і політичних провокацій. Серед них першочерговим засобом впливу на українську суспільну думку стало поширення через супутник сигналу ключових російських телеканалів практично на всю територію України. Мова йде не про свободу слова, чи озвучення іншої точки зору, а насамперед про брехливу агресивну інформаційну війну, яку підконтрольні Кремлю ЗМІ ведуть сьогодні проти України [72].

Росія використовує широкий спектр методів гібридної війни які в свою чергу є складовими мозаїки інформаційної війни [77] , а саме:

- «криве дзеркало» – перекручування та пересмикування фактів та дискурсів;

- «легітимний вигнанець» – можливість використання особи колишнього Президента Віктора Януковича для тиску та потенційно піддання сумнівам легітимність нинішньої влади;

- «спекуляції на історії» – вочевидь не новий інструмент, сутність якого полягає у педалюванні дискусійних моментів українсько-російської історії;

- «заперечення очевидного» має на меті зберігати обличчя, створювати видимість відсутності агресії; - «килимове бомбардування дезінформацією» призводить до зростання панічних настроїв, зневіри, появи численних ліній розколу в українському суспільстві, що врешті має призвести до дестабілізації ситуації всередині країни;

- «перетягування Заходу» – намагання створити проросійську коаліцію помножуються на активне лобіювання інтересів Росії діючими та колишніми

європейськими політиками. До цього варто також додати активну інформаційну компанію, яка спрямована на формування позитивного образу Росії в Європі;

- «показна миротворчість» так само має на меті створити ілюзію Москви як мирно налаштованої та непричетної до конфлікту сторони. З іншого боку, має запевнити в наявності інтересів Росії на території України та права їх відстоювати;

- «гримаси демократії» використовуються для нагнітання внутрішньополітичного напруження в Україні. Марш «Барсу» та ВВ-шників на Київ – яскравий приклад використання такого методу;

- «економічні лещата» мали б підштовхнути Україну до економічного краху. Виснажена та об'єктивно залежна від російських ринків економіка й нині знаходиться на межі, втім, спостерігаються і позитивні тенденції;

- «фактор газу для Європи» – випробувана стратегія звинувачення України у минулих реальних та майбутніх потенційних проблемах із зимовими поставками газу [77]

Отже, інформаційна війна як складник збройного конфлікту не є новим явищем, проте сучасні інформаційні канали досі не захищені від зовнішнього впливу та через брак ресурсів, часто-густо стають найвпливовішою зброєю в руках пропагандистів. Як вважає більшість дослідників інформаційного суспільства, лідерство у XXI столітті визначається не економічним фактором, а його здатністю контролювати інформаційні процеси. Інформаційні операції стали у наш час вагомою частиною військових стратегій багатьох країн. Останні досягнення в галузі науки і техніки привели до революційних змін у всіх сферах суспільного життя. У зв'язку з цим, питання інформаційної незалежності, відіграють важливу роль у підтримці національної безпеки, набирають вирішальне значення для збройних сил країни та її силових відомств. Інформаційні технології змінили звичні критерії оцінки військової потужності. Змінилися також традиційні форми збройної боротьби. Міжнародні події останнього десятиліття свідчать, що технологічна і, насамперед, інформаційна перевага відіграють вирішальну роль у досягненні цілей війн і

збройних конфліктів. На даному етапі ряд країн публічно проголосили політику з питань підготовки до інформаційної війни, яка розглядається як частина їх оборонних доктрин.

Щоб встояти перед дезінформацією та маніпуляціями, яку вміло застосовують ЗМІ та розповсюджується за допомогою різних комунікаційних каналів, людина повинна правильно фільтрувати інформацію, критично мислити, аналізувати, звертати увагу на джерела інформації, на власників медіа, «бо по мірі збільшення усвідомлення маніпуляція зменшується».

Породженням XXI століття стали так звані «гібридні війни», які є симбіозами руйнації військово-політичної системи супротивника шляхом шантажу, підкупу, диверсій, дискредитацій, інформаційного тиску, маніпуляцій масовою свідомістю. Комбінація військових та невійськових методів з залученням протестного потенціалу населення складають суть війн нового покоління [38].

Водночас поняття гібридної війни охоплює явище набагато ширше, ніж сучасні форми ведення бойових дій, види війн майбутнього або назви конкретних конфліктів змішаного типу. Насправді йдеться про оформлення нового виду глобального протистояння у сучасному дестабілізованому міжнародному безпековому довкіллі. Гібридна війна не є поверненням до стану холодної війни. Вона приходить їй на зміну, у супроводі ланцюгів гарячих конфліктів, як нова, ускладнена й нестабільна форма відносин на міжнародній арені.

Таким чином, цей термін має на увазі «об’єднання» традиційних засобів і методів застосування збройної сили і дій, супроводжуючи її застосування, і використання конфліктуючими сторонами політичних, дипломатичних, економічних та інформаційних інструментів, а також проведення підривної діяльності на території противника з метою реалізації на нього неозброєного тиску і формування громадської думки, що забезпечують психологічну перевагу над противником і міжнародну підтримку.

У різного роду термінологічних словниках можна зустріти різні

трактування поняття гібридна війна, наприклад: «Гібридна війна» це свого роду воєнна стратегія, яка об'єднує звичайну війну, малу війну та кібервійну. Термін «гібридна війна» використовують також для опису атак із застосуванням ядерної, біологічної та хімічної зброї, саморобних вибухових пристроїв та інформаційних технологій. Такий підхід до ведення конфліктів є потужним і складним різновидом війни. Іноді цей термін застосовують тоді, коли потрібно охарактеризувати складну динаміку бойового простору, що передбачає гнучку реакцію, потребує швидкої адаптації [38]

Гібридна війна планується не під стратегію фронтальної війни, а під стратегію інформаційної війни, де відбувається побудова альтернативної зомбі-реальності, всередині якої є можливим перетворення супротивника на ворога (приреченого на фізичне знищення) і нелюдь (хто не має права вважатися людьми). Так, Хофман вважає, що гібридна війна містить п’ять елементів: модальність проти структури, одночасність, злиття, комплексність, злочинність. Ці характеристики підходять навіть до простих політичних акцій. Гібридну війну відокремлює те, що вона містить одне правило – жодних правил. Її тактика відзначається гнучкістю та різноманіттям, тут можливо все. Головною і керуючою складовою гібридної війни є інформаційна, яка, маючи давню історію, на сьогодні набуває нової, модифікованої форми.

Головна мета гібридної війни, на відміну від війни класичної, – послабити державність супротивника з наміром її зруйнувати або поставити під латентний зовнішній контроль управління, завдати істотної шкоди його безпеці переважно неозброєними засобами. Істотна особливість гібридної війни полягає у майже відсутності межі між станом війни і миру. Ми вперше спостерігаємо ситуацію, коли неозброєні засоби і методи з більшою ефективністю забезпечують досягнення стратегічних цілей, ніж традиційні засоби і методи ведення війни.

Отже, гібридна війна – це війна, основним інструментом якої є створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які звичайно досягаються звичайною війною.

1.2. Особливості інформаційного протистояння Росії проти України

Аналіз воєнних конфліктів початку XXI століття свідчить про появу нових форм і методів збройної боротьби між державами для досягнення відповідних політичних цілей і вирішення міждержавних протиріч. На зміну класичним формам збройної боротьби прийшли так звані «гібридні війни».

Вони мають прихований характер та проводяться, переважно, у політичній, економічній, інформаційній та інших сферах. При цьому, для вирішення окремих завдань збройні сили залучаються в невеликій кількості. Сутність такого підходу полягає у зміщенні центру зусиль з фізичного знищення противника в рамках масштабної війни до застосування засобів так званої «м'якої сили» проти країни-противника з метою дезінтеграції та зміни її керівництва, включення до сфери свого впливу.

Російська Федерація застосувала проти України концепцію «гібридної війни», яка багато в чому є унікальною із структурно-функціонального погляду – за формою вона «гібридна», а за змістом – «асиметрична». Найчіткіше характер нового типу війни продемонстрували спочатку анексія РФ навесні 2014 року території Автономної Республіки Крим (АРК), а потім – підтримка місцевих радикальних елементів та повномасштабне вторгнення російських підрозділів до східних областей України, що привело до фактичної втрати контролю над частиною Донецької та Луганської областей [36].

РФ використовує в Україні всі компоненти:

- гібридних війн – регулярну армію, нерегулярні військові утворення, тероризм, інформаційну, економічну, соціальну, енергетичну та кібернетичну боротьбу;
- асиметричної війни (війна між противниками, у військових силах яких є істотний дисбаланс або які застосовують кардинально різні стратегії і тактику). З метою компенсування дисбалансу традиційних засобів ведення бою, РФ звертається до нетрадиційних засобів – партизанська війна,

пасивний опір, терористичні акти, психологічна війна, підтримка антиурядових угрупувань, підтримка антиурядових рухів (партій) тощо.

Кожен конкретний елемент цієї «гібридної війни» не новий по суті і використовувався у війнах минулого, однак унікальними є узгодженість і взаємозв'язок цих елементів, динамічність та гнучкість їх застосування, а також зростання ваги інформаційного чинника. Причому інформаційний чинник стає самостійною складовою і виявляється не менш важливим, ніж військовий.

Головною метою РФ у гібридній війні проти України є послаблення та децентралізація нашої держави, зміна її європейського курсу, повернення України під контроль РФ. Передумовами початку гібридної війни РФ проти Україні є:

- наявність у РФ значного політичного прошарку, зацікавленого у реалізації власних імперських амбіцій;
- прагнення РФ повернути світ від багатополярного стану до біполярного;
- усвідомлення керівництвом РФ загрози, якою буде для неї успішна Україна;
- залежність значної частини ЄС від поставок російських енергоносіїв;
- очевидне бажання Кремля шляхом підкорення України зламати волю до опору не лише країн СНД, але і республік Балтії та Польщі.

Аналіз подій в АРК та на сході України свідчить про те, що гібридна війна РФ проти України не була нагальною. РФ на протязі тривалого часу готувалась до цих подій, здійснювався вплив на керівництво України.

Характерними особливостями нинішньої гібридної війни є [26] :

- агресія без офіційного оголошення війни;
- приховування країною-агресором своєї участі в конфлікті;
- активне використання асиметричних бойових дій і мережевої війни, тобто війни, що не має одного і явного центру управління війною;
- широке використання нерегулярних збройних формувань (в т. ч. під прикриттям мирного населення) під гаслами і виглядом громадянської війни;

- неофіційне залучення державою-агресором недержавних виконавців – «ввічливих чоловічків», «добровольців», які, по суті, є найманцями і не зв’язані міжнародним правом;
- нехтування агресором міжнародними нормами ведення бойових дій та чинними угодами і досягнутими домовленостями;
- взаємні заходи політичного та економічного тиску;
- протистояння у кібернетичному просторі;
- проводяться проти слабких місць держави і місцевого населення;
- не мають явного тилу і фронту;
- широко використовують методи інформаційної боротьби і терору;
- миттєва реакція на зміну обстановки і гнучкість управління, при видимості його відсутності (керований хаос).

Крім того, ще однією з особливостей є одночасне застосування всіх методів і технологій, поєднання використання технологій м'якої і жорсткої сили з метою дезінформації та зміни керівництва держави, включення її до сфери свого впливу. Серед цих методів і технологій слід зазначити деякі, в яких агресор досяг певної досконалості:

- розвідка і контррозвідка;
- інформаційна, дезінформаційна і пропагандистська війна, що в даний час стала потужним інструментом ведення війни;
- кібервійна;
- широке використання спеціальних підрозділів;
- широке використання неурядових факторів (бізнес, незаконні збройні формування, релігійні організації, криміналітет, приватні особи), що діють порівняно незалежно, але під загальним керівництвом і централізованим управлінням;
- широке використання терористичних актів та підривних дій;
- енергетична війна;
- економічна війна, включаючи торгові, фінансові та інші інструменти;
- корупція, що виведена на принципово новий рівень, практично

перетворившись на оптові закупівлі політичного і воєнного керівництва в країнах, які піддаються агресії;

- застосування інформаційних технологій для організації масових протестних рухів у відкритій та прихованій формах, політичного та економічного саботажу;
- організація транснаціональних та регіональних об’єднань політичних сил в підтримку (або проти) політики провідних держав або окремих лідерів [38]

До початку безпосередніх дій гібридної війни РФ здійснювала [19, 26] :

- навмисну дестабілізацію внутрішньополітичної обстановки в Україні;
- ідеологічну обробку свого населення для об'єднання навколо ідей націоналізму, великодержавного шовінізму, захисту так званих «руського миру», «національних цінностей і інтересів», боротьби із «зовнішнім ворогом», а також максимальне ослаблення опозиції у всіх її проявах;
- потужну інформаційно-пропагандистську кампанію захоплення інформаційного простору України і використання його в своїх інтересах для формування у населення необхідного суспільного настрою;
- дискредитацію зовнішньої і внутрішньої політики України, нав'язування її керівництву і населенню певних ідей і цивілізаційних цінностей шляхом проведення активної інформаційної кампанії із застосуванням як державних, так і неурядових організацій;
- підрив державної влади, в тому числі, підкуп впливових урядовців, політичних діячів і керівництва силових структур, просування агентів впливу на посади в державні органи влади, розпалювання протистояння між різними політичними силами і встановлення контролю над ними;
- внесення розколу серед населення України шляхом стимулювання внутрішніх суперечностей політичного, міжнаціонального і міжрелігійного характеру (зокрема, в рамках створення і підтримки різних партій, рухів і організацій певного, в т.ч. екстремістського толку);
- підрив довіри населення до влади, а також розповсюдження в суспільстві протестних і сепаратистських настроїв методом провокації соціально-

економічних та інших проблем. [77]

Загальна схема гібридної війни РФ проти України полягає в наступному. Гібридна війна розпочинається з інформаційної війни і народних хвилювань проти діючої влади. На другому етапі відбувається просування підбурювачів, провокаторів і диверсантів під виглядом місцевого населення, які розгойдують і розжарюють ситуацію. Поступово організаційну ініціативу беруть люди, завербовані спецслужбами РФ, або навіть громадяни РФ. Далі в ході загострення конфлікту і переходу його в збройну стадію, долучаються добровольці і найманці, фахівці зі зброї і спецназівціз РФ, які діють приховано, під виглядом місцевих ополченців, або відкрито, не приховуючи свого російського громадянства (наприклад, козаки, інтербригада тощо).

Висновки до 1 розділу

Таким чином, комплекс економічних, фінансових, матеріально-технічних, інформаційно-пропагандистських та військових заходів, що здійснює РФ проти України, спеціалісти характеризують як гібридну війну, або латентну агресію.

Сьогодні Україна протистоїть агресору в особі РФ, який впровадив хаос в усю конструкцію післявоєнної побудови Європи. Агресор використовує новий формат ведення війни, сподіваючись уникнути відповідальності за життя людей, зруйновані оселі та промисловість країни, яка не бажає йти у фарватері політики РФ. Дипломатична, консультаційна та фінансова допомога з боку наших партнерів та санкції проти РФ є значним фактором впливу, але необхідно застосування ще більш потужних заходів впливу на РФ та надання Україні більших спроможностей для оборони своєї землі.

Таким чином, сучасна гібридна війна демонструє поєднання принципово різних типів і способів ведення війни, які цілеспрямовано застосовуються за певним розробленим планом для досягнення стратегічних цілей руйнування держави та поглинання території. Складовими елементами гібридної війни стало використання інформаційних методів, які сприяють створенню, розвитку та загостренню внутрішніх конфліктів.

В сучасному світі міждержавні конфлікти набувають не лише збройної форми, а також і інформаційної боротьби за думки та погляди населення країн, світової спільноти.

Протидія гібридній війні з боку української влади полягає у створенні та імплементації багаторівневої і добре структурованої системи прикордонної безпеки; імплементації в рамках скоординованої діяльності українських безпекових структур «системи підтримки прийняття рішень» для супроводження діяльності/активності всередині України; розробці превентивних стратегій, що спрямовані на залучення, на додаток до існуючих оборонних систем і методів, невійськових факторів і чинників.

РОЗДІЛ 2.
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНОЇ ЕКСПАНСІЇ РОСІЇ ЩОДО УКРАЇНИ

2.1. Інформаційна агресія як засіб модифікації суспільної свідомості

Якщо зробити короткий історичний екскурс, то можна згадати, що недружні дії Росії стосовно України були зафіксовані ще восени 2003 року біля острова Коса Тузла в Азовському морі. З 2005 року, після Помаранчевої революції, російські офіційні особи постійно нагадували Заходу, що Україна є failed state (країна, що не відбулася). Газові війни 2006 й 2009 років, покликані продемонструвати ненадійність України як газового транзитера, також можна назвати елементами гібридної війни Росії проти нашої країни. Помітний фактор «третьої сили» під час Євромайдану, збройне захоплення Криму й дестабілізація ситуації на Донбасі — це продовження, а не початок гібридної війни Росії проти України [57, с.346].

Одним із завдань Росії, на думку автора, було ліквідувати конкурента на пострадянському просторі, а також тим самим деморалізувати низку країн в Центральній та Східній Європі.

Головний фронт гібридної війни – інформаційний, який наш сусід використовував для реалізації трьох взаємопов'язаних завдань: створення сприятливого фону та репутації своїх дій, дезінформація українських громадян та створення гарного іміджу на Заході.

Починаючи з 2013 року дослідники активно звертали увагу політиків та політологів, соціологів та державних діячів щодо необхідності забезпечення інформаційної безпеки та ефективного інформаційного протистояння України з можливими супротивниками за низкою напрямків, які страждали від структурних та організаційних залишків радянської системи [58,с.1].

Фактично жодна гілка влади не сприймала цей вид безпеки як важливий та необхідний і тому ніяких рішень не приймалось як на рівні Верховної Ради,

так і інших гілок влади [21, с.221]. Нажаль навіть інформаційна функція власної держави ігнорувалась, адже відкидався самостійний пріоритетний напрям державної інформаційної політики як проект, який мав здійснюватись за допомогою інформаційних засобів для забезпечення інформаційного суверенітету в межах країни.

Початком реалізації гібридної війни, на думку автора, можна вважати поширення серед громадян Півдня України інформації про віртуальне південно-східне утворення «Новоросія» [20, с.109]. Нажаль людська свідомість частіше всього формується саме завдяки таким явищам як: чутки, міфи, думки оточуючої більшості, фрази авторитетної певної особи тощо, які без перешкод розповсюджуються завдяки засобам масової комунікації. Тому люди часто не помічають маніпулятивного впливу. Засоби масової інформації поширювали в різноманітних ток-шоу пояснення про історичну обумовленість та генетичну необхідність розподілу території суверенної країни на окремі частини. Миколаївська та Херсонська області разом з Одесою та частиною Одеської області ніби не могли існувати в майбутньому без єднання з Кримом, який був відірваний від України. Синхронно в засобах масової інформації тенденційно одноманітно висвітлювались події Євромайдану, як прояв неофашистської узурпації влади законно обраного Президента та інших гілок влади [20, с.110]. Несподівано для всіх незалежні засоби масової інформації Російської Федерації продемонстрували свою одностайність та тотожність аргументів та кореспондентських кліше які застосовувались при висвітленні українських подій новітньої історії щодо прагнення євроінтеграції [24, с.111]. Були створені та поширювались, в тому числі на південноукраїнський регіон, такі кореспондентські штампи: «Україна – розділена країна, протести не репрезентують волю народу України», «Схід проти Майдану»; «На Майдані праві радикали – це ледь не фанати самого Гітлера»; «Янукович – легітимно обраний, треба з ним миритися і чекати наступних виборів»; «Не можна робити революцію тільки через непопулярне політичне рішення – відмову від асоціації з ЄС»; «Незрозуміло чого хочуть українці; хто замість Януковича?»; «Конфлікт

в Україні – результат політичної боротьби за владу між «Партією регіонів» та опозицією або ж геополітичної боротьби ЄС і Росії»; «На Майдані намагаються силою захопити владу і не хочуть переговорів; а за кров відповідальність несуть усі сторони» [5, с.95].

Після початку відкритої фази гібридної війни починається нова фаза впливу на свідомість та психіку українських громадян. Новітні технології спричинили більш ефективне використання віртуального простору. Масово створювались сайти “RuTube”, велись чати, блоги та групи у соціальних мережах «Вконтакте», «Одноклассники» та інші в яких активно пропагувались ідеї сепаратизму, збройної боротьби, вчинення акцій непокори органам державної влади й управління України, пропагувались та вихвалялись різні ватажки і учасники проросійських терористичних угруповань тощо. Окремо завжди популяризувались ідеї та інформація антидержавного провокаційного спрямування, чим фактично підривався авторитет і престиж України, існуючі легітимні органи державної влади та місцевого самоврядування, конкретних державних діячів і українських політиків уповноважених виконувати функції держави [11]. Незважаючи на вжиті заходи щодо обмеження впливу провокаційних сайтів та інших віртуальних осередків антиукраїнського впливу на свідомість пересічних користувачів інтернет-ресурсів продовжує існувати низка осередків інформаційних ресурсів змістовне наповнення яких контролюється і координується фахівцями з інформаційних війн та впливів на свідомість зі спеціальних служб та спецпідрозділів розвідувальних органів Російської Федерації («Антимайдан»-Південний Схід», «Республіка Новоросія/Антимайдан», «Антимайдан Донбас Допомога. Загони Самооборони» та ін.) [15, с.140]. Сьогодні також продовжує діяти низка сайтів проросійських сепаратистських угруповань, зокрема: «Центральне інформаційне агентство Новоросії», «Руська весна», «КіберБеркут», «Республіканський інформаційний портал Луганської республіки», «Інформаційний портал Донецької народної республіки» та багато інших. За допомогою зазначених інтернет-ресурсів під гаслами відстоювання загальних

прав та інтересів українського населення південно-східних регіонів України, захисту права на мову російськомовної частини південноукраїнських земель та російську культуру, православ′я здійснюється наукова масова пропаганда сепаратистських ідей, проводиться консолідація екстремістські налаштованих осіб для скоєння нескоординованих терористичних актів на всій території України, навчання основам індивідуального тероризму, навіювання антидержавних ідей [13].

Отже такими прийомами Кремль намагався заполонити українську свідомість своїм «Російським світом» і схилити шальку терезів на свою користь. Виходячи з аналізу, автор констатує запланованість цієї гібридної акції, а не її спонтанність, в якому так намагається переконати міжнародну спільноту російське керівництво.

Таким чином, більшість сучасних дослідників гібридної війни,особливу увагу звертають на інформаційну складову, справа в тому, що попереду збройної агресії («зелені чоловічки», «ввічливі люди» та ін..) просувається інформаційна підготовка населення території, яке планується захопити, та знищуються всі ознаки незаконності такого втручання, як приклад: «народний мер», «народний губернатор», «народна самооборона», «возз'єднання Криму». Окремо підсилюється чуттєва негативна характеристика противника: «бойовики», «каратєлі», «каральна операція», «хунта», «самопроголошена київська влада», «самопроголошений прем'єр» та інше.

Усвідомлення необхідності і непересічної важливості впливу гібридних технологій на свідомість громадян також приходить коли починаємо аналізувати комунікаційну діяльність. Саме комунікаційна діяльність, як складова гібридної війни передбачає масований психологічний вплив через емоційний, а не логічний, розумовий спосіб донесення інформації до громадян [12]. В даному випадку мається на увазі зміщення акцентів і сутності інформаційного повідомлення на форми комунікаційної взаємодії, де основними завданнями є пошук ефективних шляхів такої подачі споживачам, формування потрібних асоціацій і образів у свідомості громадян [18, с. 179].

2.2.Форми застосування, механізми, стилі та сфера реалізації комунікаційних маніпулятивних технологій.

Про надзвичайну важливість роботи із свідомістю громадян України свідчить наявність і активна діяльність на тимчасово окупованих територіях «ДНР» і «ЛНР» підрозділів Головного розвідувального управління та Генерального штабу Російської Федерації. Слід зазначити, що вони активно працюють не лише з громадянами України Південного регіону, а також і мешканцями псевдодержавних утворень для отримання масової підтримки ідей антиукраїнського спрямування етнічними українцями [4, с.36]. Таким чином імітуючи громадянську війну, яка начебто відбувається в Україні, та використовуючи третіх осіб (терористів) задля виконання «брудної роботи» агресор не тільки уникає відповідальності з боку міжнародного права, а й займає нейтралітет, чи зовсім отримує право приймати участь у вирішенні збройного конфлікту на міжнародній арені, який начебто відбувається без його втручання [71, с. 145].

Усвідомлення необхідності і непересічної важливості впливу гібридних технологій на свідомість громадян також приходить коли починаємо аналізувати комунікаційну діяльність. Саме комунікаційна діяльність, як складова гібридної війни передбачає масований психологічний вплив через емоційний, а не логічний, розумовий спосіб донесення інформації до громадян[12]. В даному випадку мається на увазі зміщення акцентів і сутності інформаційного повідомлення на форми комунікаційної взаємодії, де основними завданнями є пошук ефективних шляхів такої подачі споживачам, формування потрібних асоціацій і образів у свідомості громадян [38]. Таким чином інформаційний фронт гібридної війни сьогодні демонструє різноплановість та багатовимірність, а саме: – робота з населенням тимчасово окупованих територій та контрольованих силами АТО; – серед громадян, населення суверенної України, яка переживає гібридну війну на Сході країни, а решта територій знаходиться в стані миру; - вплив на громадян країни-

агресора; - серед членів міжнародного співтовариства як прихильного до України, так і ні [38].

Автор приходить до усвідомлення того, що конфлікти від збройних також перейшли до прихованих форм боротьби за свідомість та відданість громадян в різних зонах розмежування конфліктуючих сторін, різних свідомісних рівнів, різних видів реальності, поширення конфлікту також на світ реальної віртуальності [61, с.64].

Не слід перебільшувати роль та значення інформаційної складової, але і забувати неможна в умовах гібридної війни, супроводжуючи та надаючи особливого колориту військової фази АТО. Фактично сьогодні протилежна сторона зазначає, що маніпулятивні свідомісні технології почали застосовуватись ще з 2006-2007рр [9, с.147]. Перші спроби створення симуляції реальних подій та донесення до громадян за допомогою цілого комплексу інформаційних каналів продемонстрували свою впливовість та важливість, наприклад, «фашисти в Києві», «звірства каральних батальйонів», «розіп′яті хлопчики», порушення міжнародних норм і використання заборонених видів озброєння тощо. Всі ці приклади симуляції спрямовані на те, щоб замінити об′єктивні уявлення цільових груп про характер триваючого конфлікту штучно створеними «інформаційними фантомами», які йдуть на користь агресору [11].

Аналізуючи наведені вище приклади міфологем можна відразу побачити характерну особливість їх побудови – всі вони або частково, або повністю запозичені з шухляд Російської імперії або Радянського Союзу для утримання громадян під впливом загальної ілюзії та штучно створеної єдності. Завдяки інформаційному впливу знищуються ознаки незаконності: «народний мер», «народний губернатор», «народна самооборона», «возз′єднання Криму». Окремо підсилюється чуттєва негативна характеристика противника: «бойовики», «каратєлі», «каральна операція», «хунта», «самопроголошена київська влада», «самопроголошений прем′єр» та інше [11].

Автор також вважає, що під час війни відбулася переоцінка значимості та принципової ролі внутрішньої політичної та економічної ситуації в країні і

необхідність втілення структурних перетворень для виходу зі стану стагнації конфлікту, на чому також наполягає світове співтовариство.

Захоплення Кримського півострову Російською Федерацією супроводжувалось також маніпулятивними гібридними технологіями впливу на свідомість громадян України як на самому півострові, так і решти України, а тому притягує увагу спеціалістів і залишається актуальною темою сьогодні. Нажаль, і по сьогоднішній день так і немає комплексного наукового дослідження цих подій. Вже стало остаточно зрозуміло, що мирне відторгнення частини суверенної країни північним сусідом стало втіленням на практиці гібридної війни. Практично ми стали свідками того, як задовго до прибуття «зелених чоловічків» було розпочато спланову інформаційну війну і обробку населення. Друковані, теле- й радіо медіа здійснювали системне та інтенсивне насичення інформаційного простору дезінформацій ними матеріалами, активну участь приймали також інтернет ресурси. Було створено квазіреальність в якій активну роль зіграли як політичні діячі, так і представники культури і техніки які користувались заслуженим авторитетом. Впливаючи своїми поглядами на пересічних громадян вони схили населення провести та прийняти активну участь в так званому референдумі і включенні Криму і Севастополя до складу Російської Федерації [19].

Було сформовано і імплантовано у суспільну свідомість ідею, що Крим – це територія з «російськими коренями» і обґрунтовано історичними фактами та сюжетами[10, С.23]. Так зазначалось, що завдяки загарбницьким геополітичним крокам імператриці Катерини ІІ територія півострова стала російською в 1783р., в часи коли Російська імперія анексувала Кримське ханство і зокрема був підписаний Маніфест про приєднання Криму до Росії. Згодом півострів перебував у складі РРФСР до 1954р., коли його було передано до складу Української РСР[29].

Слід зазначити також, що територія Криму традиційно була полікультурним регіоном, де мешкало біля 125 націй та народностей [27, С.75]. Це був єдиний регіон з мовленням засобів масової інформації сімома мовами.

На час захоплення на території регіону працювало 79 телерадіоорганізцій, в тому числі 13 телекомпаній ефірного мовлення; 4 приватні проводові радіоредакції, 14 FM-радіостанцій; 5 комунальних радіоредакцій; 39 приватних кабельних телерадіокомпаній та багато інших національних засобів масової інформації[27, с.76].

Головну роль відігравали Держтелерадіокомпанія «Крим» і Чорноморська ТРК[26]. Особливо цікавим було те, що на телеканалі «Крим» виходили в ефір передачі російською, українською, кримськотатарською, грецькою, болгарською, німецькою та вірменською мовами. В друкованих ЗМІ толерантного ставлення до етнічних мов не спостерігалося. Ісакова Т.О. висловила думку про те, що домінування російськомовного медіа продукту було обумовлено історичними чинниками: родинними зв′язками, а також недостатньою кількістю відповідної конкурентної якості кримських ЗМІ. Статистика свідчила, що друковані ЗМІ поділялись таким чином: 72%-російські, 17%-українські, 8%-кримськотатарські і по 1%-англійські, німецькі, грецькі [26].

Внаслідок розташування в Севастополі російської військової бази Чорноморського флоту між Україною та Російською Федерацією виникли тертя щодо закінчення в 2017р. терміну оренди і небажання української сторони продовжувати договір. Інформація в засобах масової інформації з ідеями про те, що НАТО планує взяти в оренду відповідні військові приміщення ще більше загострило міждержавні стосунки [20, С.105]. Після повернення кримських татар на історичну батьківщину українським урядовцям тривалий час не вдавалось зняти напругу в земельних питання, також виникли проблеми в поновленні їхніх економічних, соціальних, політичних прав.

Окремі прояви потенційних проблем почали з′являтись в результаті парламентських виборів 2006р., коли представники Партії регіонів і «Русского блока» робили перші спроби перешкоджати діяльності місцевих засобів масової інформації [21, с.229]. Телебачення ж контролювалось центральною владою і тому репрезентували проєвропейські цінності. На медійному просторі почали

розгортатись ідеологічні війни, здійснювались спроби замінити неугодних власників засобів масової інформації.

Спланованість анексії Криму тепер чітко простежується тими зовнішніми ознаками які почались ще в 2006р. Наприклад, саме в цей час з трибуни Держдуми лунають виступи депутатів К. Затуліна, В. Жириновського з неприкритими закликами здійснити відділення Криму від України за проєвропейську орієнтацію київської влади і неможливості координувати українську зовнішню політику. Наступним яскравим прикладом триваючої ідеологічної обробки населення був виступ в м. Севастополі з нагоди 225-річчя Чорноморського флоту РФ мера м. Москви Ю. Лужкова з пропозицією порушити питання про повернення м. Севастополя Росії За такі сепаратистські заклики Ю. Лужкова було оголошено персоною нон-грата в Україні [26].

Наступним кроком у втіленні маніпулятивних гібридних технологій на свідомість громадян стала активізація так званого козацького руху. Проявами діяльності якого стали постійні сутички 9 козацьких об′єднань на етнополітичному підґрунті з активістами кримськотатарського руху в м. Судак, Бахчисараї, Феодосії, селищі Партеніт [5, с. 97]. Ніби нічого незрозумілого, але почався процес створення невдоволення серед пересічних мешканців і асоціація була як з українським національним рухом, так і з представниками депортованого кримськотатарського етносу.

На території автономії проводяться інформаційно-психологічні кампанії, які дезінформують суспільство, несуть загрозу територіальній єдності країни, стоять на заваді проведенню державної політики у сфері європейської та євроатлантичної інтеграції» [26]. Поміж іншим зверталась також увага на недостатній рівень використання української мови та мов національних меншин представниками кримської журналістики.

Склалась ситуація коли центральна влада України почала повільно і невпинно втрачати контроль над засобами масової інформації Автономної республіки Крим і відповідно над настроями населення півострова, а відповідно і можливість дотримання всіх норм чинного українського законодавства.

Нажаль ми стали свідками відсутності будь-яких адекватних дій з боку української влади на всі випадки агресивних дій та спеціальних інформаційно-психологічних заходів проросійських сил, тотальність та безкарність пропагандистських ЗМІ республіки. Практично відбувався процес психологічної обробки населення в умовах неможливості доведення до людей альтернативних поглядів та позиції центральних органів влади, формування проросійсько налаштованої свідомості. Завдяки здійсненим заходам обробки свідомості людей в 2011р. майже 80% кримчан при проведенні соціологічного опитування заявили бажання возз′єднатись з Російською Федерацією, «за» відродження СРСР-79,5% та 81,0% «за» приєднання до Митного союзу[27, с.82]. Отже можна зазначити, що проведена інформаційно-пропагандистська кампанія із залученням російських спецслужб, застосування широкого спектру дезінформаційних заходів спричинили потужний деструктивний вплив на свідомість громадян України, місцеве населення Криму і суміжних територій, що сприяло формуванню їх позитивного або нейтрального ставлення до акту відторгнення півострова та перетворилося на чинник загрози національній безпеці держави.

2.3.Технології маніпуляції свідомістю громадян застосовані під час анексії Криму

Головною складовою маніпулятивної технології гібридної війни на свідомість громадян Криму стала технологія «інформаційної блокади». Вона була спрямована на формування фактичного інформаційного вакууму в українських засобах масової інформації в АРК з метою безальтернативного подання фактів, їх інтерпретація, оцінка, формування ставлення у споживачів, фільтрація змісту донесених фактів про події в Україні та Криму[19]. Завдяки вжитим заходам Росія стала домінувати в інформаційному просторі регіону. Застосовувались не лише демократичні шляхи для досягнення поставлених цілей, так, наприклад низка кримських радіокомпаній була позбавлена

можливості приймати участь у конкурсі на отримання права на наземне ефірне мовлення, задіяли також нормативно-правові обмеження до ЗМІ, давались невмотивовані відмови в реєстрації або перереєстрації кримських ЗМІ. Було проведено низку акцій «самооборони», тобто місцевих активістів щодо припинення діяльності проукраїнських ЗМІ. Низка журналістів скаржились на постійне стеження за їх пересуванням, проведенням з ними профілактичних співбесід з боку представників правоохоронних органів, прослуховування розмов тощо. На території півострова були вимкнені українські канали і замінені в свою чергу на російські. В стислі терміни , вже на лютий 2015р. на території півострову не залишилось жодного ЗМІ з проукраїнськими поглядами чи концепцією роботи [82, с.214].

Для ефективного впливу на свідомість громадян було застосовано технологію контекстуального блокування, тобто здійснювався блокувальний контроль інформаційного простору ЗМІ, жорсткий контроль вербальних позначень, наприклад могло використовуватись лише словосполучення «повернення Криму», замість приєднання, чи анексія. Завдяки чому із свідомості прибирався агресивний характер, здійснювався контроль візуальної картинки – на екранах телевізорів були відсутні зображення невдоволених анексією Криму місцевих мешканців; здійснювався тотальний контроль одноманітності інтерпретації подій, що фактично і є цензурою, коли просто не допускається альтернативне висвітлення чи інтерпретація події [67, с.70].

Наступний прийом – «використання медіаторів» - тобто демонстрація носіїв певної думки, підходу, оцінки. В якості медіаторів використовувались для різних аудиторій різні авторитети, неформальні лідери, політичні діячі, представники різних релігійних конфесій, діячі науки, культури, мистецтва, військові, спортсмени тощо. Було завезено масу таких людей під різними приводами до півострову для обслуговування різних заходів. Психологія це називає «фіксацією на авторитети», наприклад застосовувались такі словосполучення: «Лукашенко считает Крым частью России», «Лидер французского Национального фронта Марин Ле Пен заявила, что признаёт

референдум, состоявшийся в Крыму, вполне законным» ті ін. приклади [13, С.104].

Певного поширення набула технологія «ефект ореолу», тобто здійснювалось відвідування російських авторитетних діячів спорту, культури, політики до Криму, що сприяло підвищенню статусу зусиль РФ в напрямку повернення Криму і «легалізації» «референдуму» кримчан. Типовим було відвідування 26 лютого 2014р. півострову російськими діячами І.Родніна, М.Валуєв, В.Терешкова, С.Миронов, 14 березня 2014р. в Сімферополі був хокеїст В.Фетісов, борець О.Карелін та ін. [21, с.220].

Високу ефективність продемонструвала технологія «анонімного авторитету», яка передбачає цитування документів, оцінок експертів, свідків звітів та інших матеріалів, при цьому уникалось згадування імені джерела повідомлення, наприклад: «Турчинов признал полный провал так называемой антитеррористической операции…. Об этом на условиях анонимности журналистам рассказал источник в украинском Генштабе» [26, 27].

Слід окремо зазначити одну з характерних рис російських ЗМІ – оперативність, майже миттєва реакція на події та онлайн висвітлення процессу. Діючи на випередження завдяки сучасним технологіям та обладнанню «ефект першості» та «упереджувального удару». Вони успішно першими доносили потрібну інформацію до споживачів і формували бажане уявлення про події. Існує думка, що пропагандист приречений на успіх, якщо інформація досягла аудиторії раніше, ніж інформація його супротивників, конкурентів. В даному випадку повинен спрацювати ефект сприйняття: при надходженні суперечливої інформації(яку неможливо перевірити)- люди схильні віддавати перевагу тій, що надійшла першою. Змінити ж вже сформовану думку дуже важко і малоефективно.

Активно і ефективно використовувався маніпулятивний прийом «переписування історії» [15, с.136]. Досвід свідчить, що цей прийом демонструє ефективність у довготривалій перспективі, в ситуації коли потрібно поступово, повільно сформувати у населення необхідний світогляд. У громадян

формується ілюзорний світ, надумана реальність, яка сприймається як справжня, а штучно створювана картина історичної дійсності гарантувалась сфальсифікованими установками, наприклад: «После развала СССР россияне не переставали считать Крым своим», «Развал СССР превратил фарс в трагедию: сотни тысяч русских жителей полуострова оказались оторваны от своей исторической родины» [14, с.137].

Виявив свою ефективність метод «зворотнього зв′язку» який полягає в створенні відповідної реакції реципієнтів інформації на певні події. Наприклад, ЗМІ РФ достатньо активно повідомляли про штучно інсценовані масові акції на підтримку відторгнення Криму від України: « … народные сходы – в поддержку Украины и соотечественников, живущих в этой стране, начались в России в воскресенье…. В столице также состоялись мото- и автопробег». Також яскравим прикладом втілення цього маніпулятивного методу стали спілкування народу з Президентом В.В.Путіним в режимі он-лайн, що було насправді театральною виставою [13].

Підвидом досліджуваної технології стали «псевдо соціологічні опитування» а також «рейтингування», завдяки яким формувалась громадська думка, а не реально віддзеркалювалась життєва ситуація. Самі питання були сформульовані таким чином, щоб створити у аудиторії «правильний» погляд на досліджувану проблему, наприклад: «… более 90 процентов граждан считают, что Россия должна защищать интересы русских и представителей других национальностей, проживающих в Крыму. При этом около 83% россиян полагают, что Россия «должна это сделать, даже если эта позиция осложнит наши отношения с некоторыми государствами». Такі квазісоцопитування фактично формували ілюзію існування «обуреного російського народу», який усім серцем прагнув повернути Кримський півострів під свій контроль. Російські ЗМІ використовували в цій ситуації такий маніпулятивний інструмент як соціальне схвалення (або несхвалення) [18, с.180].

Ще одна техніка, яка застосовувалась для маніпуляції з свідомістю громадян, цивільного населення – це «констатації факту». Саме в медіа-

повідомленнях домінували приклади впливу на споживачів інформації. Фальсифіковані факти кореспондентами подавались як сюжет про новини, аналіз результатів соціологічних опитувань, завдяки чому у споживачів інформації відразу знижувалась критичність сприйняття навіюваної інформації, наприклад: «Крым – один из самих известных в мире исторических регионов России». [26] Щоб приспати критичність, підняти авторитет наведеної інформації кореспонденти в своїх репортажах намагались посилатись на «лідерів думки», відомих журналістів, політологів, соціологів та інших фахівців.

Значного поширення в роботі ЗМІ набули техніки навіювання як «свідки подій», «ефект присутності», які використовувались в комплексі з технікою «емоційного резонансу». Яскравим прикладом буде репортаж з місця подій в якому кореспондентом спотворюється реальність і демонструються змонтовані відповідним чином сюжети реконструйовані на підставі опитування випадкових людей, на підставі усних свідчень яких і здійснювалась відеореконструкція змісту та підводився емоційний ряд. На споживачів такої інформації надзвичайно великий вплив здійснювали коментарі «простого» населення: двірники, сантехніки, військовослужбовці, продавці, водії та ін.. Для підсилення впливу, емоційності репортаж перенасичували конкретними подробицями, які легко запам′ятовуються і «всмоктуються» у свідомість більшості населення[49].

Наприклад, коли журналіст Д.Кісельов працював на російських телекомпаніях він за допомогою інтонацій коментував діяльність українських політиків, службовців і у глядача тим самим свідомо викликав обурення, незважаючи на зміст інформації. Коли ж аналізував позицію В.В.Путіна у кримському питанні, то у його голосі відчувалась впевненість та віра у правильність, неминучість, успішність перспектив російської нації [0, с.105].

Для значного впливу на свідомість громадян ЗМІ також використовували техніку «психологічного шоку», яка втілювалась в демонстрації «насильницьких» дій кримських татар проти проросійських громадян в Криму і

тим самим свідомо налаштовували російськомовних мешканців Криму проти кримськотатарської меншини. Слід також зазначити, що агресивна пропагандистська компанія з загострення анти ісламських настроїв в Криму активно втілювалась і щодо Духовного управління мусульман Криму(ДУМК) і Меджлісу кримськотатарського народу з метою повної або часткової дискредитації місцевих мусульманських громад, а також здійснення ротації лідерів мусульманства на керованих проросійськи налаштованих. Системно ЗМІ намагались дестабілізувати ситуацію нагнітанням анти ісламських настроїв звинувачуючи ДУМК, Меджліс кримськотатарського народу та решти релігійних організацій кримських татар звинувачуючи в фінансових та ідеологічних зв′язках з «радикальними ісламістськими організаціями» [6].

Здійснювалось також маніпулювання свідомістю громадян за допомогою техніки «сенсаційності», тобто підвищення рівня нервозності і підрив психологічного захисту громадян Криму. Спираючись на принцип, що відчуття безперервної кризи значно підвищує сугестивність людей і знижує здатність до реального критичного сприйняття, фактично всі новинні блоги в російськомовних ЗМІ щодо України мали саме сенсаційне забарвлення: «Ситуация в Крыму продолжает накаляться», «Последняя экономическая надежда Крыма рухнула», «Крым оставили без правительства», «А ведь кризис только нарастает» та ін. [24, с.110].

Постійно використовувалася технологія «коментування» подій, що створювало необхідний контекст для сприйняття інформації в цілому. Такі репортажі супроводжувались власною інтерпретацією матеріалу коментатором, який пропонував споживачу «розумний! Варіант пояснення. Завдяки прийому «обід з флангу» створювалось враження об′єктивності матеріалу і неупередженості через включення в тексти пропагандистських матеріалів фактів, які на перший погляд були неприйнятні для місцевої аудиторії: «Меня впечатлило, что там (Симферополь) ездят автомобили, на которых водители сами клеят наклейки «Я за Таможенный союз». Особенно приятно, что это не какие-то активисты, а простые граждане, которые ориентированы на

интеграцию с Россией» [8, с.97]. В даному прикладі розрахунок робився на поступове, повільне, еволюційне залучення до орбіти ідеологічних і політичних поглядів, що виявляється ефективним в роботі з людьми які ще не визначились з політичними орієнтирами.

Техніка «перспективи» втілювалась в тому, що ЗМІ подавали коментарі тільки однієї сторони конфлікту, таким чином створювалась однобічна перспектива, наприклад в процесі анексії Криму всі інформаційні повідомлення щодо української сторони мали виключно негативний контекст, а росіяни та «зелені чоловічки» висвітлювались виключно з позитивного боку.

Застосовувався також прийом «відволікання уваги», що реалізовувався комбінуванням різнопланової інформації. Це реалізовувалось таким чином, що пропагандистські сюжети перемішувались з розважальними передачами для домогосподарок, а в радіопрограмах для таксистів поруч з періодичною рекламою вплітались інформаційні повідомлення в стислій і доступній формі.

Ефективно і системно застосовувалась техніка «зміщення акцентів», «створення проблем», «створення загрози» які створювали високий рівень значущості вигаданих проблем для населення, оскільки, як правило, найбільш актуальними люди вважають саме ті проблеми, які найдокладніше висвітлюються в засобах масової інформації. Штучно актуалізувалась проблема «фашистської загрози» щоб деморалізувати населення і викликати масовий страх з метою формування сприятливої атмосфери для подальшої маніпуляції масовою свідомістю населення. Створюючи тематичне домінування в інформаційному просторі ЗМІ нав′язували відповідне бачення ситуації, а реальні проблеми населення залишались поза увагою[27, с.137].

Свою ефективність продемонструвало постійне «повторення» одних і тих самих тверджень, що стало поступово сприйматись населенням як єдине вірне. В даному випадку інформаційний вплив спрямовувся не на ідеологічні установки, а на буденну свідомість громадян: «бандерівщина», «экстремисты», «радикалы», «провокации неофашистов в Киеве», «антиконституционный переворот», «правоэкстремистская организация «Правый сектор» [27, с.216].

До решти технологій залучалась також і «підміна», що передбачає використання позитивних визначень (евфемізмів) для позначення негативних дій і навпаки. Зазначений метод застосовувався для створення сприятливого іміджу акту анексії українських територій. В реальності об′єктивна ситуація приховувалась за тезами «напівправди», наприклад: «.…на региональный референдум в Конституции запрета нет. Тогда почему бы и не провести в Крыму референдум» [26-27]. Застосування прийому «хибної аналогії», що ґрунтується на схильності людей мислити аналогіями, будувати так звані псевдо логічні послідовності також давало свої результати.

Використовуючи «принцип контрасту» журналістам вдалося натякнути на «несхожість» Криму і решти України: «Мирный Крым стабилен, многонационален, в котором все люди живут нормально. Если Украина не будет выступать угнетателем русских, как на сегодняшний день, и не будет вносить дурацкие русофобские законы, то у нас будет все нормально, все спокойно». Завдяки таким висловлюванням у споживача інформації виникала єдина відповідь – терміново треба приєднуватись до Російської Федерації. Застосування систематичного повторення однакових визначень та фраз стало втіленням техніки «класифікації» [28, с.94].

Саме застосування класифікаторів, які описують об′єкти чи події, сформульована інформація форматується таким чином, щоб одержувач повідомлення несвідомо сприймав нав′язане йому визначення ситуації. По-перше, це були слова і поєднання, що описують власну «позитивну і конструктивну позицію»: «восстановление мира и стабильности», «наши русскоязычные братья», «великий славянский народ». По-друге, це формулювались «контрастуючі слова», що мають на меті охарактеризувати супротивника в негативному ключі: «фашистский переворот», «бандеровское государство», «украинские политики-эстремисты», «украинские националисты» [12].

Навіть у виступах Путіна В.В. простежується застосування низки технологій пропаганди, як емоційного резонансу, класифікації, створення

загрози, хибної аналогії, констатації факту, рейтингування, відволікання уваги та інші [27, с. 76].

Останні події ж зі збиттям українських кораблів російськими під час виходу з Керченської протоки додали ще більше гостроти і розвитку конфлікту, що спонукало розгляд запровадження військового стану. Тому треба констатувати, що мир навряд чи можливий у найближчій перспективі за такого розвитку подій.

Висновки до 2 розділу

Таким чином, аналізу реальної інформаційної ситуації в Україні на території АРК протягом 2013-2022 рр., засвідчує актуальність дослідження важливої комунікаційної складової гібридної війни. Наразі військова агресія та анексія Криму спричинили не лише людські, матеріальні, а й морально-психологічні втрати для України. На думку автора для подолання поразок, прорахунків та недоліків слід створити адекватну програму дій у відповідь на інформаційні дії агресора і намагатися протидіяти не тільки у військову контексті, а й інформаційному, притому, поєднуючи їхні методики та засоби.

Сьогодні Україна протистоїть агресору в особі РФ, який впровадив хаос в усю конструкцію післявоєнної побудови Європи. Агресор використовує новий формат ведення війни, сподіваючись уникнути відповідальності за життя людей, зруйновані оселі та промисловість країни, яка не бажає йти у фарватері політики РФ. Дипломатична, консультаційна та фінансова допомога з боку наших партнерів та санкції проти РФ є значним фактором впливу, але необхідно застосування ще більш потужних заходів впливу на РФ та надання Україні більших спроможностей для оборони своєї землі.

Військова повномасштабна агресія Росії впродовж 2022 р. розкрили очевидну неспроможність державних структур протидіяти на інформаційні виклики. Цілеспрямована інформаційна експансія РФ спрямована проти української державності частково мала успіх, але враховуючи сучасні реалії

можна констатувати, що Україна почала активно протистояти інформаційній агресії. Російська державна інформаційна концепція, використовуючи потенціал ЗМК, поширює ідеї концепції «руського миру», недостовірну інформацію, чутки, «фейки», компрометувальні фото- і відеоматеріали, тим самим втручається в зону інформаційної безпеки України. Основними універсальними конструктами російських ЗМК є: маніпулювання суспільною свідомістю: стратегія формування «образу ворога»; стратегія формування символів, смислів, конструктів та образів; стратегія формування історичної спадщини та інші.

Суспільна практика свідчить, що застосування вищезазначених стратегій, в умовах воєнного стану надають переваги країні-агресору та створюють додаткові труднощі під час проведення військових дій.

Державницьким та громадським органам, структурам слід оперативно реагувати та протидіяти російським маніпулятивним технологіям ЗМІ.

РОЗДІЛ 3.
ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОЇ АГРЕСІЇ РОСІЇ ЩОДО УКРАЇНИ

3.1. Визначення пріоритетів інформаційної державної політики в Україні

Визначення пріоритетів інформаційної державної політики в Україні обумовлено зростанням рівня невизначеності та мінливості зовнішнього та внутрішнього середовища в цій сфері. У той же час умови прогресивного й усталеного розвитку України вимагають підвищення ефективності, обґрунтованості та прогнозованості саме на довгострокову перспективу державної політики забезпечення інформаційної безпеки. Одним із пріоритетних напрямів вирішення цього протиріччя є підвищення рівня захисту інформаційного простору.

Стратегічний моніторинг і аналіз є одними з головних інструментів, що спрямовані на подолання даної невизначеності. Основними цілями цих процедур є оцінка рівня традиційних, виявлення пріоритетів та загроз національним інтересам, тенденцій їхніх змін, науково обґрунтований опис стану власних ресурсів і наслідків прийняття стратегічних рішень, а також можливостей Системи забезпечення національної безпеки держави (СЗНБ) не тільки змінювати ситуацію, але й реалізовувати нові напрями розвитку в майбутньому [2, с.12].

Саме тому в інтересах реформ, що відбуваються в секторі безпеки, були розроблені такі стратегічні документи як Енергетична стратегія на період до 2030 року, Стратегія національної безпеки України, Стратегія воєнної безпеки, Концепція та Програма реформування Воєнної організації держави, Національна стратегія розвитку інформаційного суспільства на 2007–2015 роки тощо.

Початкові напрацювання у вітчизняній законодавчій базі інформаційної політики та безпеки мали досить фрагментарний та декларативний характер і даний час не відповідають викликам часу. З 2014 року законодавча база України у сфері інформаційної безпеки відчутно збагатилася. Загалом її можна поділити на 2 групи. Перша включає концептуальні, базові документи, такі як Доктрини та Стратегії, які визначають основні загрози та тенденції в інформаційній безпеці. Друга група містить Закони України, Укази Президента, рішення РНБО України, які забороняють контент країни агресора на радіо, телебаченні та в Інтернет просторі України.

З початком російської військової агресії проти України, у якій інформаційний супровід почав відігравати ключову роль, розпочалася трансформація національного інформаційного законодавства. Стартовим нормативно-правовим актом у цьому напрямку стало рішення РНБО «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року, введене в дію Указом в. о.Президента України від 1 травня 2014 року № 449/2014. Поворотним твердженням документу стало: «Розглянувши стан забезпечення інформаційної безпеки, Рада національної безпеки і оборони України зазначає, що останнім часом Російська Федерація поширює недостовірну, неповну, упереджену інформацію про Україну, через що намагається маніпулювати суспільною свідомістю в Україні та за її межами» [49,50].

Потрібно відмітити те, що відсутність злагодженої та системної інформаційної політики в нашій державі призвели до того, що сьогодні Україна змушена вести оборонну інформаційну кампанію аби протидіяти інформаційним викликам та загрозам із боку Росії. Про це, зокрема, вказується і в Стратегії національної безпеки України, де визначено, що актуальними загрозами національній безпеці України є агресивні дії Росії, в тому числі інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини

світу [70]. У п. 3.6. вказаного документу визначені основні загрози інформаційній безпеці, а саме: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства [70]. Крім вищевказаної Стратегії, Президент України своїм указом № 47/2017 від 25 лютого 2017 року затвердив Доктрину інформаційної безпеки України [22].

Значна увага інформаційній складовій у Доктрині приділена у ст. 32. Як основу кризового реагування на воєнні загрози та недопущення ескалації воєнних конфліктів Україна розглядає такі основні заходи і дії: − взаємоузгоджене використання політико-дипломатичних, інформаційних та силових інструментів держави для протидії деструктивному тиску агресора на Україну та примушення його до дотримання норм міжнародного права та власних зобов'язань; − посилення розвідувальної діяльності в інтересах підготовки та проведення Україною стратегічних комунікацій, контрпропагандистських заходів та інформаційно-психологічних операцій; − підвищення ефективності спеціальних інформаційних заходів впливу в районі проведення антитерористичної операції в Донецькій та Луганській областях і на тимчасово окупованій території та зосередження сил і засобів для організації ефективної протидії проведенню ворожих інформаційно-психологічних операцій проти України [22].

6 травня 2015 року РНБО схвалила проект нової Стратегії національної безпеки, яка розрахована до 2020 року [70]. Цей стратегічний документ передбачає забезпечення національної безпеки, окрім іншого, у сфері інформаційних ресурсів, критичної інфраструктури та кібербезпеки. Стратегія серед основних актуальних загроз національній безпеці України чітко визначає розвідувально-підривну і диверсійну діяльність, дії, спрямовані на розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі і ненависті, сепаратизму і тероризму, створення і всебічну підтримку, зокрема військову, маріонеткових квазідержавних утворень на тимчасово окупованій території частини Донецької та Луганської областей; інформаційно-психологічну війна,

приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу та ін.

Окремими загрозами інформаційній кбербезпеці, а також інформаційним ресурсам Стратегія визначає:

− ведення інформаційної війни проти України; − відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства;

− уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;

− фізичну і моральну застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Важливим є те, що у документі прописані пріоритети забезпечення інформаційної безпеки. Мова йде про:

− забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;

− створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; − протидію інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;

− розробку і реалізацію скоординованої інформаційної політики органів державної влади; − виявлення суб’єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; − створення і розвиток інститутів, що відповідають за інформаційнопсихологічну безпеку, з урахуванням практики держав-членів НАТО;

− удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу. Пріоритетами забезпечення

кібербезпеки і безпеки інформаційних ресурсів Стратегія визначає:

− розвиток інформаційної інфраструктури держави;

− створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);

− моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;

− розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

− забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;

− реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС;

− створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;

− розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО [70].

Отже, сьогодні вкрай необхідно напрацювати рекомендації щодо вирішення вказаних проблем. Саме тому необхідно об'єднати зусилля законодавців, правоохоронних органів, вчених і практиків, ЗМІ, громадськості та направити їх не тільки на обмеження застосування маніпулятивних механізмів впливу на масову свідомість і поведінку, а й на усунення самих передумов такого способу впливу.

З огляду на складну політичну ситуацію в Україні та інформаційні впливи з боку Російської Федерації, з 2014 року було утворено ряд інституцій покликах стояти на захисті інтересів та безпеки нашої держави. Так 14 січня 2015 року Кабінет Міністрів України ухвалив постанову «Питання діяльності Міністерства інформаційної політики України» (МІП) [42], відповідно до якої

затверджено відповідне Положення про створення Міністерства інформаційної політики України. Вперше за історію незалежної України, була створена окрема урядова установа, основною метою якої стало формування інформаційної політики України та відбиття інформаційних нападів проти нашої держави. Положення про МІП було публічно обговорено з народними депутатами України, громадськими організаціями, професійними об'єднаннями. Зокрема, свої пропозиції надали: Комітет з питань свободи слова та інформаційної політики ВРУ, Комітет з питань безпеки і оборони ВРУ, медіа-юристи. Документ з урахуванням їхніх зауважень було подано на розгляд Кабінету Міністрів України. Положення пройшло погодження в Держкомтелерадіо України, Міністерстві фінансів, Міністерстві економіки та Міністерстві юстиції. Згідно з Положенням, МІП є головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема, з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів. У своїй діяльності Міністерство інформаційної політики України базується виключно на принципах захисту свободи слова та думки, захисту прав громадян на вираження своєї позиції. При МІП створено Громадську раду, до якої увійшли представники громадських організацій, ЗМІ та медіа-експерти. Вона виконуватиме функції нагляду за діяльністю Міністерства. Ключові завдання МІП затверджено в Програмі дій Уряду, а також викладено у Коаліційній угоді, підписаній п'ятьма парламентськими фракціями Верховної Ради України. Такими завданнями є: − розробка стратегії інформаційної політики України та концепції інформаційної безпеки держави; − координація органів влади в питаннях комунікації та поширення інформації; − протидія інформаційній агресії з боку Росії. [70].

Надважливим і конструктивним кроком МІП стало ініціювання у 2015 році інтернет-проекту «Інформаційні війська України». Сама ідея інформаційної оборони країни зародилася у волонтерів а згодом перетворилася на проект при МІП. Метою проекту було мобілізувати користувачів соціальних

мереж України для відстежування і спростування фейкових новин та неправдивої інформації у боротьбі з російською пропагандою. Особливістю проекту стало те, що до нього мав змогу долучитися кожен бажаючий, котрий хотів зробити свій внесок в інформаційну боротьбу України. Аби вступити до лав інформаційних військ, необхідно зареєструватись на сайті. Після реєстрації треба ретельно виконувати отримані завдання і щодня приділяти час інформаційній боротьбі [70]. «Інформаційні війська України» є інноваційним інститутом у протистоянні російській інформаційній війні. З 1 серпня 2017 року проект почав функціонувати як самостійний [42]. Разом з тим, створення Міністерства призвело до його осуду з боку деяких журналістів та громадськості. Наприклад, Незалежна медіа-профспілка України (НМПУ) виказала занепокоєння тим фактом, що «нове міністерство інформації було створено без консультацій з масовими журналістськими організаціями, без врахування точки зору журналістів і медіа-експертів» [43]. У щорічному звіті організації НМПУ про стан свободи ЗМІ у світі робиться висновок, що «створення Міністерства інформаційної політики показує, що уряд піддається спокусі використовувати контроль над ЗМІ у відповідь на виклики, пов'язані з безпекою» [45]. Серед деяких вітчизняних політичних експертів, журналістів, політиків існували та й досі існують думки, що це Міністерство є загрозою демократичним цінностям, свободі слова. Також не схвалили таку ініціативу Міжнародна Федерація журналістів та Європейська федерація журналістів запропонувавши ліквідувати цю установу. Генеральний секретар міжнародної правозахисної організації «Репортери без кордонів» відзначив: «У демократичному суспільстві, регулювання засобів масової інформації є обов’язком самих ЗМІ, або, можливо, незалежного органу, але у жодному разі це не є функцією виконавчої влади. Створення Міністерства інформації є гіршою відповіддю на серйозні проблеми для української влади» [41].

Таким чином, вкрай необхідним завданням як для органів влади, так і для недержавних інституцій, наукових і освітніх закладів є розробка та впровадження відповідних документів щодо реалізації пріоритетів

інформаційної державної політики в Україні за такими напрямками:

1) умовах гібридної війни вже безсумнівним є факт, що інформаційний простір сьогодні є театром ведення військових дій та інструментом проведення національної політики, тому надзвичайно важливими є питаннями інформаційної безпеки та впровадженням новітніх інформаційних технологій;

2) важливими питаннями як на загальнодержавному, так і на місцевому рівні є питання іміджу держави та офіційної комунікації. Задля цього необхідно розвивати такі напрямки, як: культурна та цифрова дипломатія, популяризація національної культури та ідентичності, механізми електронного врядування, взаємодія органів державної влади зі ЗМІ, залучення громадських інституцій до прийняття рішень тощо;

3) враховуючи важливість інтересів інформаційної безпеки, слід відзначити, що в Доктрині також окреслені гуманітарні пріоритети в інформаційній сфері.. Також важливим є питання щодо медіа-грамотності та інформаційної культури населення. Розвитку цих напрямків повинна приділятися належна увага, і провідна роль в цьому належить не лише владним інституціям, а і науковцям, юристам-практикам, а також організаціям громадянського суспільства.

4) необхідність постійного аналізу і стратегічного планування з усього комплексу питань безпеки припускає існування при Президентові України спеціального дорадчого органу – Ради національної безпеки і оборони України, при цьому, необхідно виділити серед широкого спектру завдань Ради національної безпеки України ті, які повинні вирішуватися безпосередньо на користь політичній безпеці: виявлення внутрішніх і зовнішніх загроз об’єктам безпеки; розробка основних напрямів стратегії забезпечення безпеки і організація підготовки державних програм з її забезпечення; підготовка оперативних рішень із запобігання надзвичайних ситуацій, які можуть спричинити істотні соціально-політичні наслідки; розробка пропозицій для координації діяльності органів виконавчої влади в процесі реалізації ухвалених рішень в області забезпечення інформаційної безпеки, а також оцінка їх

ефективності; вдосконалення системи забезпечення інформаційнобезпеки шляхом розробки пропозицій щодо реформування існуючих або створення нових органів.

Отже, сьогодні існує розуміння на рівні керівництва держави запроваджувати в Україні комплексну, системну та дієву інформаційну політику задля сприяння протидії інформаційним викликам з боку Росії та розвитку інформаційного суспільства. При цьому слід зазначити, що для більш досконалого процесу вироблення і реалізації такої політики необхідно використовувати весь наявний арсенал керівних документів державної інформаційно-правової політики та в перспективі вибудувати цілісну систему документів як стратегічного, так і тактичного характеру в інформаційній сфері.

Таким чином, слід визнати, що Україна, її державні органи влади, громадянське суспільство та ЗМІ не були готові до такої масованої військової та інформаційної агресії, що в експертному середовищі отримала назву російсько-українська гібридна війна. Саме тому першочерговим завданням усіх державних, громадських, наукових, експертних, журналістських інституцій є розробка термінових ефективних заходів щодо нейтралізації інформаційної – диверсійної діяльності Російської Федерації проти України та протидії її подальшому розгортанню. Крім того, виклики, що постали перед Україною, потребують вжиття негайних заходів щодо розробки нової Доктрини національної безпеки України, модернізації всієї системи інформаційної безпеки держави.

3.2. Вдосконалення механізмів протидії російській інформаційній експансій: зарубіжний досвід та вітчизняна практика

Важливим напрямом протидії інформаційній війні з Росією, поряд з організаційними заходами, є безпосередні практичні дії української влади і суспільства у вимірі захисту інформаційної сфери нашої держави. Специфічні умови воєнного часу, в яких перебуває на сьогодні Україна, посилили увагу

державних органів і громадянського суспільства як і до зарубіжного досвіду.

Керівництву країни необхідно зважено підійти до раціонального використання наявних інформаційних ресурсів з метою політичного, соціального, економічного, духовного розвитку на користь особи, суспільства і держави. Важливу роль для інформаційної безпеки грає найбільш сприятливе, оптимальне функціонування системи її забезпечення.

Нині стає очевидним, що багатьом сучасним війнам передують війни інформаційні. Україна, нажаль, не стала винятком зазначеного ходу подій, перетворившись на об'єкт політичних маніпулювань з боку РФ за допомогою інформації**.**

Тому надзвичайно актуальним є питанням дослідження інформаційної політики та інформаційної безпеки країни Європи та США. Підходи до забезпечення інформаційної безпеки, прийняті у країнах Східної Європи, наразі не є уніфікованими, що зумовлено геополітичною специфікою відповідних країн, одні з яких входять до Північноатлантичного Альянсу (НАТО) та Європейського Союзу (ЄС), інші – прямують до членства у вказаних організаціях, а деякі – входять до євразійських міждержавних утворень. Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері [1, с. 18].

У Польщі – державі, яка є членом ЄС та НАТО, у 2017 році було утворено неурядову організацію, яка займається питаннями виявлення та протидії російській пропаганді – фундація Центр аналізу пропаганди та дезінформації. Ця структура є першою такого роду інституцією у Польщі, діяльність якої спрямована на системний аналіз та ідентифікацію загроз інформаційного характеру у польському інформаційному просторі. Також у Міністерстві закордонних справ Польщі є команда експертів, які здійснюють боротьбу з історичними дезінформаціями з боку РФ[45].

Втім, не менш важливим є і досвід інших країн Східної Європи, які проходять аналогічний шлях у процесі становлення та розвитку

інформаційного суспільства З точки зору забезпечення інформаційної безпеки у Східній Європі доцільно буде визначити репрезентативними країни різних геостратегічних спрямувань, тому в рамках роботи, потрібно зосередитись на огляді питань забезпечення інформаційної безпеки у Румунії, Болгарії. Передусім зауважимо, що Румунія та Болгарія є членами Північноатлантичного Альянсу та Європейського Союзу. Відповідно, на них поширюються стандарти цих міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки. Це, зокрема, стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002) «Безпека в організації Північноатлантичного договору (НАТО)» [101], офіційна політика НАТО у сфері кіберзахисту [102], стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту [103] й уточнена за результатами Варшавського саміту [103] тощо. Також Румунія та Болгарія, як країни-члени ЄС, втілюють у національній політиці забезпечення інформаційної безпеки стандарти ЄС, в тому числі передбачені «Європейськими критеріями безпеки інформаційних технологій» (1991 р.) [95], «Єдиними критеріями безпеки інформаційних технологій» (1996 р.) [95], документом «Мережева та інформаційна безпека: європейський політичний підхід» (2001 р.) [96], документом «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» (2007 р.) [99] тощо.

Відповідно, основними напрямами забезпечення інформаційної безпеки у вказаних країнах є: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; зміцнення інформаційної безпеки на державному рівні шляхом впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних он-лайн послуг тощо;

розвиток міжнародного співробітництва з питань інформаційної безпеки. Основними викликами інформаційній безпеці Румунії та Болгарії, як країн ЄС, є некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів; відсутність на європейському рівні партнерства між державним та приватним секторами; обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем; відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури [12].

Відповідно до п. 4.7.1 Національної стратегії, провідну роль у забезпеченні кіберзахисту країни відіграє Міністерство оборони Болгарії. Ефективне забезпечення кібербезпеки при цьому передбачає розбудову існуючих та створення нових розширених можливостей для кіберзахисту, сумісних з вимогами НАТО і ЄС, а також проведення адекватних структурних і організаційних реформ, зокрема: розробку політики у сфері забезпечення кібербезпеки, розробку відповідної концепції й методичних документів, що передбачають захист національної безпеки шляхом активної протидії кібер- і гібридним загрозам у кіберпросторі; реалізацію інвестиційних проектів для кіберзахисту у рамках спільних ініціатив, у тому числі ініціативи НАТО/ЄС «Smart Defense» та «об'єднання й спільного використання», а також створення можливостей для кібероборони в рамках загального процесу планування у сфері оборони; створення Оперативного центру кіберзахисту відповідно до плану розвитку Збройних сил Болгарії до 2020 року за допомогою центру NCIRC НАТО із забезпеченням безперервного моніторингу і повної оперативної інтеграції в національну мережу NKOMKS, розвиток колективного потенціалу реагування на кібер- і гібридні загрози на національному й міжнародному рівні; погоджений обмін інформацією про кіберінциденти за допомогою державних установ, НАТО і ЄС, а також співробітництво з

діловими й науковими колами; накопичення досвіду у сфері кіберзахисту й підвищення професійної підготовки персоналу шляхом періодичної підготовки й участі в навчаннях, розширення участі у роботі центру кіберзахисту НАТО та інших партнерських центрів; удосконалювання й розвиток взаємодії із промисловістю й науково-дослідними організаціями на основі «кластерної кібероборони»; активну участь у міжнародних програмах НАТО і ЄС у рамках науково-дослідних проектів; адаптація й впровадження моделі ES75 щодо спільного використання ресурсів на національному рівні для професіоналів, інші форми залучення експертів з кіберпромисловості та наукових кіл. Пункт 7.3 Стратегії передбачає створення механізмів і технічних ресурсів для постійного моніторингу можливих загроз кібербезпеці з точки зору масштабів, джерел і природи (кібер-, гібридні), тенденцій у геополітичному контексті й аналізу національної картини кібербезпеки, а також розвитку здатності застосовувати адекватні форми протидії, в т.ч. підтримувати створення джерел контр-інформаційних впливів [99].

В Румунії на сьогоднішній день активно триває процес розбудови системи кібернетичної безпеки держави як на законодавчому, так і на організаційному рівнях. При цьому ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації, у структурі якої створено національний центр кібербезпеки [105]. Головною функцією цього центру є поєднання систем технічного захисту із можливостями спецслужби з метою отримання інформації, необхідної для попередження, припинення та подолання наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави [99]. Законопроект «Про кібербезпеку», який у грудні 2014 року був схвалений сенатом Румунії, також передбачає створення Національної системи кібернетичної безпеки Румунії, технічну координацію якої покладено на Румунську службу інформації як головного суб’єкта кібербезпеки держави [99]. Національна стратегія забезпечення кібербезпеки Румунії (2013 р.) при цьому передбачає, що Румунія забезпечує

функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційного суспільства, а також забезпечення відповідності основних прав і свобод громадян та інтересів національної безпеки у відповідних правових рамках. Важливим “Інформація і право” № 4(23)/2017 65 для цього є розвиток культури кібербезпеки користувачів комп’ютерів і телекомунікаційних систем, їх поінформованість щодо потенційних ризиків, а також про можливості їх мінімізації. Збільшення поінформованості щодо ризиків і загроз, пов’язаних з діяльністю, здійснюваною в кіберпросторі, а також способів запобігання та протидії їм вимагають ефективної комунікації й співробітництва між всіма учасниками діяльності у цій сфері, тож Румунська держава бере на себе роль координатора заходів, здійснюваних на національному рівні, забезпечуючи кібербезпеку відповідно до визначених під керівництвом ЄС і НАТО підходів [100].

З початку 2017 року офіційно розпочав свою діяльність Центр протидії тероризму та гібридним загрозам при Міністерстві внутрішніх справ Чеської Республіки. Його створенню передували перегляд стратегічних підходів НАТО щодо реагування на нетрадиційні способи ведення війни, а також схвалення Єврокомісією стратегії боротьби з гібридними загрозами та сприяння стійкості ЄС, яка стала доповненням програми розширення співробітництва з Північноатлантичним альянсом. У рамках реалізації стратегії було заплановано створення загальноєвропейського центру для збору та аналізу інформації щодо гібридних загроз. Основною метою діяльності Центру є розвінчування міфів і дезінформації з боку Російської Федерації. Частково цей центр провадить публічну освітню роботу, тобто, має публічні акаунти в соцмережах, де описуються ворожі наративи, приклади дезінформації. Також там є фахівці, які аналізують хто і яким чином, через які вебсайти, через які ЗМІ, через яких людей розповсюджує інформацію. Центр тісно співпрацює зі спецслужбами й іншими правоохоронними органами [45].

Наразі країни Східної Європи вважають вирішення проблеми

забезпечення інформаційної безпеки особи, суспільства, держави, їх захисту від внутрішніх та зовнішніх, у тому числі гібридних загроз, одним з найбільш важливих стратегічних пріоритетів забезпечення національної безпеки. Україна має співпрацювати з іншими країнами Східної Європи у розбудові систем регіональної та міжнародної інформаційної безпеки з метою протидії загрозам стратегічній стабільності, таким, як кібертероризм та кіберзлочинність, орієнтуючись при цьому на стандарти ЄС та НАТО. В цьому контексті для України є важливим досвід країн Східної Європи щодо приведення національного законодавства у відповідність до вимог вказаних міжнародних організацій, передусім – щодо забезпечення балансу між свободою й безпекою в інформаційній сфері на законодавчому рівні.

Для України має стати досвід однієї з країн-лідерів ЄС за показниками розвитку інформаційного суспільства – Фінляндії. В рейтингу країн ЄС Фінляндія займає перше місце за рівнем цифрової грамотності (понад 50% населення), друге місце – за показником поширення мережі широкосмужного зв’язку (34% населення) [95]. Основними державними установами, відповідальними за розробку та реалізацію політики інформаційної безпеки, є Міністерство транспорту та комунікацій та Омбудсмен з питань захисту даних (Data Protection Ombudsman) тощо. Повноваженнями Міністерства транспорту та комунікацій є розробка законодавства щодо комунікаційних мереж, безпеки даних, забезпечення доступу до комунікаційних послуг, а також розробка і реалізація національної політики в сфері інформаційної безпеки. В грудні 2008 року урядом Фінляндії прийнято Національну стратегію інформаційної безпеки на 2009-2015 рр. [94]. В Стратегії визначено п’ять пріоритетних цілей державної політики в сфері інформаційної безпеки: розвиток співробітництва з питань інформаційної безпеки на національному та міжнародному рівнях; підтримання національної конкурентоспроможності та створення сприятливих умов для національних операторів інформаційно-комунікаційних технологій; вдосконалення системи управління ризиками в сфері інформаційної безпеки; забезпечення захисту основоположних прав громадян та інтелектуального

капіталу країни; підвищення громадської обізнаності в сфері інформаційної безпеки. Структурним підрозділом Міністерства транспорту та комунікацій є Управління Фінляндії з регулювання комунікацій (Finnish Communications Regulatory Authority – FICORA), яке уповноважене здійснювати контроль та державне регулювання у сфері інформаційно-комунікаційних технологій [95]. До повноважень FICORA відноситься контроль функціональності електронних комунікаційних мереж, інформування про можливі загрози інформаційній безпеці, підвищення обізнаності громадян з питань інформаційної безпеки, планування і управління використанням радіочастот, мережевими адресами, а також контроль змісту програм і реклами на телебаченні та радіо. В структурі FICORA функціонує CERT-FI (Computer Emergency Response Team of Finland) – фінська комп'ютерна група швидкого реагування, основним завданням якої є попередження, виявлення та реагування на інциденти у сфері інформаційної безпеки, а також поширення інформації про загрози інформаційній безпеці. До компетенції CERT-FI відноситься: проведення моніторингу інцидентів на національному рівні; підтримання обізнаності громадськості про загрози інформаційній безпеці; вироблення рекомендацій для зміцнення інформаційної безпеки; поширення інформації про способи попередження інцидентів, пов'язаних з інформаційною безпекою; надання допомоги у вирішенні проблем у сфері інформаційної безпеки; співробітництво з постачальниками обладнання та програмного забезпечення, з правоохоронними органами; проведення моніторингу і аналізу загроз інформаційній безпеці на міжнародному рівні тощо [88]. Омбудсмен з питань захисту даних (Data Protection Ombudsman) - незалежний орган, уповноважений забезпечити захист права громадян на недоторканість приватного життя шляхом здійснення контролю за обробкою персональних даних та надання консультацій з цих питань. Омбудсмен спільно з FICORA видає спеціалізований журнал «Tietosuoja», що містить інформацію про норми і практику в сфері захисту даних, про безпеку даних в електронних системах комунікації, а також вимоги ЄС щодо рівня захисту даних в країнах-членах [95]. Серед неурядових організацій, які займаються питаннями

інформаційної безпеки, провідна роль належить Фінській федерації комунікацій та телеінформатики (Finnish Federation for Communications and Teleinformatics – FiCom) та Фінській асоціації з питань інформаційної безпеки (Finnish Information Security Association) [95]. Фінська федерація комунікацій та телеінформатики об'єднує компанії, що працюють у сфері інформаційно-комунікаційних технологій. Основна мета діяльності федерації – розвиток бізнес-можливостей своїх членів та підвищення їхньої конкурентоспроможності. Діяльність FiCom включає планування і координацію заходів щодо розвитку інформаційно-комунікаційних технологій, здійснення моніторингу ситуації в ІКТ-секторі, здійснення впливу в сфері регулювання ринку інформаційно-комунікаційних технологій тощо. Фінська асоціація з питань інформаційної безпеки є найбільшою неприбутковою асоціацією Фінляндії в сфері інформаційної безпеки, яка функціонує з 1997 року й об'єднує понад 90 членів. Метою діяльності асоціації є розвиток професіоналізму й обізнаності в сфері інформаційної безпеки. Діяльність асоціації включає організацію дискусій, конференцій, участь у різних програмах з інформаційної безпеки. В країні реалізується низка програм в сфері інформаційної безпеки, що фінансуються урядом Фінляндії. Такими програмами є Фінський проект з Інтернет-обізнаності та безпеки (The Finnish Internet Awareness and Safety project), Проект TrustInet та Інтернет-автобус (Internet Bus) [94]. Фінський проект з Інтернет-обізнаності та безпеки, розрахований на період 2008- 2010 роки, є спільним проектом трьох організацій: «Save the Children Finland», Ліга захисту дітей імені Маннергейма (The Mannerheim League for Child Welfare) та FICORA. Метою проекту є просування безпечного користування мережею Інтернет та боротьба з незаконним контентом. В рамках проекту реалізуються такі заходи, як організація Дня безпечного Інтернету, створення навчальних програм з питань безпеки Інтернет для провайдерів веб-контенту, встановлення «телефону довіри» для користувачів Інтернет для повідомлення про незаконний контент та інші проблеми.

У Фінляндії з 2017 року розпочав роботу Центр по боротьбі з гібридними загрозами. Серед гібридних загроз засновники центру виділяють, серед іншого, поширення неправдивої інформації, атаки проти інформаційних систем, а також інші види атак за допомогою сучасних технологій [45].

В розробці і впровадженні політики інформаційної безпеки чільне місце посідає Естонія. В зазначені країні розробка і впровадження політики інформаційної безпеки належить до компетенції Міністерства економіки та комунікацій, а точніше таких його структурних підрозділів, як Департамент державної інформаційної системи та Естонський центр інформатики [90]. Департамент державної інформаційної системи уповноважений координувати політичну діяльність в сфері інформаційних технологій та розробляти плани в сфері державних адміністративних інформаційних систем, а саме: державні IT-бюджети, законодавство в сфері інформаційних технологій, координація IT-проектів, IT-аудити, стандартизація, міжнародне співробітництво в сфері державних інформаційних систем. Естонський центр інформатики є виконавчим органом у загальній системі координації державної інформаційної політики та розвитку державного сектору інформаційних технологій. Основне завдання Центру – координувати розробку і управління державною інформаційною системою. До компетенції Центру відноситься управління проектами, включаючи підготовку IT-проектів для державних інституцій; проведення моніторингу ситуації з інформаційними технологіями; створення державних реєстрів; розвиток комп'ютерних мереж; вироблення правових засад у сфері інформаційних технологій; здійснення державних закупівель інформаційних технологій тощо. Міністерством економіки та комунікацій Естонії розроблено національну політику інформаційної безпеки. Основна мета політики Естонії в сфері інформаційної безпеки – створення безпечного і відкритого для міжнародної співпраці інформаційного суспільства. Більш конкретними цілями політики інформаційної безпеки є усунення неприйнятних ризиків, захист основних прав людини, забезпечення обізнаності та тренінгів в сфері інформаційної безпеки, участь у міжнародних ініціативах з е-безпеки, а

також підвищення конкурентоспроможності економіки. 8 травня 2008 року урядом Естонії затверджено Стратегію кібербезпеки Естонії на 2008-2013 роки [90]. Стратегічними цілями Естонії у сфері кібербезпеки є створення багаторівневої системи безпекових заходів; розширення компетенції та обізнаності громадян країни з питань інформаційної безпеки; правове регулювання питань кібербезпеки; зміцнення позиції Естонії як однієї з країн-лідерів у міжнародній співпраці в сфері кібербезпеки. При створенні багаторівневої системи безпекових заходів пріоритетне значення надається захисту критичної інформаційної інфраструктури, розробці і впровадженню заходів безпеки та організаційному співробітництву. [89, 90].

З метою ефективного створення інформаційного захисту варто звернути увагу на досвід США та держав-членів ЄС, проте для об'єктивної оцінки фактів варто не забувати, що всі країни мають більш ефективну систему технологій. На сьогоднішній день у США надзвичайно важливе питання – це національна безпека. Ураховуючи особливості сучасного світу, воно включає в себе прогнозування міжнародних відносин; національні доктрини та стратегії національної безпеки; військові стратегії та прогнозування, забезпечення інформаційної безпеки. Усі ці структурні елементи взаємозв'язані. Незважаючи на те, що США мають надзвичайну потужну як юридичну, так і технічну базу, 2016 року виник скандал (розслідування котрого триває). Глава Національної розвідки та Міністерства національної безпеки звинуватили Росію у втручанні в перебіг президентських виборів методом злому серверів Демократичної партії США. Країни-члени Європейського союзу ще в 1990-х ухвалили правове підґрунтя забезпечення інформаційної безпеки як у всьому Альянсі, так і в кожній державі окремо. Першочерговими завданнями – захищати загальні цінності, основні інтереси та незалежність Союзу; зміцнювати безпеку Союзу та держав-членів усіма способами; розвивати та консолідувати демократію й законність, повагу до прав людини й основ-них свобод. Ці функції не втратили своєї важливості, однак світ диктує свої правила, та з'явилися нові проблеми. Відтак, розслідування німецькими спецслужбами дій російських хакерів та ЗМІ

продемонструвало, що Москва послідовно провадить інформаційну політику, котра має на меті дискредитацію канцлера Німеччини Ангели Меркель та дестабілізацію політичного клімату в ФРН. Аналогічна ситуація була засвідчена в інших європейських державах. У зв'язку з цим, Європейський союз вимушений був осучаснювати своє законодавство щодо інформаційної безпеки. У 2016 році Європейський парламент ухвалив план забезпечення нової Стратегії європейської політики безпеки і оборони. Згідно з цим актом, організаторами інформаційних атак Росії на Європу є МЗС Росії та Федеральне агентство "Россотрудничество", які застосовують комплексні заходи, величезний перелік інструментів, включаючи засоби масової інформації, інформаційно-аналітичні центри та спеціальні фонди. За словами європейських експертів, найбільшу загрозу з них для Європейського Союзу становлять російські пропагандистські агентства, зокрема: агентство «Спутник», телеканал «Russia To-day» та фонд «Русский мир» [76, с.72].

Однак варто брати до уваги той факт, що Україна знаходиться у стані війни з Росією, яка відпрацьовує разом з військовою ще й інформаційну тактику війни, застосовуючи при цьому різні інструменти та засоби і не гребує відвертою брехнею. Тим паче, що Кремль здійснює свої інформаційні атаки на Україну і з територій інших країн здійснюючи всілякі провокації. Якщо проаналізувати історичний досвід інших, зокрема, європейських країн, то можемо згадати приклад міністерства інформації у Великій Британії, заснованому 1939 році після її вступу у Другу світову війну, як інституції, покликаної контролювати інформаційний простір країни в складних умовах воєнного часу з метою запобігання ідеологічних, інформаційних диверсій ворога. Провівши аналогію між Україною та Британією, можна відзначити, що Британія створила таке Міністерсво задля боротьби із потужною нацистською пропагандою, тоді як Україна задля боротьби з пропагандою Росії. Британія також створила мережу за допомогою регіональних інформаційних комітетів, які надавали оперативну інформацію з регіонів та допомагали формувати внутрішню політику під час війни [76]. Тому, вважаємо створення Міністерства

інформаційної політики цілком виправданим, але потрібно змінити парадигму його роботи.

Таким чином, важливою рисою сучасних міжнародних відносин є стрімкий розвиток інформаційного суспільства, основу якого складають інформаційно-комунікаційні технології (ІКТ). Важливими тенденціями сучасного етапу розвитку людства є також інтенсифікація транскордонних інформаційних потоків, поширення різноманітних способів і засобів інформаційних війн, які практично не контролюються державою. За цих умов набувають поширення нові інформаційні загрози та виклики, що вимагають від держав негайного реагування й застосування нестандартних заходів і рішень.

В зв'язку з цим пріоритетним питанням в Україні на регіональному і національному рівнях стає інформаційна протидія. Так, гібридна війна на теренах нашої держави розпочалася задовго до відкритого військової агресії. Ще від початків незалежності України російські канали супутникового мовлення, радіомовлення транслювали передачі, кінопродукцію із своєю викривленою ідеологією, спрямованою на підрив європейських цінностей та нагнітання міжетнічної ворожості, у тому числі маніпулювання мовними, релігійними, економічними питанням. В 2022 р. латентна форма війни за допомогою інформації переросла у відкритий збройний конфлікт.

Україна за понад вісім років війни накопичила чималий досвід протистояння інформаційній гібридній агресії з боку Росії. Окрім вдосконалення законодавчої бази щодо протистояння гібридним викликам, що стало предметом дослідження в попередніх розділах, Україна має власний досвід боротьби з інформаційною експансією. Серед інституцій, які були створені вже у ході російської агресії та входять до сфери інформаційної безпеки є Український кризовий медіа-центр, започаткований зусиллями провідних вітчизняних експертів у сфері міжнародних відносин, комунікацій та зв'язків з громадськістю, аби виконувати функцію публічного майданчика для виступів представників української влади, експертів, представників міжнародних організацій та дипломатичного корпусу з оперативними заявами

та аналізом ситуації в країні [80]. На базі інформаційного агентства «Укрінформ» створено об'єднаний інформаційно-аналітичний центр «Єдина Країна». Центр став офіційним інформаційним ресурсом, мета якого - об'єктивне інформування громадськості в Україні та за кордоном про розвиток суспільно-політичної, військової та економічної ситуації в державі та її окремих регіонах, єднання суспільства перед фактом внутрішніх економічних труднощів та зовнішніх військових загроз.

Окремий напрямок діяльності Центру – висвітлення дипломатичної діяльності України [82]. Важливого інституційного й організаційного значення набув Інформаційно-аналітичний центр Ради національної безпеки і оборони України, який був створений за Указом Президента України № 398/2014 від 12 квітня 2014 року «Про Інформаційно-аналітичний центр» [29]. До його основних завдань належать забезпечення аналітичного та прогнозного супроводження діяльності РНБО щодо здійснення координування діяльності органів виконавчої влади з питань національної безпеки в інформаційній сфері; підготовка пропозицій стосовно інформаційного супроводження діяльності органів виконавчої влади та правоохоронних органів щодо забезпечення стабілізації суспільно-політичної ситуації в Україні. Окрім того, у 2017 році Міністерство інфраструктури створило Генеральний секретаріат цифрової інфраструктури та державне підприємство, яке буде опікуватися питаннями кібербезпеки. До сфери державного підприємства, належать питання кіберзахисту, контролю за пожежно-техногенними ситуаціями, фізичної охорони і оборони об'єктів критичної інфраструктури. У рамках роботи Генерального секретаріату цифрової інфраструктури планується створення спільної робочої групи з представниками СБУ, які займаються питаннями кібербезпеки, а також Нацполіції, Державної служби захисту інформації, РНБО. ЄС виділив на цю структуру близько 60 млн. гривень [30].

Базовим завданням інформаційної політики держави на деокупованих територіях на сьогоднішній день є припинення процесу взаємовідчуження громадян України в умовах війни. На окупованих територіях в свідомості

суспільства активно формується образ ворога з українця як «фашиста», а державної влади – як «київської хунти». Але, з іншого боку, подібні віддзеркалені цінності «образу ворога» доволі довго й активно насаджувались в Україні щодо мешканців Донбасу. Їх впровадження розпочалось ще з часів Майдану, квінтесенцією чого стали гасла «Спасибо жителям Донбасса за президента…», «Хто не скаче, той москаль» та інші. Під час АТО це інформаційне відчуження посилилось і відобразилось у нових значеннях – «вата», «колоради», «укроп», які активно використовують навіть лідери окремих фракцій Державної Думи Росії та Верховної Ради України. Об'єднання громадян до однієї групи (електоральної, політичної, соціальної, регіональної) за таких обставин відбувається не за принципом наявності певних об'єднуючих ознак, а за негативним принципом – відсутності єдиних рис та об'єднуючих принципів, характеристик з категорією ворога. Це сприяє не лише створенню, а й подальшому закріпленню у свідомості громадян межі між мешканцями Донбасу та рештою громадян України. Значна кількість українських політиків реалізують публічну політику, базуючись на емоціях електорату. В окремих випадках йдеться про популяризацію полярного мислення («так-ні», «хороший-поганий», «хто не з нами, той проти нас») та емоцій найнижчого рівня – на кшталт тих, які використовуються у виступах ворожих лідерів, зокрема лідерами сепаратистів та кремлівськими ідеологами на кшталт Кисельова чи Соловйова [37].

За прикладом Польщі, Україна створила державну структуру аналогічного формату. На виконання положень Стратегії національної безпеки України з урахуванням загроз інформаційній безпеці та масштабів агресивної інформаційної експансійної політики РФ проти України, політичне керівництво вчасно прийняло рішення щодо необхідності утворення Центру протидії дезінформації, який інституційно був створений рішенням РНБО України від 11 березня 2021 року, яке було введене в дію Указом Президента України від 19 березня 2021 року. Цим Указом було затверджено положення про Центр протидії дезінформації, який відповідно до його засад його функціонування є

робочим органом Ради національної безпеки і оборони України. До його основних ключових завдань належить: здійснення заходів з протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері; посилення та забезпечення інформаційної безпеки держави; виявлення та протидіїдезінформації; протидія пропаганді, деструктивним інформаційним впливам і кампаніям; запобігання спробам маніпулювання громадською думкою тощо [45].

У цьому розумінні варто не лише проводити системну інформаційну політику, спрямовану на популяризацію єдності на базі позитивних цінностей. Доцільним виглядає також встановлення правової відповідальності для високопосадовців, які поширюють регіональну нетерпимість або сепаратизм. У складних умовах управління деокупованими (особливо прифронтовими) територіями, що перебувають під контролем української влади, питання формування та реалізації інформаційної державної політики, з охопленням в перспективі і окупованих ворогом частин Донецької та Луганської областей, є фундаментально важливим. Адже населення цих територій подекуди досі демонструє неоднозначні настрої та оцінки конфлікту з Росією. В умовах інформаційного вакууму сподіватися на справжню реінтеграцію громадян, що мешкають на цих територіях, в суспільно-політичне та культурне поле України не варто. Безумовною є необхідність орієнтації внутрішньої політики держави на захист інформаційного простору України, протидію потенційним і реальним загрозам в інформаційній сфері засобами державного управління за трьома основними напрямками: інформаційно-психологічним, технологічного розвитку та захисту інформації [37]. Дієвими можуть бути різноманітні заходи обмежувального характеру, зокрема щодо вчинення протиправної інформаційної діяльності, а також заходи, спрямовані на перевірку інформації, її повноти, актуальності, неупередженості, об’єктивності, правдивості й релевантності [2].

Інформаційна політика держави на деокупованих територіях має розроблятися й реалізовуватися не лише шляхом пошуку конкретних

відповідей на окремі виклики та загрози, але й орієнтуватися на створення безпечних умов функціонування інформаційного простору в цілому. На наш погляд, стратегія реінтеграції деокупованих (а в подальшому і тимчасово окупованих) територій Донецької й Луганської областей має бути комплексною і включати низку заходів у різних сферах, в тому числі в інформаційній. До таких заходів в першу чергу слід віднести: - розробку і реалізацію активної інформаційної кампанії шляхом налагодження постійної трансляції на окуповані території Донбасу ефіру центральних українських телеканалів українською та російською мовою з метою об'єктивного висвітлення подій в Україні та світі і розвінчання неправдивих міфів, що поширюються Російською Федерацією; - створення для протидії «ідеям руського міра» власного національного інформаційно-культурного проекту (наприклад, «Велика Україна», «Український світ», «Великі українці» тощо), спрямованого на консолідацію українського народу; - проведення інформаційно-просвітницької кампанії популяризації історії та культури Донбасу серед усіх категорій населення; - створення єдиного електронного порталу – бібліотеки видань з історії України; - створення системи інформаційного висвітлення ініціатив та проектів щодо питань реінтеграції Донбасу через вітчизняні ЗМІ, зокрема шляхом створення окремих рубрик, теле- і радіопередач, присвячених цій тематиці **[**31**].**

Важливим завданням інститутів інформаційної безпеки є впровадження ефективної комунікативної політики як на внутрішньому, так і на зовнішньому рівні. Сама стратегія комунікативної політики має бути спрямована на інтеграцію регіонів України. Нині спостерігається великий розрив між громадянами та владою. Держава зобов'язана розробити таку комунікативну політику, яка б забезпечила перманентний діалог «державна влада – громадяни», та забезпечити відкритість державного управління. Громадяни мають отримувати доступ до інформації щодо їх прав, обов'язків, можливостей, про діяльності органів державної влади та мати можливість у виробленні державної політики.

Втім саме у зазначеній сфері на сьогодні, поряд із позитивами (насамперед в декларації завдань і шляхів патріотичного виховання молоді, набуття ними здібності критичного мислення й критичного сприйняття інформаційного середовища) виявляють себе серйозні прогалини, пов'язані, зокрема, з історичною, політичною (політологічною), в цілому – українознавчою освітою. Нині РФ збільшує кількість годин на викладання історії в школах і вищих навчальних закладах, де основу складає не науковий, а ідеологічний підхід із фальшуванням історичних подій на користь Росії. Така ж тенденція спостерігається на тимчасово окупованих територіях Донбасу та в анексованому Криму.

В Україні ж в умовах війни виявила себе тенденція на скорочення годин на викладання курсів з історії, політології, публічного управління та практично, їх вилучення з навчального процесу у ЗВО. Останнє тлумачиться як прояв компетентнісного підходу при формуванні навчальних планів, де тенденційно на практиці сприймається саме поняття «компетентності спеціаліста» із обмеженням їх чисто фаховими навичками – без ідейного змісту як патріотично підготовленої молодої особи з чіткою громадянською позицією, знаннями історії України, готової працювати на благо суспільства. Для подолання вже нанесеної шкоди та зміцнення інформаційної безпеки, актуальним є вирішення питання підготовки фахівців із захисту інформаційного простору від деструктивних впливів. Для цього у вищих навчальних закладах слід увести спецкурси, створити відповідні спеціальності, налагодити обмін науковцями. Адже своєчасний аналіз ситуації, превентивні дії та реакція фахівців на ту чи іншу загрозу є запорукою інформаційної безпеки країни. Серед актуальних завдань є розробка методології виявлення та запобігання впливу на суспільну свідомість, провокацій, дезінформації. Державна інформаційна політика має стати стрижнем у формуванні патріотизму молодого покоління, розвивати прогресивне мислення, консолідувати суспільство навколо національної ідеї.

Найважливіші функції держави і суспільства у протидії інформаційній

агресії РФ мають перебрати на себе засоби масової інформації. Так, розвиток ІКТ у сучасному світі приніс суттєві зміни у життя та функціонування суспільства. Важко уявити теперішній світ без Інтернету, телебачення, радіо, періодичної преси. Влада інформації стала вирішальною в керуванні державою та її захисті. Немає сумніву, що ЗМІ відіграють ключову роль у сучасних конфліктах і мають вплив на баланс сил у світі. Перемога у сучасних конфліктах залежить від формування внутрішньої та зовнішньої громадської думки, а не від перемоги на полю бою [8, с.97]. Як свідчить приклад найбільш розвинених і активних гравців світової арени, в їх відносинах із зовнішнім світом одна з пріоритетних ролей віддається сьогодні саме ЗМІ. Як відзначають експерти, якщо країна в сучасних умовах не зуміє увійти в світову інформаційно-телекомунікаційну систему як самостійний гравець, то їй доведеться поступитися частиною своєї незалежності іншим, більш розвиненим в цьому відношенні державам. Трансформувати ЗМІ в систему, здатну ефективно конкурувати з суперниками за кордоном, означає не тільки забезпечити інформаційну безпеку країни, а й створити ще один важливий інструмент для захисту зовнішньополітичних інтересів [60, с.40].

З огляду роль ЗМІ у сучасному політичному процесі, аналіз сучасного політичного процесу як глобального, так і локального масштабу нині можна чітко констатувати визначну роль у ньому ЗМІ, які просто не можуть бути виключені з поля зору і розглядаються комплексно. Так існує прямий зв'язок між ЗМІ та станом інформаційної безпеки. Роль ЗМІ у гібридній інформаційний війні, яку веде Росія проти України, подвоюється. У сучасних умовах, з одного боку, нашій державі потрібно перетворити власні медіа у своєрідний щит від кремлівського інформаційного тероризму та інформаційних впливів на внутрішньодержавному та міжнародному рівнях, а, з іншого боку, забезпечити суспільне мовлення і недопущення монополізації жодного типу ЗМІ в Україні. Окрім того, ЗМІ мають чесно і прозоро висвітлювати діяльність самої влади [64, с. 5].

Серед першочергових кроків інститутів інформаційної безпеки для її

захисту має стати збільшення об'єму україномовної преси, телепередач, кіно, Інтернет-ресурсів, а також забезпечення їх просування на зовнішній ринок іноземними мовами; інформаційно працювати із Південно-Східними регіонами України; пошук шляхів просування національного інформаційного продукту на територію РФ; створення позитивного іміджу України та брендування його на міжнародній арені тощо [5, с.99]. Окрім державних інституцій забезпечення інформаційної безпеки, важливу роль має інститут громадянського суспільства. Адже громадські об'єднання можуть стати неформальним центром з реалізації національних цінностей та інтересів. Тільки комплексне поєднання усіх цих напрямів дасть нову якість реалізації стратегії інформаційної безпеки.

Підсумовуючи варто наголосити, що інформаційна війна Росії проти України почалася ще за довго до відкритого збройного втручання. Москва намагалася втримати Україну у своєму інформаційному полі ще від початків незалежності. З огляду на ігнорування побудови комплексного механізму забезпечення інформаційної безпеки держави, Україна виявилася вразливою до російської інформаційної агресії. Цілком справедливо, що російсько-українську війну вважають гібридною, адже вона є асиметричним конфліктом та поєднує разом з військовими діями і не військові. Інформаційний компонент є визначальним у таких війнах, окрім того їх наслідки є не менш руйнівними ніж у класичних конфліктах і це цілком прослідковується на прикладі України. Росія завжди мала імперський характер зовнішньої політики. Той світовий порядок, який постав після «холодної війни» ніяк її не влаштовує, так як Росії відводиться роль другорядної держави у ньому. Тож у глобальному сенсі розвязуючи війну з Україною, метою Москви стало відновлення російської величі, але вже в новому світовому порядку який будуватиме Росія, ї їй має

За сучасних умов війни на Сході роль ЗМІ України є надважливою. За допомогою телебачення, радіо, газет, журналів, Інтернет-видань потрібно зуміти встояти на цьому інформаційному фронті. Важливим завданням ЗМІ також є допомога українцям усвідомити самих себе, свою історію, свій величезний потенціал і міць. Як зазначав київський митрополит Іларіон у своїй

праці «Слово про Закон і Благодать», що тільки створивши свій власний позитивний образ, народ може усвідомити себе господарем на своїй землі. У наш час завдання розповсюдження і промоції такого образу мають виконувати ЗМІ. Україні при цьому необхідно створити категорію журналістів високого класу, журналістів-експертів міжнародного класу, які б аналізували міжнародну тематику. Це, своєю чергою, сприяло б включенню України до глобального інформаційного контенту. Одним із основних завдань ЗМІ водночас є контрпропаганда (комплекс заходів, які націлені на боротьбу з ідеологічною пропагандою противника), яка б підштовхувала населення до аналізу інформації а не сліпої довіри тому, що вкладають в голови з екранів кремлівські пропагандисти. Однак можна простежити, що деякі вітчизняні ЗМІ підхоплюють більшість негативних сюжетів російських медіа, і часто самі підкидають такі сюжети за кордон. Що ж до системи контрпропаганди, то вона, попри усі розмови про її необхідність, фактично відсутня. Неоперативність, а часом і упередженість у висвітленні тих чи інших питань в українських медіа приводить до того, що інформаційні служби за кордоном часто-густо використовують російські телематеріали про Україну, що веде до зміщення акцентів у висвітленні подій в бік російських інтерпретацій [39, с. 38].

Важливою складовою у побудові загальної інформаційної картини відіграють соціальні мережі. Всі медіа активно використовують журналістику скріншотів, цитуючи повідомлення з особистих сторінок користувачів Facebook, Twitter, ВКонтакте тощо. Ця ділянка інформаційного простору слугує не тільки джерелом новин, а й емоційним тлом сприйняття поточних подій. Нині в Україні досить ефективно використовуються соціальні мережі і дають певний результат. Майдан теж починався із закликів на Fecebook об’єднатися і вийти на протест у знак непогодження з не підписання Януковичем Угоди про асоціацію з ЄС. Важливою рисою соціальних мереж є те, що тут люди можуть ділитися власними думками, ініціативами об’єднуючись у певні групи. Однак іншою стороною питання є те, що соціальні медіа широко використовуються ворогом для інформаційно-політичної підтримки військового вторгнення в

Україну, компрометації її євроатлантичного та євроінтеграційного курсу[37].

Підсумовуючи вищевикладене, можна окреслити основні механізми протидії російській інформаційній експансій

- консолідація суспільства;

- поширення національної ідеї та ідентичності; - зниження рівня ворожості;

- контроль влади;

- сприяння позитивному мисленню суспільства;

- виховання патріотичності;

- відбиття та реагування на російські інформаційні атаки;

- професіональний аналіз подій на основі реально існуючих фактів;

- поширення інформації про основні досягнення, культуру та традиції України.

- спростування російських фейків.

Аналізуючи інформаційну безпеку України у гібридної агресії, варто констатувати факт, що за період незалежності України, влада не спромоглася забезпечити ці регіони якісним інформаційним продуктом, спрямованим на формування у свідомості населення національної приналежності до України. Фактично з початку незалежності Україні не вдалося вибудувати в східних регіонах та Криму продуманої, зваженої та стратегічної інформаційної політики, яка б стала надійною платформою для подальшого захисту від агресивних інвормаційних впливів.

У регіональному розрізі Кремль всіляко прагне скомпрометувати роль НАТО, ЄС, ОБСЄ і тим самим зруйнувати систему безпеки в Європі. Для реалізації планів з відновлення «Великой Росии» та побудови «Руского мира» Москва розробила специфічні методи, де роль інформації є визначною. Воєнний фактор мав другорядне значення, натомість інформаційний вийшов на перший план.

Виходячи з цього встає необхідність додання процесу забезпечення інформаційної безпеки оптимальності, вибору якнайкращого з можливих

варіантів з врахуванням зарубіжного досвіду.

Основними шляхами вдосконалення системи забезпечення інформаційної безпеки України, можуть бути:

- розробка і ухвалення стратегії інформаційної безпеки, інформаційних довгострокових програм, направлених на забезпечення конкретних видів інформаційної безпеки(зокрема кібербезпека);

- своєчасне внесення до нормативно-правових документів змін і доповнень, з метою їх відповідності міжнародному стану;

- ініціація, формування, реалізація та оцінка інформаційної політики з реальним станом речей, враховуючи інтереси суспільства та складових соціальних груп, а також держави;

- вдосконалення організаційної структури системи забезпечення інформаційної безпеки та її політичної складової (ефективність роботи Міністерства інформаційної політики);

- підвищення ефективності діяльності суб'єктів забезпечення інформаційної політики України (ЗМК, інтернет-ресурсів, соціальних мереж);

- пошук і вибір раціональних рішень для комплексного використання наявних можливостей і ресурсів в системі протидії фейкам, ботам та та в цілому пропаганді.

ВИСНОВКИ

Дослідження гібридної війни в умовах сучасних інформаційних технологій дозволяє не тільки проаналізувати поняття «інформаційна експансія», «інформаційна війна» а й історичні та політичні передумови російської агресії проти України, а й запропонувати дієві механізми запобігання виникненню подібних явищ у майбутньому. Українські реалії та світові тенденції зумовлюють необхідність зважати на мілітарні чинники політичного процесу. Процеси, що поєднують сфери інформації та оборони, й події на Сході України виявили феномен медіатизації війни, де основна роль відводиться інформаційним технологіям.

Медіатизація війни призводить до посилення політизації конфлікту, коли політичні методи домінують над воєнними, що дедалі посилює роль та значення інформаційних технологій.

Автор погодився з твердженням про комплексність інструментарію інформаційної війни та, враховуючи досліджені аспекти гібридної війни, здається цілком зрозумілим і виправданим запровадження Україною тимчасових обмежень на доступ до окремих інформаційних сайтів, засобів масової інформації, фізичних осіб, тому що це один з елементів та форм прояву діяльності агресора на території суверенної країни і вплив на стратегічні ресурси з метою її дискредитації..

Таким чином, комплекс інформаційно-пропагандистських та заходів, що здійснює РФ проти України, можна охарактеризувати поняттям «інформаційна війна», а «інформаційну експансію» потрібно трактувати як комплекс технологій пропагандистського спрямування, які поширюються як державними органами так приватними інформаційними установами для досягнення власної політичної, економічної, інформаційної вигоди.

Висвітлюючи особливості інформаційного протистояння Росії проти України, слід зазначити, що ми програємо нашому східному сусідові: він веде цю війну більш успішно, більш активно, не нехтуючи засобами дезінформації

Безумовно, правда завжди перемагає, але це потребує часу. Тому треба активніше вдосконалювати інфосферу суспільства, постійно пропагувати суспільно значущі цінності, а найголовніше – перетворювати ці цінності в реальність. А із цим у нас завжди труднощі, незалежно від того, хто перебуває при владі. Будь-яка війна, у тому числі й «гібридна», колись закінчиться, а інформаційна боротьба за розум і серця людей не закінчиться ніколи, оскільки ми вступили в інформаційну епоху, де головним джерелом багатства та благополуччя людей стає інформація. Якою вона дійде до людей, який світ вони створять – чи європейський, чи руський, чи якийсь інший – залежить від кожної людини, від громадянського суспільства та держави. Тому головний висновок в процесі інформаційної експансії, – це потреба у формуванні ідеалу нашого майбутнього, який був би близьким і зрозумілим для кожного громадянина України незалежно від національності та місця проживання.

Основними механізмами, та методами реалізації інформаційної експансії Росії щодо України стали маніпуляції, пропаганда та дезінформація. Основною метою РФ було розколоти Українську державу з середини та створити хаос. Інформаційна сфера виявилася найбільш вразливою у безпековому секторі України, виявивши проблеми і в законодавчій та інституційних сферах.

Об’єктивна реальність гібридної війни поставила питання пріоритетів інформаційної державної політики в Україні та адаптації інституційного забезпечення інформаційної безпеки до нових умов та напрацювання нових механізмів у цій сфері.

До основних пріоритетів інформаційної безпеки потрібно віднести: застосування асиметричних дій проти всіх форм і проявів інформаційної агресії; створення системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей; створення, розвиток, координація інститутів, що відповідають за інформаційно-психологічну безпеку; удосконалення професійної підготовки у сфері інформаційної безпеки, впровадження

загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу; розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки.

Інформаційний складник механізмів протидії інформаційній експансії Росії щодо України став наскрізним для всієї російської агресії. Спираючись на потужну багаторічну інформаційно-психологічну обробку своїх громадян і громадян України, активну кампанію в соціальних мережах, часткове скуповування українських ЗМІ, Росія створила власний контент в Україні, до чинників боротьби із зазначеною ситуацією потрібно віднести: використання стратегічного контенту (книги, телесеріали, фільми, наукові дослідження в протидії російській пропаганді, створювати власний інформаційний продукт, збільшувати підтримку громадянами дій керівництва держави в умовах війни.

Щодо вдосконалення механізмів протидії російській інформаційній експансій в дискурсі зарубіжного досвіду та вітчизняної практики, потрібно відзначити, що проти України здійснюється неймовірно потужна інформаційна війна з використанням механізмів, стилів та сфер реалізації комунікаційних маніпулятивних технологій. На думку автора, Українська держава повинна не лише оборонятися в інформаційній війні, а й вести наступальні дії по відношенню до агресора. Крім того, необхідним є вироблення стратегії та тактики ведення боротьби в інформаційному полі та утворити структуру, яка буде займатися аналізом та збором необхідної інформації для боротьби на «випередження супротивника».

Для досягнення результатів в повномасштабній російсько-українській війні необхідно не тільки проводити бойові дії, а й висвітлювати, виправдовувати характер їх дій та залучати як можна більшу кількість населення на свою сторону. Методом розумного переконання це зробити вкрай важко, і тому виникає потреба у викривленні сприйняття тих чи інших подій, застосуванні методів інформаційної експансії.

Отже, гібридну війну можна виграти тільки гібридними засобами, за допомогою ефективних і стрімких технологій, які будуть адаптовані до власних

умов та цілей.

Посилення впливу інформації на політичну сферу призвело до появи проблеми забезпечення інформаційної безпеки держави, як складової національної безпеки. Крім того, саме забезпечення інформаційної безпеки багато у чому визначає ситуацію у всіх інших сферах національної безпеки.

Саме в 2022 році пропагандистська антиукраїнська кампанія виявила недостатній рівень розробленості наукових та методологічних напрацювань у сфері інформаційної безпеки України та показала слабку координацію діяльності державних органів, науковців, громадянського суспільства для протидії інформаційній агресії, яка справила значний вплив на свідомість в українському суспільстві, хоча потрібно констатувати, що останні місяці війни демонструють, що державні органи спроможні вирішувати завдання інформаційної безпеки.

На вирішення зазначеної проблеми потрібно зосередити увагу, як державним органам, так і фахівцям, експертам, громаді. За таких умов потрібно адекватно реагувати на інформаційні виклики та сформувати концепцію наступальної інформаційної політики, у тому числі й в медіа-просторі закордонних держав з використанням потужностей й можливостей, кадрового потенціалу новоствореного Центру протидії дезінформації як робочого органу РНБО України. Також доцільно посилити контроль за діяльністю інформаційних структур та їх структур, органів влади та місцевого самоврядування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безперстова О, 2017, Мало кто знает, что в Финляндии белые тоже воевали против красных, которых полностью поддерживала и финансировала большевистская Россия, *Факты,* 20 января, с.4.
2. Бегма В.М., Загорка О.М., Косевцов В.О., Шемаев В.М. Стратегічне управління військовотехнічним співробітництвом в інтересах застосування воєнної безпеки України; Монографія / Під заг. ред. Руснака І.С. — К.: ПІНБ, НАОУ, 2005. — 228
3. Богуш В.М., 2005, Інформаційна безпека держави, К., МК-Прес, 432 с.
4. Брехуненко В., 2014, Спершу свідомість, потім зброя, *Український тиждень,* № 52, с. 36.
5. Валюшко І. О., 2016, Витоки інформаційної агресії Росії в Українському інформаційному просторі, *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*, Випуск 1-2 (29-30), С. 95 –99.
6. Валюшко І. О., 2017, Інформаційна безпека України: трансформація законодавства після російського вторгнення, *Історико-політичні студії. Збірник наукових праць*,№ 2 (8),С. 30 - 43.
7. . Валюшко І. О., 2016, Кібербезпека України: наукові та практичні виміри сучасності, *Вісник НТУУ «КПІ» Політологія. Соціологія. Право*. № 3/4 (31-32), С. 117-124.
8. Валюшко І. О., 2016, Інформаційна агресія Росії, *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*, Випуск 4-5, С. 105-110..
9. Валюшко І. О., 2016, Основні виклики і загрози в інформаційних війн, *Науковий вісник Дипломатичної академії України. Зовнішня політика і дипломатія: традиції, тренди, досвід. Серія «Політичні науки»* / За заг. ред. В.Г. Ціватого, Н.О. Татаренко, Випуск 23, Частина ІІ, С. 142-147.
10. Війна «гібридна», 2015, Політологічний енциклопедичний словник, уклад.: Л. М. Герасіна, В. Л. Погрібна, І. О. Поліщук, Харків, Право, 816 с.
11. Гібридна війна: питання та відповіді [online] Доступно:

https://ms.detector.media/trends/1411978127/gibridna_viyna_pitannya_i_vidpovidi/

12. Гібридна війна Росії проти України: уроки та висновки [online] Доступно: https://www.ukrinform.ua/rubric-polytics/2107122-gibridna-vijna-rosii-proti-ukraini-uroki-ta-visnovki.html
13. Гібридна війна Росії проти України: уроки та висновки. Укрінформ. 2016 [online] Доступно: https://www.ukrinform.ua/ rubric-polytics/2107122-gibridna-vijna-rosii- proti-ukraini-uroki-ta-visnovki.html.
14. «Гібридна» війна Росії – виклик і загроза для всієї Європи[online] Доступно: http://old.razumkov.org.ua/ukr/upload/GIBRID-WAR-FINAL-1-1.pdf. 86. Магда Є. Гібридна агресія Росії: уроки для Європи - Київ: КАЛАМАР, 2017. – 268 с.
15. Горбань, Ю., 2015. Інформаційна війна проти України та засоби її ведення, *Вісник Національної академії державного управління при Президентові України* [online] Доступно: http://nbuv.gov.ua/UJRN/Vnadu_2015_1_21
16. Горбулін В., 2016, «Гібридна війна» як ключовий інструмент російської геостратегії реваншу, *Дзеркало тижня Україна,* № 2, с.3.
17. Горбулін, В., 2015. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу, *Дзеркало тижня,*2015, № 2 (24 січня). – с. 3.
18. Головко, ВВ., 2015. Україна в умовах антитерористичної операції та російської збройної агресії (2014 р.), *Український історичний журнал*, Вип. 3 (№522), с. 176-193.
19. Гусаров В., 2017, Сили інформаційних операцій Росії: яким має бути відповідь України?, *Інформаційно-аналітичний центр Національної безпеки України* [online] Доступно: http://mediarnbo.org/2014/10/07/sili-informatsiynih-operatsiy-rosiyi-yak (дата звернення: 15.03.2018).
20. Гай-Нижник, П., 2016, Російсько-українська війна: особливості розв'язання військово-політичного конфлікту на Сході і Півдні України за сучасних геополітичних умов, *Українознавство,* № 4. с. 103-121.
21. Гулай, В., 2016, Розгортання «гібридної» війни Російської Федерації в

умовах системної кризи державної організації України: інформаційно-комунікативні аспекти', Україна в системі змін парадигми світопорядку XX–XXI століть,монографія, Вінниця: ТОВ «Нілан-ЛТД», с. 214-230.

22. Доктрина інформаційної безпеки, затверджена Указом Президента України від 25.02.2017 р. №47/2017. База даних Законодавство України [online] Доступно: http://zakon2. rada.gov.ua/laws/show/47/2017 (дата звернення: 27.03.2017).
23. Донбас у системі інформаційної безпеки держави: регіональні особливості, зовнішні виклики, інструменти боротьби з антиукраїнською пропагандою, Аналітична доповідь,К. : ІПіЕНД ім. І. Ф. Кураса НАН України, 2015, 196 с.
24. Динис Г., 2016, Сучасні гібридні збройні конфлікти (приклад агресії Російської Федерації проти України) *Геополітика України: історія та сучасність,* № 2, с. 108-112.
25. Залізняк, Л. 2016. Україна та Росія: війна цивілізацій', Російська окупація і деокупація України: історія, сучасні загрози та виклики сьогодення: мат. Всеукр. наук.-практ. конф, К.: МП Леся, с. 12-31.
26. Інформаційна війна проти України: міф чи реальність? [online] Доступно:: http://intkonf.org/slivka-vv - informatsiyna-viyna-proti-ukrayini-mif-chi-realnist
27. Ісакова, ТО., 2015,Маніпулятивні технології Російської Федерації під час анексії Криму: особливості застосування, *Стратегічні пріоритети, Вип.(37), с.74-82.*
28. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп., 2016, за заг. ред. А. Баровської , К., НІСД, 109 с.
29. Інформаційно-аналітичний центр. Указ Президента України №398/2014 12 від квітня 2014 року [online] Доступно:: http://zakon3.rada.gov.ua/laws/show/ru/398/2014.
30. Кібербезпекою об'єктів критичної інфраструктури опікуватиметься держпідприємство при Мінінфраструктури [online] Доступно:: http://ua.interfax.com.ua/news/general/465659.html. 195

31. Коваль З., 2013, Проблематика протидії інформаційно-психологічним загрозам Україні засобами державного управління, *Теоретичні та прикладні питання державотворення: електрон. наук*. Фах, Вип. 13. [online] Доступно: http://nbuv.gov.ua/j-pdf/tppd_2013_13_12.pdf.
32. Костюк І. А., 2017, Інформаційні війни в контексті революційних подій в Україні, *Актуальні проблеми соціальних комунікацій: матеріали студентської наукової конференції, 22 травня 2014 р. – Київ, 2014. – С. 57–60.*
33. Концепція (основи державної політики) національної безпеки України. Схвалено постановою Верховної Ради України від 16.01.1997, *Урядовий кур'єр,*1997, 06 лютого.
34. Лещенко А., 2017, Три мероприятия к годовщине расстрела Небесной Сотни организуются с территории России, *Факты,* № 24, с.4.
35. Лозовий В. С. «Інтерпретації історії у політиці Російської Федерації як загроза національній безпеці України». Аналітична записка [online] Доступно: http://www.niss.gov.ua/articles/1796/
36. .Литвиненко О. М. «Виклики національній політиці пам'яті в часи «гібридної війни». Аналітична записка [online] Доступно: http://www.niss.gov.ua/articles/1818/
37. Магда Є. В., 2015, Гібридна війна: вижити і перемогти, Харків,Віват, 304 с.
38. Магда Є. Гібридна війна: питання і відповіді / Є. Магда // MediaSapiens. – 2016 [online] Доступно: http://osvita.mediasapiens. ua/trends/1411978127/gibridna_viyna_pitannya_i_ vidpovidi/.
39. Маклюэн М., 2003, Понимание Медиа: Внешние расширения человека / М. Маклюэн ; пер. с англ. В. Николаева ; закл. ст. М. Вавилова, Москва; Жуковский : «КАНОН-пресс-Ц», 464 с.
40. Міжнародне безпекове середовище: виклики і загрози національній безпеці України, 2013,К.:НІСД, 64 с.
41. Міністерство інформаційної політики України. Офіційний веб-портал. [online] Доступно: http://mip.gov.ua/content/pro-ministerstvo.html.

42. МІП: «Інформаційні війська України» стають самостійним проектом Інтернет [online] Доступно: http://mip.gov.ua/news/1931.html.
43. Медіа профспілка висловлює жаль через методи створення Міністерства інформполітики. Незалежна медіа профспілка України [online] Доступно: http://nmpu.org.ua/2014/12/media-profspilkavyslovlyuje-zhal-cherez-metody-stvorennya-ministerstva-informpolityky/.
44. Олійник О.В., Соснін О.В., Шиманський Л.Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави [online] Доступно: http://old.niss.gov.ua/book/Sosnin_2.htm
45. Панченко О.А. Інституційне забезпечення процесів протидії російській інформаційній експансії та пропаганді в сучасному світі [online] Доступно: file:///C:/Users/USER/Downloads/243797-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-559920-1-10-20211107.pdf
46. Про інформацію: Закон України від 02.10.1992 № 2657–XII База даних Законодавство України [online] Доступно: http://zakon5. rada.gov.ua/laws/show/2657–12 (дата звернення: 27.03.2017).
47. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. Рішення РНБО від 28.04.2014 [online] Доступно: http://zakon2.rada.gov.ua/laws/show/n0004525-14.
48. Про Стратегію національної безпеки України. Указ Президента України від від 12.02.2007 № 105/2007 [online] Доступно: http://zakon3.rada.gov.ua/laws/show/105/2007/ed20070212
49. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». Указ Президента України від 26.05.2015 № 287/2015 [online] Доступно: http://zakon3.rada.gov.ua/laws/show/287/2015/paran7#n7.
50. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України». Указ

Президента України від 24.09.2015 № 555/2015 [online] Доступно: http://zakon2.rada.gov.ua/laws/show/555/2015.

51. Про Доктрину інформаційної безпеки України. Указ Президента України від 08.07.2009 № 514/2009 [online] Доступно: http://zakon3.rada.gov.ua/laws/show/514/2009.
52. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України від 25.02.2017 № 47/2017 [online] Доступно: http://www.president.gov.ua/documents/472017-21374.
53. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України». Указ Президента України від 15.03.2016 № 96/2016 [online] Доступно: http://www.president.gov.ua/documents/962016-19836.
54. Про інформацію. Закон України від 02.10.1992 № 2657-XII (з усіма змінами та поправками) [online] Доступно: http://zakon2.rada.gov.ua/laws/show/2657-12/ed20170101
55. Почепцов Г., 2015, Сучасні інформаційні війни Київ, ВД «Києво-Могилянська академія», 498 с.
56. ПопикВ.І.,Горовий В.М., Онищенко О.С., 2015, Проблеми суспільної безпеки в процесі розвитку соціальних мереж, монографія, Нац. акад. наук України, Нац. б-ка України ім. В. І. Вернадського, Київ: НВЦ НБУВ,200 с.
57. Перепелиця Г.М., 2015, Україна – Росія: війна в умовах співіснування, К.: Видавничий дім «Стилос»,880 с.
58. Півцов Г.В., 2017, Інформаційно-психологічна боротьба у воєнній сфері, монографія, Харків, Вид. Рожко С.Г., 276 с.
59. Півцов Г.В. 2014, Реалізація підходів інформаційної війни Російською Федерацією в сучасному інформаційному просторі України, *Наука і техніка Повітряних Сил,* Харків, ХУПС, № 2(15), с. 10–13.
60. Радковець Ю. І., 2014,Ознаки технологій «гібридної війни» в агресивних діях Росії проти України, *Наука і оборона*, 2014, № 3, с. 36–42.

61. Требін М., 2002, Інформаційне суспільство. Війни нової епохи, *Віче*, № 4, 64–68.
62. Расторгуев С.П., 2003, Философия информационной войны, Москва : Московский психолого-социальный институт, 496 с.
63. «Репортери без кордонів» засуджують створення Міністерства інформації в Україні. Інститут масової інформації [online] Доступно: http://imi.org.ua/news/46755-reporteri-bez-kordoniv-zasudjuyutstvorennya-ministerstva-informatsiji-v-ukrajini.html.
64. Рубан Ю., 2009, Україна як суб'єкт і об'єкт сучасних міжнародних інформаційних воєн, *Стратегічні пріоритети, Національний інститут стратегічних досліджень*, № 2(11), с 5–9.
65. Путін веде в Україні гібридну війну – генерал Каппен [online] Доступно: http://geostrategy.org.ua/ua/komentari/item/409-putin-vede-v-ukrayini-gibridnuviynu-–-general-kappen/
66. Світова гібридна війна: український фронт: монографія, 2017, за заг. ред. В.П. Горбуліна, Київ : НІСД,496 с.
67. Смола Л., 2016, Інформаційно-психологічний складник гібридної війни, *Національна безпека і оборона,* №9-10 (167-168),С. 68-71.
68. Соціокультурні механізми формування ментального імунітету проти зовнішніх маніпуляцій свідомістю населення України: монографія, 2015, В. Горовий (кер. проекту), О. Онищенко, В. Попик та ін.; НАН України, Нац. бка України ім. В. І. Вернадського, Київ, 228 с.
69. Стець створив «Інформаційні війська України», до яких може долучитися кожен, у кого є Інтернет [online] Доступно: http://detector.media/infospace/article/104110/2015-02-23-stets-stvorivinformatsiini-viiska-ukraini-do-yakikh-mozhe-doluchitisya-kozhen-u-kogo-einternet/.
70. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015 [online] Доступно: http://zakon2.rada.gov.ua/laws/show/287/2015 (дата звернення: 27.03.2017).

71. Сищук, ОА, 2015. Інформаційно-психологічний компонент «гібридної» війни, Україна в системі змін парадигми світопорядку XX–XXI століть: тези міжнар. наук.-практ. конф, К.:Київський ун-т ім. Б. Грінченка, с. 143–147.
72. Сугестивні технології маніпулятивного впливу: Навчальний посібник [online] Доступно: http://pidruchniki.com/19790213/ psihologiya/sugestivni_tehnologiyi_manipulyativnogo_ vplivu.
73. Сутність гібридної війни проти України [online] Доступно: http://goal-int.org/sutnist-gibridnoi-vijni-proti-ukraini/
74. Твердохліб О.С., 2015, Концептуальні підходи до розроблення інформаційної політики держави у кризових умовах, *Теорія та практика державного управління і місцевого самоврядування,* №2, С. 14-18.
75. Технології розвитку і захисту національного інформаційного простору: [монографія] / [О. Онищенко (кер. проекту), В. Горовий, В. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – Київ, 2015. – 296 с.
76. Ткачук Т.Ю., 2017, Забезпечення інформаційної безпеки: досвід окремих країн східної Європи, *Інформація і право,*4(23),с. 62-72.
77. Требин М., 2005, Войны XXI века, М.: АСТ; Минск: Харвест, 608 с.
78. Туман «гібридної війни»: чому шкідливо мислити гібридно [online] Доступно: https://commons.com.ua/ru/tuman-gibridnoyi-vijni-chomu-shkidlivo-misliti-gibridno/
79. Тодоров І., 2016, Внутрішні витоки та зовнішні чинники російської агресії на Донбасі Російська окупація і деокупація України: історія, сучасні загрози та виклики сьогодення: *Матеріали Всеукраїнської науково-практичної конференції* , К., «МП Леся», с. 250- 256.
80. Український кризовий медіа-центр інформуватиме світ про події в державі війни [online] Доступно: http://www.ukrinform.ua/ukr/news/ukraiinskiy_krizoviy_media_tsentr_informu vati me_svit_pro_podiii_v_dergavi_191 4819

81. Україна протидіє інформаційній агресії війни [online] Доступно: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113969&cat_id=109884.
82. Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукраїнської науково-практичної конференції, м. Маріуполь, 9 червня 2017 р., Маріуполь: ДонДУУ, 311 с.
83. Чирва Р., 2014, Інформаційна війна – зброя, страшніша за ядерну, *Профспілкові вісті*, № 13, с. 8–9.
84. Шатун В.Т., 2016, Національної безпеки України, *Наукові праці. Державне управління*, Вип. 255, Т. 267, С. 174-180.
85. Шевчук В. П., Тараненко М. Г., 1999, Історія української державності, К., Либідь480 с.
86. Шпига П. С., 2014. Основні технології та закономірності інформаційної війни, *Проблеми міжнародних відносин,* Вип. 8, с. 326–339.
87. Як Росія веде інформаційні війни [online] Доступно: http://www.theinsider.ua/rus/politics/537f3dbe5c890/.
88. ENISA Country Reports 2009 [online] Доступно: http://www.epractice.eu/files/media/media2624.pdf
89. Estonian Cyber Security Strategy [online] Доступно: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf
90. Estonian Data Protection Inspectorate [online] Доступно: http://www.aki.ee/eng/
91. Information Tecnhology Security Evaluation Criteria : [online] Доступно:: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsecen_pdf.pdf
92. CERT-Fi [online] Доступно: http://www.cert.fi/en/index.html
93. Finnish Ministry of Transport and Communications [online] Доступно: http://www.lvm.fi/web/en/home
94. Common Criteria for Information Technology Security Evaluation [online] Доступно: https://www.commoncriteriaportal.org/files/ccfiles/CCPART

2V3.1R4.pd

95. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298 : [Online tool]. – Available at : http://ec.europa.eu/information_society/eeurope/2002/ news_library/ pdf_files/netsec_en.pdf
96. Communication from the Commission : Towards a general policy on the fight against cyber crime. COM (2007) [online] Доступно: http://eurlex.europa.eu/LexUriServ/site/en/com/ 2007/com2007_0267en01.pdf
97. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009)149 [online] Доступно: http://ec.europa.eu/information_ society/policy/nis/strategy/activities/ ciip/index_en.htm
98. Cyberintelligence : [Online tool]. – Available at : https://www.sri.ro/cyberintelligence-en.html 19. The Senate passed the draft low regarding the cyber security of Romania : [online] Доступно: http://actmedia.ua/daily/the-senate-passed-the -draft-law-regarding-the ceber-securityof-romania/55734
99. NATO Bucharest Summit Declaration, 3 April 2008 : [Online tool]. – Available at : http://www.nato.int/docu/pr/2008/p08-049e.html
100. North Atlantic Treaty Organization. Active Engagement/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation: [online] Доступно: http://www.nato.int/ lisbon2010/strategic–concept–2010–eng.pdf
101. NATO Lisbon Summit Declaration, 20 Nowember 2010 [online] Доступно: http://www.nato.int/docu/pr/2010/p10-049e.html
102. NATO Warsaw Summit Communiqué, 9 July 2016 : [online] Доступно:: http://www.nato.int/cps/en/natohq/official_texts_133169.htm
103. National Cyber Security Strategy : Cyber Resilient Bulgaria 2020 (2016) : [online] Доступно: https://www.itu.int/en/ITU-D/Regional-

Presence/Europe/Documents/Events/2016/Cyb ersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf

104. Romania’s Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013) [online] Доступно: https://www.cert.ro/vezi/document/ strategia-de-securitate-cibernetica
105. Speaking and Listening - the Ministry Abroad. MOI Digital[online] Доступно:: http://www.moidigital.ac.uk/blog/speaking-and-listeningministry-abroad.