МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

імені Михайла Драгоманова

Історичний факультет

Кафедра історії міжнародних відносин та гуманітарних дисциплін

МАГІСТЕРСЬКА РОБОТА

на здобуття освітнього ступеня **«магістр»** на тему :

«Інформаційний фронт України в умовах повномасштабної війни 2022 р.»

Студентки 2мімвз групи

спеціальності 291 Міжнародні відносини,

суспільні комунікації та регіональні студії

Васильєвої Валерії Сергіївни

Науковий керівник :

доктор історичних наук, професор

Стоян Тетяна Андріївна

Національна шкала _____

Кількість балів : _____ Оцінка :

ЕКТС _____

Голова комісії _____ _____

(прізвище та ініціали) (підпис)

Члени комісії _____ _____

(прізвище та ініціали) (підпис)

Київ – 2025

ЗМІСТ

ВСТУП……..3

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОГО ПРОСТОРУ…….....10

1.1. Структура інформаційної системи в Україні……...10

1.2. Вплив інформаційного простору на суспільні процеси……..13

1.3. Інформаційна безпека як складова національної безпеки……...15

РОЗДІЛ 2. ЗДАТНІСТЬ МАС-МЕДІА ВПЛИВАТИ НА СУСПІЛЬСТВО. ДЕЗІНФОРМАЦІЯ ТА ЇЇ НАСЛІДКИ……19

2.1. Роль ЗМІ у формуванні громадської думки……19

2.2. Соціальні мережі як інструмент впливу на думку народу…….21

2.3. Зусилля держави у боротьбі із дезінформацією……..24

РОЗДІЛ 3. НЕБЕЗПЕКА ПІД ЧАС ІНФОРМАЦІЙНОЇ ВІЙНИ……...26

3.1. Класифікація небезпек та загроз в інфо-середовищі……...26

3.2. Фейки та їх розповсюдження…….32

РОЗДІЛ 4. ПОВНОМАСШТАБНЕ ВТОРГНЕННЯ РОСІЇ В УКРАЇНУ ТА ЗМІНИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ……...39

4.1. Вплив РФ на українську інформаційну систему……39

4.2. Гібридна війна та застосування інформаційної зброї……44

РОЗДІЛ 5. РОЗВИТОК ІНФОРМАЦІЙНОЇ СИСТЕМИ……54

5.1. Виклики та загрози інформаційного простору……....54

5.2. Розвиток інформаційної системи України та майбутні зміни……61

ВИСНОВКИ…….....68

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……71

ВСТУП

Актуальність теми дослідження. Вивчення інформаційного простору є надзвичайно важливою та актуальною проблемою у сучасному світі через глобальну цифровізацію, зростання кіберзагроз і вплив інформаційних технологій на всі сфери життя, зокрема й в площині міжнародних відносин. Інформація визначає громадську думку, політичні процеси, економічні рішення та навіть соціальну поведінку людей. Маніпуляції у медіа, соціальних мережах та онлайн-платформах можуть призводити до серйозних наслідків, включаючи дестабілізацію державних структур, розкол у суспільстві та посилення конфліктів.

Хоча сучасні технології прогресують та здебільшого спрощують життя людства, на разі ми можемо спостерігати, що виникли нові форми загроз: кібератаки, витоки персональних даних, поширення фейкових новин та інформаційні війни. Захист національного інформаційного простору стає стратегічним завданням кожної держави.

У контексті міжнародних відносин та військових конфліктів інформаційний простір використовується як інструмент ведення гібридних воєн. Дезінформаційні кампанії спрямовані на підрив довіри до урядів, розпалювання паніки та маніпуляцію громадською свідомістю. Соціальні мережі стали основним джерелом інформації для мільйонів людей. Зараз будь-хто може поширити вірну або фейкову інформацію через мас-медіа та вплинути на думку громадян, змусити їх змінити позиції щодо певних ситуацій, новин. Державам варто обмежувати доступ до об'єктивних даних і сприяти поширенню фейкових новин, адже це створює можливості для розгортання конфліктів й напруги між усіма користувачами та водночас, породжують ризики зловживання персональними даними.

На даному етапі,–держави та міжнародні організації розробляють закони, що регулюють кібербезпеку, конфіденційність даних, боротьбу з фейками та захист

інформаційних прав громадян. Це стає ключовим аспектом забезпечення безпеки та стабільності у цифрову епоху.

Якщо поглянути на інформаційний простір на початку повномасштабного вторгнення росії в Україну, то можемо з'ясувати, що перед безпекою у сфері міжнародних відносин постало багато викликів та загроз, оскільки російсько-українська війна у 2022 р. стала не просто збройним, а й інформаційним конфліктом глобального масштабу. Все частіше у міжнародних конфліктах набирають обертів так звані – «гібридні війни», де інформація використовується як зброя для впливу на суспільну думку, політичні процеси та поведінку міжнародних гравців. Вивчення цього процесу є надзвичайно важливим для розуміння ефективності протидії інформаційним загрозам.

Починаючи з 24 лютого 2022 року, російська Федерація, далі РФ, посилила свій агресивний метод ведення війни, завдяки застосування інформаційно-психологічної боротьби з використанням широкого арсеналу маніпулятивних, пропагандистських прийомів, кібератак та дезінформації. Інформаційна війна, яку веде росія проти України є новим елементом у теоретичних дослідженнях міжнародних відносин. Це вимагає переосмислення традиційних понять сили, суверенітету та безпеки у глобалізованому світі, де інформація стає зброєю військової та економічної потужності.

На нашу думку, інформаційний простір став інструментом координації дії міжнародних організацій таких, як ООН, НАТО, ЄС та інших іноземних урядів. Протидія дезінформації, розвінчання фейків і підтримка незалежних ЗМІ – стали важливим інструментом для подальшої міжнародної комунікації й співпраці. Тож, Україна навпаки, продемонструвала всім на світовій арені, що інформація може бути використана для формування коаліцій, залучення допомоги та посилення тиску на агресора. Іншим державам точно стане корисним український досвід, адже кризові ситуації у політиці – є неминучі.

Дослідженням питань інформаційної безпеки та проблеми захисту національного інформаційного простору займалися наступні науковці :

Марущак А. «Питання ефективності діяльності державних органів у сфері захисту інформаційного простору України» - це аналіз результатів роботи державних структур, таких як : СБУ, РНБО, Мінцифри, Нацрада з питань ТБ і радіомовлення. Автор розбирає їхню діяльність стосовно протидії інформаційним загрозам; розглядає недоліки правового регулювання та пропонує шляхи підвищення ефективності захисту інформаційного простору України.

Кормич Б. «Інформаційна безпека : організаційно-правові основи» - це детальний огляд системи інформаційної безпеки, її структуру, а також принципи державної політики, нормативно-правову базу та функції органів влади. Значна увага приділена організації захисту інформації в органах державної влади.

Ліпкан В. «Інформаційна безпека як складова національної безпеки України» - це дослідження взаємодії держави, громадян і суспільства загалом. Автор пояснює, які загрози виникають на кожному рівні, які потреби має держава й громадянин у доступі до достовірної інформації, а також пропонує різні способи як захистити інформацію від її витоку.

Петрик В. «Сутність інформаційної безпеки держави, суспільства та особи» - детально розглядає механізми інформаційних війн, фейки, пропаганду, маніпуляції, психологічні операції, роль медіа у війнах, технології російської пропаганди.

Проблемні питання забезпечення інформаційної безпеки в Україні від моменту проголошення незалежності у 1991 році до сьогодення досліджували наступні історики, політологи та науковці :

Р. Лук’янчук – один з перших дослідників після проголошення незалежності України, хто досліджував інформаційну політику, державне управління

інформаційною безпекою, моделі протидії інформаційним загрозам; писав про інфопростір та його регулювання в умовах гібридних загроз.

А. Бабенко, В. Гавловский, Д. Дубов, В. Номоконов, М. Погорецький, В. Шеломенцев – мали схожі погляди та одну найголовнішу тему своїх досліджень: Безпека інформаційного простору. Їхні джерела, які є важливими для формування думок про інформаційну систему України та кібербезпеку держави, тому всі їхні праці додані до списку джерел в кінці дослідження.

Безліч іноземних журналістів та істориків дають оцінку російсько-українській війні і нам важливо аналізувати їхні роботи для порівняння стратегій та досвіду інших країн (США, Естонія, Ізраїль), аби перейняти кращі міжнародні практики кіберзахисту; зрозуміти, як глобальні структури (НАТО, ЄС, ООН) реагують на ці виклики. Іноземні дослідження про початок російського вторгнення в Україну:

1. Overreach: The Inside Story of Putin's War on Ukraine — журналістський і історичний нарис Оуена Меттьюза про походження вторгнення та перший рік війни. Виданий у 2022 році, як електронна версія і перевиданий у паперовому форматі 2023 р. https://en.wikipedia.org/wiki/Newsweek

2. The Russo-Ukrainian War — ґрунтовна історія конфлікту від Сергія Плохія, що простежує розвиток війни починаючи з 2014 року й до повномасштабного вторгнення, опублікована 2023 р. https://www.amazon.com/Russo-Ukrainian-War-Serhii-Plokhy/dp/1802061789?utm_source=chatgpt.com

3. Destroying the Myth of Russian Invincibility — дослідження Джона С. Гаррела, видане у січні 2024 р., аналізує хід війни та розвіює міфи про "непоборність" російської армії. https://www.penandswordbooks.com/9781399031769/the-russian-invasion-of-ukraine-february-december-2022/

Стаття «Russia's War Against Ukraine: Context, Causes, and Consequences» (2024) — академічний огляд, опублікований у журналі Problems of Post-Communism, що аналізує контекст вторгнення, його причини та наслідки. https://en.wikipedia.org/wiki/The_Zelensky_Effect?

Мета дослідження : провести дослідження особливостей розвитку інформаційного простору України на початку повномасштабного вторгнення та з'ясувати як агресивні методи РФ у веденні інформаційної війни вплинули на українське населення, владу та світову спільноту загалом.

Відповідно до поставленої мети, **завданнями магістерської роботи є :**

- визначити ключові особливості інформаційного середовища в Україні;

- встановити роль українських ЗМІ та їх вплив на сприйняття інформації;

- дослідити роль соціальних мереж як платформу для поширення новин та здатності змінювати думку читачів;

- проаналізувати реальні та потенційні загрози інформаційній безпеці України;

- надати практичні рекомендації щодо вдосконалення державної інформаційної політики та створення ефективної системи інформаційної безпеки України;

- порівняти досвід України з іншими країнами (Естонією та Ізраїлем) у боротьбі з інформаційними загрозами;

- сформувати майбутній план щодо зміцнення інформаційної безпеки України.

Об'єктом дослідження є сам інформаційний простір України на початку повномасштабного вторгнення Росії у лютому 2022 року, а також Засоби масової інформації, державні інформаційні ресурси, різні комунікаційні платформи українського суспільства.

Предметом дослідження є особливості функціонування, трансформації та впливу інформаційного простору України під час перших місяців війни, зокрема механізми протидії пропаганді та дезінформації, виклики та загрози управління інформаційним середовищем у кризовий період, взаємодія із міжнародними організаціями для припинення воєнних дій зі сторони росії, діяльність урядів іноземних держав стосовно протидії російської агресії.

Хронологічні межі даної роботи охоплюють 2 межі :

1) довоєнний період (з 2019 до 23 лютого 2022 року);

2) воєнний період (від 24 лютого 2022 року до сьогодення).

Верхня хронологічна межа обумовлена 2019 роком, адже саме з цього моменту почалися нові реформи у сфері інформаційного забезпечення. Важливими для українців стали наступні зміни :

1. Закон «Про забезпечення функціонування української мови як державної», що визначив українську мову основною для сфер ЗМІ, реклами й телебачення.

2. Блокування російських соцмереж (ВКонтакте, Одноклассники, платформа Яндекс), заборона російських телеканалів (ZIK, NewsOne, СТС).

3. Створена Стратегія кібербезпеки (2021 року), яка сприяла захисту цифрової інформації та протидіяла фейкам.

Географічні межі дослідження охоплюють східну частину Європи та північну частину Азії, а саме – територію України в її міжнародно визнаних кордонах, включно з тимчасово окупованими територіями Автономної Республіки Крим, міста Севастополя, окремих районів Донецької, Луганської, Запорізької та Херсонської областей, також західну частину росії.

Окрім того, з огляду на глобальний характер інформаційного простору, дослідження враховує діяльність українських медіа, державних інституцій та користувачів у світовому цифровому середовищі (зокрема у соцмережах, міжнародних ЗМІ, кіберпросторі).

Структура магістерської роботи. Структурно робота складається із п'яти розділів, які поділяються на підрозділи (всього їх 13) , висновків та списку використаних джерел та літератури. Загальний обсяг роботи становить 76 сторінок, основного тексту – 67 С.

РОЗДІЛ І. ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

1.1. Поняття та структура інформаційного простору

Найперше з чого варто почати, так це з визначення самого поняття «інформаційного простору». Це сукупність інформації, яка може зберігатися та циркулювати в процесі соціальних комунікацій. За різними критеріями класифікації можна поділити на : інформаційний простір окремої людини, групи людей, засобів масової інформації та держави. Даний простір містить у собі інформацію про сучасне, минуле й майбутнє. Здатен зберігати та накопичувати дані у активній та генетичній пам'яті окремих людей, етнічних спільнот, народів, а також на фізичних носіях. Суб'єктами інформаційного простору можуть бути : особи, що матимуть ідентичні або протилежні інтереси; професійні організації або громадські об'єднання громадян; економічні організації та різні соціальні інститути. До основних компонентів інформаційного простору належать :

-інформаційні ресурси;

-засоби інформаційної взаємодії;

-інформаційна інфраструктура.

Структурою інформаційного простору є сукупність стійких закономірних зв'язків між елементами системи. До основних складових належать – інформаційні поля та інформаційні потоки [3, с. 27].

Я рахую, що інформаційне поле має сприйматися як сукупність всієї можливої інформації, збереженої в повному обсязі. Сам інформаційний потік стосується даних, які переміщуються в інформаційному просторі через канал зв'язку. Інформаційна інфраструктура - це середовище, в якому особи мають можливість збирати, зберігати, передавати, автоматично обробляти та поширювати інформацію в суспільстві. Інформаційна інфраструктура суспільства формується на основі інформаційних та телекомунікаційних систем (ІТС) та мереж зв'язку, індустрії інформатизації, телекомунікацій та засобів зв'язку; системи формують

та захищають інформаційні ресурси; системи забезпечення доступу до ІТС, систем зв'язку та інформаційних ресурсів; інформаційний ринок, індустрія інформаційних послуг; система підготовки та перепідготовки кадрів, проведення наукових досліджень.

Ресурси інформації можуть бути поділені на : державні та недержавні ресурси; ті, що належать громадянам, державним органам влади, органам місцевого самоврядування, підприємствам, організаціям, установам та громадським об'єднанням. Відмінність інформаційних ресурсів від інших типів полягає в тому, що вони зазнають деградації через моральну, а не фізичну деградацію; вони не стають фізичними, та не зводяться до носія, що є набагато потужнішим і може значно зменшити споживання інших ресурсів, що призводить до величезної економії зусиль і засобів [33, с. 16].

Розглянемо основні характеристики інформаційного простору :

-він є неоднорідним і структурованим з акцентами на різні соціальні групи і теми;

-має динамічний розвиток у силу постійних змін, які відбуваються у різних сферах життя окремих країн, регіонів та світу загалом, а також нових акцентів в інформаційній політиці;

-інформаційний простір країни має бути захищеним від впливу інших держав.

Мета формування і розвитку національного інформаційного простору України полягає у створенні моделі державної інформаційної політики, а також політико-правових, економічних, організаційних та матеріально-технічних умов забезпечення розвитку та захисту національного інформаційного простору.

Щодо контролю інформаційного простору в мережі Інтернет, то детальне вивчення наукових джерел і зарубіжного досвіду дозволяє зробити висновки що методами контролю інформаційного простору в мережі Інтернет виступають наступні :

1) блокування або заборона доступу до сайтів, що містять інформацію, яка порушує чинне в тій чи іншій країні;

2) фільтрування інформаційного потоку в місцях загального користування (інтернет-кафе, навчальні заклади, підприємства) – передбачає обмеження доступу до інформації на основі “чорних списків” – заборони доступу до адрес, що містяться в списку чи “білих списків” – дозволу доступу тільки до конкретних адрес, а також за ключовими словами;

3) відстеження активності інтернет-користувачів;

4) авторизація користувачів при доступі в інтернет із застосуванням провайдерами програмних чи апаратних засобів [7, с. 87-88].

Через швидкий прогрес інформаційних технологій у суспільстві протягом 20-го століття виник так званий віртуальний простір. Його поступове і досить умовне поєднання з реальним простором («real place») через інформаційні та телекомунікаційні системи і мережеві технології різного функціонального призначення, які використовують електромагнітний спектр у процесах обробки, передачі та зберігання інформації і діють як єдине ціле, а також відповідне програмне забезпечення (ПЗ), призвело, в результаті, до формування так званого кіберпростору («cyberspace») [3, с. 91].

Отже, можна дійти висновку, що інформаційний простір розглядається як сукупність інформаційних ресурсів, технологій, комунікаційних мереж і соціальних взаємодій, що забезпечують обмін даними та знаннями в сучасному суспільстві.

Дослідження цього підрозділу вказує на те, що інформаційний простір є динамічним та розвивається під впливом технологічного процесу, соціальних процесів та політичних факторів. Зрозумівши його структуру дозволить ефективніше використовувати інформаційні ресурси та забезпечувати інформаційну безпеку всередині нашої країни.

1.2. Вплив інформаційного простору на суспільні процеси

Загальновідомий факт, що XXI століття характеризується активним розвитком інформаційних технологій. З'являються нові поняття, такі як : комп'ютеризація, оцифрування та інформатизація. Як можемо помітити, то технологічна та інформаційна глобалізацію світу породила нові потужні інформаційно-комунікаційні технології, віртуальні спільноти, соціальні мережі, які мають інші правила життя і підходять для всіх вікових груп населення.

Інформаційний простір – це сукупність всіх каналів поширення інформації, тобто : телебачення, Інтернет, друковані ЗМІ, соціальні мережі тощо, які здатні формувати суспільну думку, світогляд і поведінку людей. Він має як позитивний, так і негативний вплив на соціальні, політичні, економічні та культурні аспекти суспільства [9, с. 29].

На думку одного з дослідників у галузі інформації, Володимира Кириченко, маємо наступне твердження : «сучасне інформаційне суспільство – це є світ, який створили за образом та подібністю до людини».

Сьогодні гостро постає питання про те, як впливає інформаційне суспільство на формування ідентичності особистості, адже ідентичність – важлива передумова безпечного та комфортного існування як окремої людини, так і соціальних спільнот, суспільства в цілому. Ні для кого не секрет, що остання інформаційна революція призвела до створення нової галузі – інформаційної індустрії, яка пов'язана з виробництвом технічних засобів, методів та технологій для здобуття нових знань.

А також, дуже стрімкий розвиток комп'ютерної техніки та інформаційних технологій сприяв розвитку суспільства і призвів до вдосконалення техніки і технологій, які чинять вплив на формування ідентичності особистості [6, с. 74].

З цієї причини ідентичність повинна реалізовувати об'єктивний аспект стабільності, а також суб'єктивний аспект змінності та варіативності. У цьому

інформаційному середовищі людина стикається з множинними категоріями ідентичності.

Вплив інформаційного простору на соціальні процеси :

1. Формування суспільної думки. Медіа впливають на те, як люди сприймають певні події. Новини, аналітичні статті та соціальні мережі можуть змінювати уявлення про політику, економіку, соціальні питання.

2. Маніпуляції та пропаганда. Інформаційний простір може використовуватися для маніпуляції суспільною свідомістю. Політики, корпорації, держави використовують ЗМІ для поширення вигідних наративів.

3. Формування нових норм і цінностей. Через кіно, музику, блоги популяризуються нові ідеї та стилі життя. Наприклад, екоактивізм, толерантність, фемінізм або національна ідентичність можуть ставати більш поширеними завдяки медіа [1].

Вплив інформації на політичні процеси :

Медіа можуть як сприяти розвитку демократії (просвіта громадян, дебати), так і підривати її (дезінформація, впливові групи). Вибори часто залежать від інформаційних кампаній.

Окрім того, держави використовують інформацію як зброю, тобто розповсюдження фейків, створення кібератак, втручання у внутрішні справи інших країн через соцмережі.

Психологічний вплив : багато новин, фейків, агресивного контенту можуть викликати тривожність, депресію, відчуття безсилля. Соцмережі використовують алгоритми, що викликають звикання. Алгоритми соцмереж підсилюють радикальні погляди, адже показують лише той контент, який підтверджує думку користувача. Це може спричиняти конфлікти [33, с.102].

Отже, аналізуючи всю вищу наведену інформацію, можна дійти висновку, що інформаційний простір — потужний інструмент, що формує суспільство. Від

того, як люди фільтрують інформацію, залежить рівень критичного мислення, демократичність суспільства та його розвиток. Важливо навчитися аналізувати медіа, розпізнавати маніпуляції та вірно й правильно використовувати інформацію.

1.3. Інформаційна безпека як складова національної безпеки

Відомо, що безпека – це найголовніша мета й базова потреба не лише людини, а й цілого суспільства, так як від подолання загроз залежить розвиток людського суспільства. Високоякісна національна безпека вимагає врахування усіх аспектів : соціально-політичних, економічних, правових, геополітичних, екологічних та техногенних. Також, важливу роль у цьому складає інформаційне забезпечення національної безпеки.

Тож, розвиток інформаційного суспільства і зміни в різних сферах суспільних відносин призвели до появи ряду як позитивних, так і негативних наслідків. До позитивних наслідків відносять такі:

- пришвидшення передачі інформації значного обсягу,

- прискорення обробки інформації та її впровадження [16, с. 3],

- трансформація інформації, що ототожнюється з цифровим або віртуальним простором.

Як зазначає Б. Кормич, «основні дії щодо збирання, зберігання, передачі та розповсюдження інформації здійснюються за допомогою спеціальних технічних засобів і технологій. Відповідно з розвитком науки та техніки ці інформаційні засоби і технології перетворилися на один із найважливіших компонентів інформаційних процесів, одночасно із самою інформацією та суб'єктами інформаційних відносин» [27, с. 18].

Отже, розвиток вищезгаданих інформаційних засобів й технологій має переваги та недоліки – збільшення фактів протизаконного збору і використання

інформації, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків і баз даних, знищення та модифікацію даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку, несанкціонованого доступу до інформаційних ресурсів, порушення технологій обробки інформації, запуску програм-вірусів [4, с. 3].

На даний момент, гостро постає питання безпеки та захищеності відносин, пов'язаних зі збором, обробкою, зберіганням та використанням інформації.

Слід зазначити, що в інформаційних відносинах протягом останніх років сформувався та вже затвердився термін "інформаційна безпека". Що під ним розуміють? Це стан захищеності надважливих інтересів людини, суспільства і держави в цілому [16]. Отже, в самому визначенні вже закладено певні підстави для класифікації, які розглянемо згодом.

На думку В. Ліпкана, "інформаційна безпека" є невід'ємним напрямом розвитку інформаційного суспільства, що повинен відбуватися не тільки шляхом збільшення технологічних можливостей здійснення обміну інформацією, а й через адекватну і якісну співпрацю між власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг. [3, с. 61].

На думку А. Марущака пріоритетом у розвитку інформаційного права України є проблеми інформаційної безпеки. Слід зауважити, що загрози національній безпеці України, які виникають у сфері національних інформаційних ресурсів, мають бути вирішені завдяки правомірному використанню телекомунікацій у сучасному інформаційному суспільстві, що зможуть давати відсіч кібернетичним загрозам [17, с. 22].

Отже, рівень сучасних викликів і загроз в інформаційній сфері доводить важливість прийнятих положень статті 17 Конституції України, в якій наголошено на тому, що захист державного суверенітету і забезпечення

інформаційної безпеки є однією з основних функцій держави і всього українського народу [34, с. 89].

Інформаційна безпека є невід’ємною складовою національної безпеки, її регулювання потребує потужних механізмів не лише у формі політичних рішень, а й у прийнятті нормативно-правових актів. В Україні інформаційна безпека регулюється за допомогою наступних нормативно-правових актів : Конституція України, Концепція національної безпеки України, Закон України «Про інформацію», Закон України «Про Національну програму інформатизації», і звісно Указ Президента України «Про Доктрину інформаційної безпеки України».

Закони про національну безпеку України визначають, що інформаційна безпека є невід'ємною частиною національної безпеки. Основними об'єктами національної безпеки є людина, суспільство, держава. Головне завдання інформаційної безпеки – це забезпечити їхні інтереси [35].

На жаль, механізми управління інформаційною безпекою суттєво відстають у розвитку в порівнянні з іншими країнами. Тобто збільшується ризик рівня кіберзлочинності та створюються незворотні наслідки для держави, підприємства, суспільства та особи. Якщо взяти до увагу глобальний світ – то спостерігається широкий діапазон кіберзлочинів, які включають в себе :

•фінансові злочини, мета яких є отримати суму коштів незаконним шляхом;

•злочини, які відбуваються завдяки використанням гаджетів (мобільних телефонів, планшетів, ноутбуків та комп'ютерів);

•злочини спрямовані на отримання доступу до Інтернет-даних.

Останнім часом, інформаційна безпека займає одну з провідних позицій в системі національної безпеки. Інформація – це основна зброя у протидії держав світу в боротьбі за світове панування у глобальному інформаційному просторі. Розвиток таких галузей, як : оборонна промисловість, енергетика, зв'язок, наука

і медицина, транспорт та виробництво товарів залежить від інтенсивності, повноти, якості та своєчасності інформаційного простору [14, с. 174-175].

Ризики пов'язані із загрозою інформаційної безпеки – це негативні, протизаконні дії через які сама держава, організації цілком або частково втрачають можливість реалізувати свої інтереси в інформаційній сфері, адже порушується стале функціонування, відбувається витік даних або затримка розвитку технічних об'єктів інформаційної безпеки.

Без сумніву можна сказати, що шкода, яка завдана державі внаслідок реалізації ризиків, впливає на всі суб'єкти суспільства. Отже, державна політика щодо забезпечення інформаційної безпеки має опиратися на превентивну діяльність органів державного управління для надання гарантій інформаційної безпеки особистості, також соціальним групам, суспільству та державі в цілому. У сучасних умовах інформаційна складова національної безпеки держави відіграє важливу роль, адже в ній присутні певні ризики та загрози (кібертерорризм, кіберзлочинність, агресивна пропаганда та поширення антидержавних гасел, обмеження доступу населення до публічної інформації). На мою думку, політика інформаційної безпеки має орієнтуватися на забезпечення гарантій інформаційного суверенітету України та покращення інформаційної безпеки для всіх суб'єктів сфери інформатизації, тому що інформаційне забезпечення – це процес задоволення потреб людства.

РОЗДІЛ 2. ЗДАТНІСТЬ МАС-МЕДІА ВПЛИВАТИ НА ЛЮДЕЙ. ДЕЗІНФОРИАЦІЯ ТА ЇЇ НАСЛІДКИ

2.1. Роль ЗМІ у формуванні громадської думки

Почнемо з визначення поняття «ЗМІ». Це різні платформи і канали, які збирають, обробляють та поширюють інформацію для користувачів, використовуючи різноманітні технічні засоби. Це газети, журнали, радіостанції, телеканали, інформаційні служби, онлайн-видання тощо.

Засоби масової інформації є професійними й бюрократизованими організаціями, які існують та функціонують у публічній сфері у межах чинних правових норм. ЗМІ належать до системи мас-медій. [15, с. 193].

Засоби масової інформації виражають і формують громадську думку, яку прийнято розглядати як колективне судження людей, в якому ставлення до подій і явищ виявляється у формі схвалення, осуду або вимоги. Громадська думка формується в процесі руху інформації в суспільстві, відображає людське буття, суспільну практику людей і виступає як регулятор діяльності. ЗМІ значно впливають не тільки на свідомість слухачів, а й на вчинки цілої групи людей. [29, с. 77].

Громадська думка активно бере участь у здійсненні влади та стає важливим механізмом впливу на прийняття політичних рішень всіх рівнів. Оскільки вона виступає знаряддям політики, то її формування є сферою боротьби за владу. Основними видами громадської думки є референдум, опитування населення, громадські збори, маніфестації, всенародні обговорення. Кожне суспільство прагне мати справжніх громадян, які матимуть спільну ідею. Адже єдність переконань є основою розвитку будь-якої держави. Тому державі не байдуже, як формуються політичні переконання її громадян, їх ставлення до політичної системи, характер громадянської соціалізації [21, с. 212].

Звісно, ЗМІ відіграють вагому роль у житті народу, групи людей, жителів населених пунктів. Їм належить виконання деяких функцій, а саме :

1) функції соціальної комунікації та інформування;

2) виховання у громадян патріотичних цінностей;

3) створення відповідного соціально-політичного клімату.

Я також рахую, що надзвичайно важливо, аби держава контролювала засоби масової інформації, відповідно до чинних законів та Конституції, щоб унеможливити прояви інформаційної шкоди для своїх громадян. Засоби масової інформації здатні не тільки інформувати, повідомляти новини, а й пропагувати певні ідеї, погляди, вчення, політичні програми і, тим самим, беруть участь у соціальному управлінні, є частиною політичної системи поряд із парламентом, виконавчою владою, незалежним судом.

Це пояснюється тим, що ЗМІ здійснюють свою політичну, управлінську роль у політичній системі шляхом обговорення, підтримки, критики й осуду різних політичних програм, платформ, ідей і пропозицій окремих осіб, громадських формувань, політичних партій. Також, ЗМІ виконують роль своєрідного громадського контролю і оприлюднення його результатів [31, с. 48].

Отже, підсумовуючи усе вище сказане, можна дійти висновку, що основні функції мас-медіа в ліберально-демократичному суспільстві - це контроль за владою та встановлення довірливих стосунків між владою й суспільством. Засоби масової інформації мають на меті впливати на суспільство, тому часто обирають цікаві теми - обговорюють кризи різних сфер життя, роблять феноменальні заяви, запускають обговорення до етапу протесту.

2.2. Соціальні мережі як інструмент впливу на думку народу

На сьогоднішній день, соціальні мережі набувають все більшої популярності як варіант комунікації. За допомогою соціальних мереж встановлюється зв'язок між окремими індивідами незалежно від їх місця знаходження, відбувається обмін інформацією, аудіо та відеоматеріалами. Соціальні мережі мають ряд переваг і водночас трохи недоліків.

Якщо, поглянути на соціальні мережі під час ведення інформаційної війни, то можна зрозуміти, що їх головна функція - здійснення психологічного маніпулювання на користувачів.

Користувачі знаходять собі «лідерів думок» та беззаперечно довіряють всьому тому, що вони озвучують, рахуючи, що це правдива інформація. Завдяки таким «лідерам», відбувається переконання їх користувачів у потрібному напрямку колективної думки, нав'язуючи певні ідеї та правила щодо функціонування держави [21, с. 85-86].

Не секрет, що соціальні мережі можуть виконувати роль не лише знаряддя впливу, але й платформи для збору інформації. Користувачі не звертаючи зайвий раз уваги – самостійно надають певні особисті дані, дані про життя та стають незахищеними перед майбутніми зловмисниками. З іншого боку, соціальні мережі можуть бути знаряддям і допомогою для організаторів революцій та переворотів.

Серед нещодавніх ситуацій, варто відзначити значний вплив соціальних мереж на громадську думку в умовах війни РФ та Грузії в серпні 2008 року. Висвітлення інформації щодо цієї війни в російськомовній частині соціальних мереж назвали першою війною у соціальних мережах, в інформаційному просторі [24, с. 22].

Яскравим прикладом впливу соціальних медіа на політичні процеси є президентські вибори в Сполучених Штатах Америки 2016 року. Ця виборча кампанія продемонструвала, як цифрові платформи можуть маніпулювати громадською думкою та підривати демократичні процеси. Соціальні мережі

стали важливими майданчиками для інформаційних атак, де різні політичні сили активно просували свої погляди, дискредитували опонентів і маніпулювали емоціями виборців.

Також можемо згадати ситуацію, як росія активно впливала на користувачів соціальних мереж та поширювала власні прокремлівські ідеї, впливаючи на свідомість людей. Крім того, російські «хакери» активно застосовували ботів для маніпуляцій суспільною думкою, особливо під час військових та гібридних конфліктів, зокрема під час анексії Криму, військової агресії на сході України у 2014 році, втручання в сирійський конфлікт, а також повномасштабного вторгнення на територію України в лютому 2022 року.

Розвиток соціальних медіа в Україні став особливо помітним у період 2014–2015 років, коли активну роль почали відігравати онлайн-спільноти громадських організацій, волонтерів, активістів, політиків та професіоналів. Ці ресурси стали важливим джерелом інформації під час таких подій, як Революція Гідності, анексія Криму та початок військових дій на Донбасі, і закріпилися як серйозна альтернатива традиційним засобам масової інформації та телебаченню [2].

Соціальні медіа дуже сильно впливають на політичну активність громадян і це має суттєві наслідки для демократії. Як вже казали раніше – поширення неправдивої інформації сприяє політичній дезорієнтації суспільства, коли воно поділяється на протилежні табори, що ускладнює можливість вести конструктивний діалог і досягати компромісу.

Будь-яка інформація в спільнотах здатна впливати на зацікавленість громадян у політичному житті, а також на формування їхніх політичних уподобань, що особливо проявляється під час виборчих кампаній [15, с. 126].

Вперше роль соціальних медіа в політичних процесах була помітна під час президентських виборів у США 2008 року. Цей інформаційно-політичний досвід у використані соціальних мереж під час виборчої кампанії Барака Обами у 2008 році значною мірою вплинув на виборчу кампанію Володимира Зеленського в

Україні у 2019 році, де участь соціальних медіа була також активно задіяна [8, с. 78].

Загалом, варто відзначити, що сьогодні соціальні медіа відіграють значно більшу роль у сучасній політиці, ніж це було раніше. Вони дають можливість політичним діячам, кандидатам у партії, на пост Президента спілкуватися з виборцями, поширювати інформацію про свою діяльність та позицію, мобілізувати виборців. Соціальні мережі стали своєрідним посередником між політиками та народом, де каналом зв'язку виступатимуть офіційні сторінки у соціальних мережах політиків та органів влади, на яких публікуються пости з описом їх основних позицій. Така робота політичних діячів у мережах позитивно позначається на їх іміджі та робить їх «ближчими до народу», встановлюючи більш близьку взаємодію. Варто пам'ятати, що більшість повідомлень, що викладаються на таких сторінках мають за мету змінити думку читача, вплинути на його погляди, а не проінформувати людей [21, с. 89-90].

У висновку хочеться зазначити, що соціальні мережі набувають великої популярності, кількість їх користувачів зростає постійно. Цей є неминуче у нашому сучасному глобалізованому інформаційному середовищі. Завдяки значній кількості прихильників та їх різносторонності соціальні мережі можуть слугувати інструментом ведення інформаційної війни та маніпулювання задля досягнення впливу на думку громадськості. Однак, при величезній кількості негативних характеристик використання нових можливостей передачі інформації, соціальним мережах притаманні й позитивні відгуки їх функціонування. З їх допомогою можливо істотно підвищити ефективність громадської організації, сприяючи виникненню поняття «громадянське суспільство» на практиці.

Нові форми взаємодії держави та суспільства передбачають створення інститутів та громадських організацій, що забезпечуватимуть приріст соціального капіталу учасників комунікацій. Негативні чинники впливу мереж на свідомість людини

сьогодні переважають, що породжує потребу захисту користувача та безпеку інформації в інформаційному просторі.

2.3. Зусилля держави в боротьбі з дезінформацією

Не секрет, що саме Інтернет є простором свободи. Всі бажаючі можуть оприлюднити будь-що будь-якої миті і зробити доступним для всіх інших людей у світі. З одного боку, тепер легко дізнатися про все на світі лише за одну секунду. Але це має іншу негативну сторону – неправдива інформація легко розпалює ненависть між групами людей, тобто дезінформація через соціальні мережі має згубний вплив.

Дезінформація - це всі форми неправдивої, неточної чи недостовірної інформації, створеної, поданої і розповсюдженої з метою цілеспрямованого нанесення шкоди чи здобуття вигоди. Вона впливає на громадян, включно з маніпулятивною чи відверто неправдивою інформацією, становить серйозний виклик для Європи і світу [23, с. 163].

Дезінформація здатна послабити довіру до ЗМІ, завдати шкоди нашим демократіям, обмежуити здатність громадян робити поінформований вибір, часто підтримує радикальні й екстремістські ідеї та дії. Масові онлайн-кампанії з дезінформації широко використовуються недобросовісними сторонами для сіяння недовіри і провокування напруженості у суспільстві, із серйозними потенційними наслідками для еволюції націй, Європи і всього світу.

Зростання дезінформації і серйозність її загрози стали причинами підвищення обізнаності й занепокоєнь у громадянському суспільстві серед країн-членів ЄС і на міжнародному рівні. Цілеспрямована дезінформація з метою впливу на вибори і міграційну політику були двома основними категоріями, які можуть завдати шкоди суспільствам. Іншими сферами є охорона здоров’я, навколишнє середовище. [25, с. 114].

Наразі, відбуваються неприємні зміни в суспільстві: зменшення довіри громадськості до ЗМІ, зниження стандартів мас-медіа, складнощі у пошуку чесних журналістів та велике зростання кількості “фейкових” новин. Зараз державна політика у сфері інформаційного забезпечення спрямована на те, щоб протидіяти неправдивим даним та просунути медіа-грамотність серед населення.

Отже, можна дійти висновку, що в сучасному інформаційному просторі, дезінформація є серйозною загрозою для національної безпеки, суспільної стабільності та демократичних процесів. Вона поширюється через соціальні мережі, новинні платформи та різні канали комунікації, що значно ускладнює її виявлення та протидію. Держава відіграє ключову роль у боротьбі з дезінформацією, використовуючи правові, технологічні та просвітницькі методи. Проте, ефективність державних заходів залежить від їх збалансованості: важливо забезпечити захист інформаційного простору без порушення свободи слова. Отже, боротьба з дезінформацією потребує комплексного підходу, що поєднує жорстку політику щодо маніпулятивного контенту з активною просвітницькою роботою серед населення.

РОЗДІЛ 3. НЕБЕЗПЕКА ПІД ЧАС ІНФОРМАЦІЙНОЇ ВІЙНИ

3.1. Класифікація небезпек та загроз в інфо-середовищі

Інформаційна система часто піддається атакам, небезпекам, тож в цьому розділі розглянемо види загроз інформаційній безпеці, як з ними боротися та їм протидіяти. Згідно із Законом України “Про основи національної безпеки України”, до загроз національним інтересам і національній безпеці в інформаційній сфері відносять такі: прояви обмеження свободи слова та доступу громадян до інформації; розповсюдження насильства, порнографії, жорстокості; комп’ютерна злочинність та тероризм; розголошення державної таємниці інформації, а також конфіденційної інформації, яка була спрямована на забезпечення потреб та національних інтересів суспільства і держави; спроби маніпулювати суспільною свідомістю, шляхом поширення недостовірної, неповної або упередженої інформації [23].

Які з існують способи впливу на інформацію або шляхи реалізації загроз?

Професор В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації, тобто:

1) за джерелами походження: природного походження, антропогенного походження; техногенного походження;

2) за ступенем гіпотетичної шкоди: загроза та небезпека;

3) за частотою повторення: повторювані та продовжувані;

4) за ймовірністю реалізації: вірогідні, неможливі, випадкові;

5) за сферами походження: екзогенні та ендогенні;

6) за характером реалізації: реальні, потенційні, здійснені, уявні;

7) за значенням: допустимі та неприпустимі; за рівнем детермінізму: закономірні та випадкові;

8) за структурою впливу: системні, структурні та елементні;

9) за ставленням до них: об’єктивні та суб’єктивні;

10) за об’єктом впливу – особа; суспільство; держава [13].

Схожі погляди стосовно загроз інформаційній безпеці має науковець : А. Логінов та виклав їх у своєму дисертаційному дослідженні. Зокрема, вчений визначає такі загрози:

– розкриття інформаційних ресурсів;

– порушення цілісності інформаційних ресурсів;

– збій у роботі обладнання [14].

Щодо Б. Кузьменка та О. Чайковської, ті пропонують класифікацію загроз, яка базується на визначенні властивостей інформації:

– загрози порушення конфіденційності інформації, в результаті реалізації яких інформація стає доступною суб’єкту, що не має повноважень для ознайомлення з нею;

– загрози порушення цілісності інформації (будь-яке зловмисне спотворення інформації, оброблювана за допомогою автоматизованих систем);

– загрози порушення доступності інформації, які виникають при умовах, коли доступ до певного ресурсу автоматизованих систем для легальних користувачів блокується [10, с. 6-7].

Вчені С. Гуцу [4] та О. Литвиненко [11] сходяться у поглядах на тому, що основні загрози інформаційній безпеці можна представити у такому вигляді:

– загрози впливу неякісної інформації (фальшивої, недостовірної, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво інформації, пошук, одержання, її розповсюдження, передавання та використання; праву на інтелектуальну власність на інформацію, зокрема, і речову).

Ми можемо підтвердити той факт, що інформаційна безпека не полягає тільки у захисті інформації. Це набагато ширше поняття. Так, суб'єкт інформаційних відносин може постраждати (отримати матеріальні і/або моральні збитки) від несанкціонованого доступу до інформації [1, с. 20].

Інформаційна система збільшується щосекунди, тож і ризики проникнення невідомих користувачів до неї теж збільшуються. На разі, будь-хто може отримати доступ до даних, що зберігаються в Інтернеті, або створити свій власний веб-ресурс. Ці особливості глобальної мережі надають зловмисникам можливість скоєння злочинів в соцмережах, викривляти дані, інформацію, ускладнюючи їх виявлення й покарання. Зловмисники розміщують шкідливі програми на веб-ресурсах, «маскують» їх під щось корисне та легкодоступне, достовірне. Тому зараз є важливою місією не дати витекти даним, запобігти небезпеці, уникнути можливих загроз.

Почнемо із визначення поняття загрози інформаційної безпеки — це сукупність факторів та умов, які руйнують стабільність, безпеку та утворюють порушення інформаційної безпеки.

Під інформаційною безпекою розуміють захищеність даних та інфраструктури від будь-яких навмисних або випадкових дій, результатом яких може стати пошкодження даних, нанести збитків їхнім власникам або інфраструктурі, що підтримує інформаційну безпеку [48, с.176].

Стандартною моделлю безпеки даних слугує модель із трьох категорій :

1. Конфіденційність — стан даних, за якого доступ до них здійснюють тільки ті особи, що мають на нього право. З цього виходить, що є загроза конфіденційності і вона полягає в тому, що дані оприлюднюють та інші люди можуть отримати

доступ до них, хоча такого права не мають. Дана небезпека виникає тоді, коли отримано доступ до деяких секретних даних, що зберігаються в комп'ютерній системі чи передаються від однієї системи до іншої.

2. Цілісність — уникнення несанкціонованої зміни даних та існування даних у неспотвореному вигляді. Порушення цілісності передбачає будь-яку умисну зміну даних, що зберігаються в комп'ютерній системі чи передаються з однієї системи в іншу. Вона виникає, коли зловмисники навмисно змінюють дані, тобто порушується їхня цілісність. Цілісність даних може бути пошкодженою внаслідок випадкової помилки програмного або апаратного забезпечення [37, с.212].

Небезпечними діями для інформаційної системи також є цілеспрямована крадіжка або знищення даних на робочій станції чи сервері; пошкодження даних користувачами в результаті необережних дій. Такі дії може виконувати хакер - кваліфікований ІТ-фахівець, який чудово розуміється на комп'ютерних системах і втручається в роботу комп'ютера без дозволу та може дізнатися деякі особисті відомості або пошкодити дані, що зберігаються в комп'ютері. Їхні мотиви можуть бути різними: помста, задля розваги, за винагороду. Людина «хакер» по суті є мережевим зломщиком, розробником комп'ютерних вірусів й інших кіберзлочинів. У багатьох країнах злом комп'ютерних систем, викрадання інформаційних даних, створення та поширення комп'ютерних вірусів карається законом [42, с. 20].

На інформаційну безпеку системи даних можуть впливати різноманітні зовнішні чинники — «природні» загрози – неправильне зберігання документів може привести до втрати даних, часто також відбуваються крадіжки комп'ютерів і носіїв, форс- мажорні обставини тощо.

Таким чином, у сучасних умовах наявність розвиненої системи інформаційної безпеки стає однією з найважливіших умов конкурентоздатності й навіть життєздатності будь-якої організації.

Загрози є абсолютно різні та їх зараз у сучасному світі дуже багато, що відтепер стали їх класифікувати за різними ознаками:

1. За спрямованим напрямком самої загрози:

Загрози порушення конфіденційності - інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Це відбувається тоді, коли отримано доступ до обмеженої, прихованої інформації, яка зберегалася в комп'ютерній системі або передавалася від однієї системи до іншої. У таких випадках часто використовують термін «витік». Подібні загрози можуть виникати внаслідок збоїв роботи програмних та апаратних засобів, хакерських атак та взлому іншими користувачами.

2. Загрози цілісності - це небезпечні дії, які пов'язані з модифікацією тієї чи іншої інформації, що зберігається в інформаційній системі. Такі види порушень цілісності можуть бути викликані різними чинниками — від умисних дій персоналу до пошкодження обладнання.

3. Загрози доступності – це здійснення дій, які певним чином перешкоджають або ускладнюють доступ до ресурсів інформаційної системи. У таких випадках, доступ до послуги або інформації блокують і почати знову користуватися даними можливо лише за певний час, який не забезпечить виконання тих чи інших бізнес-цілей [40, с. 319-320].

За розташуванням виділяють наступні джерела загроз:

Зовнішні (джерела загроз розташовані поза системою);

Внутрішні (джерела загроз всередині системи).

За розмірами нанесеного збитку:

Загальні – це наприклад, нанесення збитку об'єкту безпеки в цілому, заподіяння значної шкоди). Ще один приклад : ситуація з вірусом «I love you», що став

причиною пошкодження комп'ютерних систем у багатьох містах світу, і завдав загального збитку біля 100 мільйонів доларів США

Локальні – це загрози, які заподіяли шкоди окремим частинам об'єкту безпеки.

Приватні загрози – це заподіяння шкоди окремим властивостям елементів об'єкта безпеки. Чудовий приклад - це гучний «касетний скандал» [41, с. 365].

За природою виникнення:

Природні (об'єктивні) – це загрози, що викликані впливом на інформаційне середовище фізичних процесів або стихійних природних явищ, що не залежать від роботи людини;

Штучні (суб'єктивні) є викликані впливом на інформаційну сферу людини. Штучні також поділяють на :

Випадкові, або ненавмисні погрози – це можуть бути помилки програмного забезпечення, збої в роботі систем, «людський фактор», відмови обчислювальної та комунікаційної техніки;

Навмисні (умисні) загрози — неправомірний доступ до інформації, розробка спеціального програмного забезпечення, використовуваного для здійснення неправомірного доступу, розробка та поширення вірусних програм і т. д. Навмисні загрози зумовлені діями людей і вони є головною причиною злочинів і правопорушень [40, с.148-149].

Фахівці провели аналіз з інформаційної безпеки досліджень та з’ясували, що понад 65 % шкоди, що наноситься інформаційним ресурсам, є наслідком ненавмисних помилок. Тож, варто звернути увагу на ефективнішому впровадженні комп'ютерних систем для забезпечення безпеки. Так, Національним інститутом стратегічних досліджень була запропонована програма «Електронна Україна».

Ризики небезпеки несуть співробітники спецслужб, які, маючи доступ до секретної інформації з певних причин, тобто навмисно роблять інформацію

загальнодоступною. Був один випадок, коли колишній генерал СБУ, один з керівників ГУР України Валерій Кравченко у лютому 2004 року, маючи доступ до секретних матеріалів, безпідставно розповсюдив їх, зокрема журналістам французьких ЗМІ [37].

Носіями небезпеки та нести загрозу можуть: конкуренти, злочинці, корупціонери, адміністративно-управлінські органи.

3.2. Фейки та їх розповсюдження

З того моменту, як людина почала отримувати, зберігати та передавати інформацію іншим, з’явився термін під назвою "дезінформація" , що трактується як окремий вид брехні. Метою є поширення неправдивої інформації для досягнення певних цілей.

З давніх часів дезінформація була невід’ємною частиною боротьби за владу та широко використовувалася під час збройних конфліктів. Саме софісти — професійні ритори, були першими, хто навчав мистецтву переконання, часто використовували логічні викривлення, аби довести навіть неправдиві тези. Вони рахували, що істина відносна, тому головне — переконати слухачів, а не шукати правду.

У Афінах політики та полководці часто використовували емоційні виступи на народних зборах для тиску та зміни думок громадян. Наприклад, Перікл під час Пелопоннеської війни зображував Афіни як “оплот свободи”, а Спарту — як тиранію, щоб підтримати бойовий дух.

Міфологія була незмінним ідеологічним інструментом. Наприклад, походження афінян від богині Афіни підвищувало їхню силу, могутність та політичне домінування. Таким чином формувалися національні гасла, що виправдовували політичні дії або війни. Такі прийоми також використовував Октавіан проти Марка Антонія у битві за владу та спадок Цезаря [14, с. 71].

Прикладом є також маніпуляція громадською думкою під час Великої французької революції та ще багато прикладів.

Пізніше, ставало складніше, адже з’явилася та стрімко розвивалася друкована преса й почалася нова боротьба – за унікальність, новизну інформації та рейтинги видання. Наприкінці XIX століття конкурентоспроможні видавці газет Джозеф Пулітцер та Вільям Герст змагалися за аудиторію, застосовуючи маніпуляції із новинами, гонитву за сенсаціями та політичну пропаганду. Велика кількість нової зацікавленої аудиторії закріпила остаточне позиціонування преси як ще одного каналу для можливого розповсюдження маніпуляції [7, с. 123].

Під час Другої світової війни, завдяки медіа підтримці використовувалися новини - як один із найуспішніших методів боротьби. Кожна сторона конфлікту активно використовувала плакати, кіно, радіо, пресу для формування потрібних настроїв. У нацистській Німеччині Йозеф Геббельс, міністр пропаганди, створив систему тотального інформаційного контролю. Пропаганда зображувала Гітлера як “рятівника народу”, ворогів — як “деградованих”, а поразки — як тимчасові “тактичні відступи”.

Союзники активно застосовували операції з обману противника, наприклад:

1. Операція “Мінсміт” (1943): підкинуте тіло з підробленими документами, для переконання німців у нападі на Грецію, а не Сицилію.

2. Операція “Фортитьюд” (1944): створення фальшивої армії під командуванням генерала Паттона для введення німців в оману щодо місця висадки в Нормандії.

3. У відповідь на бомбардування Великої Британії у 1940 році уряд запустив "Кампанію гніву", як інструмент інформаційної війни проти нацизму.

В усіх пропагандистських кампаніях використовували образ ворога, який уособлював зло. У радянській пропаганді німці зображувалися як “фашистські звірі”, у західній — Гітлер як “божевільний диктатор”, у німецькій — союзники як “загроза європейській культурі” [56, с. 45-46].

Радіопередачі, листи з фронту, навіть повідомлення про втрати піддавалися цензурі, щоб не знижувати бойовий дух.

Із створенням інтернету почали з'являтися та поширюватися різні види онлайн-новин та соціальних мереж. Саме соціальні мережі стали платформою для розповсюдження дезінформації.

Поговоримо про фейки під час російсько-української війни та їх активне поширення в інформаційному просторі. росія роками поширювала дезінформацію не лише в українському інформаційному просторі, але і за кордоном: трансляція своїх каналів та залучення «іноземних фахівців», які говорили потрібний текст.

Це відбувалося й до, і під час повномасштабного вторгнення й далі росія продовжує здійснювати інформаційні кампанії для пригнічення України.

Ще в 2014 року росія поширює фальшиві твердження про нацизм в Україні. Для цього росіяни використовують як і пропагандистські ресурси, так і так званих «експертів». Вони називали нацистськими всі добровольчі формування в Україні. Згодом почали звинувачувати українську владу в нацизмі, зокрема й Володимира Зеленського. Керівник російського МЗС Сергій Лавров звинуватив Зеленського у тому, що той нібито надає свою охорону «нацистам для проведення смолоскипних маршів», а речниця МЗС РФ Марія Захарова заявила, що Зеленський «ось-ось визнає свої нацистські погляди».

Ці заяви є спробами дискредитувати вище військово-політичне командування України в очах західного суспільства, а для російського суспільства байка про нацизм в Україні є виправданням війни [47, с.155].

Ще одним фейком, який росія використовує як виправдання агресії, є нібито заборона російської мови в Україні. Цю тезу використовують ще з 2014 року, наче російськомовні жителі Східної частини «потребують захисту». У своїй пропаганді росіяни орієнтуються на закон «Про забезпечення функціонування української мови як державної», який Верховна Рада прийняла у квітні 2019

року. Зокрема, закон передбачає, що державною мовою в Україні є лише українська, однак російська не забороняється на індивідуальному рівні.

У країні-агресора цей закон схарактеризували таким, що забороняє російську мову. Однак слово «заборона» жодного разу не зустрічається у тексті Закону, тоді як «захист» — десятки разів.

Ще з 2014 року росія блокує проведення гуманітарних коридорів зі сходу України. У 2014-2015 роках це стосувалося виведення українських військ. Зокрема, наприкінці серпня 2014 році росіяни зірвали «зелений коридор» для військових поблизу Іловайська на Донеччині та вбили 366 людей, 429 отримали поранення, ще 300 — потрапили в полон [51, с. 163].

На початку повномасштабного вторгнення між Україною та росією були певні домовленості щодо гуманітарних коридорів для евакуації цивільного населення з тимчасово окупованих територій. Російська сторона їх зривала. Міністерка з питань реінтеграції тимчасово окупованих територій Ірина Верещук в червні говорила, що з понад трьохсот гуманітарних коридорів, які мали б відбутися, запрацювали лише 160. В той час російські пропагандистські ЗМІ писали, що Україна не евакуює своїх громадян або проводить евакуацію лише іноземців. Зокрема, на початку березня російські видання розповсюджували інформацію, що Україна нібито вивозить із Сум іноземних студентів, а місцевих мешканців не підпускає до автобусів. Про те, що ці заяви не відповідають дійсності, писали «STOP Fake».

Крім цього, росіяни обстрілюють гуманітарні колони, які направляють міжнародні організації до тимчасово окупованих територій чи територій, на яких ведуться бойові дії. Зокрема, ще до початку повномасштабного вторгнення, у лютому 2022 року, гуманітарний конвой Червоного Хреста потрапив під обстріл на Луганщині. А 9 березня росіяни обстріляли гуманітарну колону, яка рухалася до Маріуполя [51, с. 207].

У березні 2022 року росіяни поширили у своїх медіа, що в Маріуполі українські війська використовували житлові будинки як прикриття та обстрілювали мирних мешканців. Подібні фейки поширювали й щодо інших міст, де ведуться бойові дії або які розташовані близько до лінії фронту.

У жовтні російська пропагандистська інформагенція «РІА Новини» заявила, що Україна готує підрив «брудної бомби». Цю інформацію їм надали «джерела, що заслуговують на довіру». Одразу після цього очільник російського міноборони Сергій Шойгу зателефонував колегам з Франції, Великої Британії, Туреччини та США, щоб повідомити про це. Своєю чергою міністри оборони цих країн заявили, що інформація є брехнею. Тоді Росія скликала Раду Безпеки ООН, однак представниця Великої Британії назвала це засідання «гаянням часу».

В Інституті вивчення війни зауважили, що росія використовує ці заяви, щоб уповільнити постачання зброї. А міністр закордонних справ Дмитро Кулеба сказав, що «росіяни часто звинувачують інших у тому, що планують самі».

Стосовно поширення фейків закордоном, то з 2016 року, після інциденту між Дональдом Трампом та виданнями The New York Times і The Washington Post, популярність фрази "фейкові новини" значно зросла. Його часто використовують для опису речей, які не є однаковими, включаючи брехню, чутки, обман, дезінформацію, змови та пропаганду. Насправді, більшість інформації, яка поширюється зараз, не зовсім фальшива і це вводить в оману. Замість повністю сфабрикованих новин, агенти впливу переробляють справжній вміст та використовують гіперболічні заголовки, з'єднуючи достовірні факти із вигаданими темами або людьми.

Щоб захиститися від дезінформації, варто навчитися виявляти дезінформацію та серйозно ставитися до контенту, який є в соціальних мережах. Зазвичай дезінформація створена для маніпуляцій емоціями, через що сприймається гостріше і болючіше, ніж "сухі" факти. На жаль, споживання інформації через

призму емоцій призводить до того, що у користувача блокується критичне мислення.

У боротьбі між допитливим пошуком першоджерела і бажанням якнайшвидше поділитися "сенсаційною", але не факт що достовірною новиною, перемагає останнє. Ось чому фейкові новини часто стають вірусними. Аби не потрапити у пастку дезінформації, варто досліджувати джерела новин, а також звертати увагу на якість подання інформації. Щоб розуміти яким чином ЗМІ і соціальні мережі можуть маніпулювати свідомістю, щоб не стати жертвою цього процесу –чудово було б пройти курси з медіаграмотності [14, с. 210].

Отже, аналізуючи всю вище наведену інформацію, можна дійти висновку, що фейки створюються з метою ввести людей в оману, маніпулювати їхніми емоціями або змінити погляди й поведінку. Найчастіше фейки поширюються у соціальних мережах, спільнотах та групах, де користувачі можуть пересилати цю інформацію друзям, рідним і таким чином поширювати неправдиві дані.

З початку повномасштабного вторгнення росії в Україну, в Інтернеті активно ведеться інформаційна війна. Основна її ціль — деморалізувати українців, зменшити силу, психологічно вплинути на людей : посіяти паніку, навести страх та заплутати.

Щоб розпізнати фейк, треба :

1) перевіряти джерело — офіційні сторінки урядових структур, ЗСУ, ОП, Міністерства оборони;

2) звертати увагу на дату — часто фейки використовують старі матеріали;

3) порівнювати інформацію з кількох незалежних джерел.

РОЗДІЛ 4. ПОВНОМАСШТАБНЕ ВТОРГНЕННЯ РОСІЇ В УКРАЇНУ ТА ЗМІНИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

4.1. Вплив РФ на українську інформаційну систему

Не секрет, що в сучасних умовах інформаційна війна є одним з вирішальних факторів перемоги. Наразі, це дуже важливо для України, яка веде боротьбу проти ядерної держави з переважаючим військовим потенціалом. Рівень політичної підтримки, обсяги допомоги та масштаби запроваджених проти агресора санкцій напряму залежать від того, як ці події в Україні сприймають за кордоном.

За об'єктивними даними можемо сказати , що перший раунд інформаційного протистояння протягом 50 днів війни виграла Україна. Українська інформаційна система виявилася високого рівня, завдяки злагодженій співпраці Офісу президента, Міноборони, МЗС та українських журналістів. Ми ще раз довели нашу готовність і вміння відстоювати чітку позицію у світових ЗМІ, натомість з боку росії побачили лише поширення неправдивої інформації[11].

Росія – агресор, який веде нечесну боротьбу. Деякі дослідники пояснюють такі варварські дії росії тим, що США послідовно підштовхували Україну до членства в НАТО й тим самим спричинили «протидію» з боку росії.

Проти тих держав, які підтримують вступ України в ООН, росія навіть відкрила додатковий інформаційно-дипломатичнй фронт та публічно звинувачує ті держави у помсті, не дає жодній з них висловити свою позицію, а також безпідставно застосовує право вето лише з міркувань помсти.

Саме таким чином, наприклад, Росія повела себе відповідно до Колумбії, яка одна з небагатьох держав Латинської Америки (якщо не єдина) відкрито підтримала Україну. Отже, у цьому випадку бачимо старі методи використання кампаній дезінформації [5, с. 194].

Врешті решт, аналіз міжнародного інформаційного поля говорить про значну кількість російських за своїм походженням і проплачених Російською Федерацією авторів та журналістів, які за час правління Путіна змогли закріпитися у міжнародних інформаційних агентствах.

Інформаційна війна в сучасних умовах — це частина гібридної війни, тобто такої, що поєднує традиційні бойові дії з інформаційними операціями, застосовуючи економічний тиск, кібератаки, політична дестабілізація та психологічна війна. росія ще з 2014 року вдається до всіх можливих інструментів агресії проти України, зокрема до впливу на громадську думку. Тож ефективне протистояння в інформаційній війні стане складником нашої перемоги. Від того, як за кордоном сприймають події в Україні, залежить і рівень політичної підтримки, і обсяги допомоги [3].

Складно оцінити точні витрати Росії на інформаційну війну проти України, оскільки інформація про бюджет доволі засекречена. Згідно оцінок Міжнародного центру перспективних досліджень, щороку на інформаційну війну на Заході проти України витрати Росії досягають 4 мільярдів доларів. Одночасно, за даними української розвідки, Росія мала в планах витратити 1,5 мільярда доларів тільки на дестабілізацію України навесні 2024 року.

Ще у 2013–2014 роках, Росія готувалася до агресії. З початку повномасштабного вторгнення змінилися тільки, мабуть, кількість і тональність російської пропаганди.

У 2013–2014 роках російська пропаганда намагалася розгойдати в нас конфлікти і тим самим виправдати своє того часу вторгнення. Ці ж зусилля ми бачили протягом 2021 року й на початку 2022-го. На початку вони прагнули виправдати своє вторгнення, розповідали різні нісенітниці. Досі залишається велика кількість закликів бомбувати Україну, знищувати нашу інфраструктуру, бомбити електростанції тощо.

На прикладі Криму та Донеччини, ми бачимо, що в людей, які користувались російськими новинами, було викривлене уявлення про війну, з якою прийшла росія на українські землі. Вони справді вважали, що українці прагнуть їх знищити, убити, заборонити їм розмовляти на російській мові, і, саме тому, росія їм допомагає визволитися. З часом, багато людей зрозуміло, що це все неправда, проте, на жаль, уже було пізно. Аби таких необізнаних людей було менше на нашій території, ми прагнемо їм пояснити, хто і з якою метою намагається їх обманути [19, с. 26].

Сучасні українські медіа-компанії мають на меті :

– підвищити якість контенту українських медіа;

– поширити медіаграмотність серед українців;

– протистояти дезінформації.

Отже, як висновок можна зазначити наступне - українські журналісти та програмісти від початку повномасштабного вторгнення російських військ на територію України, активно працюють задля покращення інформаційного фронту. Саме ці, вище перераховані організації, щоденно ведуть боротьбу проти дезінформації, аби українці завжди могли отримати правдиву новину, без перебільшень, вигадок та фейків. Українцям варто вміти фільтрувати отриману інформацію, тобто коли находять підозрілі повідомлення – обов’язково перевіряємо їх. Я впевнена, що кожен з нас хоче, аби брехня й пропаганда не існували в нашому житті тому дотримуємося наступних правил : користуватися лише перевіреними та офіційними джерелами; намагатися критично мислити і аналізувати та перевіряти підозрілу інформацію; заблокувати російський контент.

4.2. Гібридна війна та застосування інформаційної зброї

Слід зазначити , що за останні роки російсько-український конфлікт зазнав глибокого і довгострокового характеру і призвів до значних змін у відносинах Києва і Москви. Не секрет, що російська агресія завдала Україні кардинальних економічних, людських, територіальних втрат.

Російсько-українська «гібридна» війна є першим таким масштабним конфліктом. Агресія Кремля несе не лише грозу державності та суверенітету України, а й єдності ЄС і в цілому. Тому вкрай важливим є пошук ефективних відповідей, створення спільної політики протидії російському вторгненню.

Зазначимо, що ця «гібридна» агресія Росії не є новацією Кремля, але, саме на українському напрямі російський режим використовує майже весь арсенал «гібридних» воєн, починаючи з прямої збройної агресії і закінчуючи комплексом економічних, енергетичних, інформаційних та інших засобів розгойдування країни зсередини. Серед них — шпигунство, інформаційні диверсії, дискредитація державних структур, експорт корупції, підтримка деструктивних сил активно застосовується проти європейських країн [33, с. 147].

Яка ціль війни?

Цілями у війні росії з Україною є створення перешкод європейському та євроатлантичному курсу України, руйнування української державності, повернення Росії у сферу впливу. Стосовно ЄС, то для Кремля за основу є зруйнувати єдність європейського співтовариства, заплямувати його базові цінності, посилити вплив і контроль РФ над процесами на континенті, зафіксувати порядок та новий устрій в Європі за російським сценарієм.

Якщо проаналізувати цілі, які переслідує Кремль, можна зробити такі висновки : по-перше, не допустити членства в ЄС і НАТО країн, які створені на теренах колишнього СРСР — Грузії, Молдови та України в першу чергу. По-друге, знищити євроатлантичну та європейську єдність і здобути залежні від Москви режими в більшій кількості європейських країн [14].

Щодо програми максимум — вийти на зразок «Ялти-2», під час якої задовольнити сучасний поділ світу на зони впливу, як, наприклад , це було після Другої світової, і що, як результат, призвело до холодної війни. З огляду на це і збільшуються ставки у великій геополітичній грі через залучення Росії в сирійську авантюру. За результами агресії, і це очевидно, після шести років війни Росії проти України, понад 7 % території нашої держави опинилися під окупацією, отже, демократія європейського зразка виявилася надзвичайно уразливою перед євразійською дикою експансією.

Стратегічні завдання російської гібридної агресії – послідовне руйнування базових європейських цінностей, які об'єднують країни ЄС, створення хаосу, формування впливової проросійської думки в європейському колі, підтримка та просування розбіжностей між європейськими державами. Отже, наразі йдеться вже не про відсіч європейського впливу на пострадянському просторі, а про здійснення масштабної гібридної експансії саме на території ЄС, щоб максимально послабити і поділити Європейський Союз, мінімізувати американську присутність на континенті, змінити за російським сценарієм вже усталений європейський політичний устрій [19, с. 58-60].

Слід зазначити, що «гібридна» війна – це особливий тип збройного конфлікту, в якому бойові дії займають другорядну роль. Її мета полягає через застосування різних видів сили, створюючи економічний та психологічний тиск на людей. Варто зазначити, що росія була не першою державою, яка застосувала «гібридну» війну проти інших країн, а Україна — не першою жертвою «гібридної» війни. Ще задовго до того, як вперше з'явилася відповідна термінологія, спостерігались різні прояви «гібридної» війни та загроз. Проте, російська агресія (має «гібридний» характер) проти України швидко популяризувала ідею «гібридних» воєн, зокрема, у тих країнах, які усвідомлюють загрозу національній безпеці з боку Кремля.

Розглянемо етапи типової гібридної війни:

1. Підготовчий (вжиття заходів з формування політичних, ідеологічних та військових передумов майбутньої агресії).
2. Активний (введення прихованої агресії проти обраної країни заради безпосереднього втілення поставлених цілей).
3. Заключний (закріплення своїх позицій в країні, що є об'єктом агресії).

Розглянемо особливості російській «гібридній» агресії проти України :

з лютого 2014 р. в центрі Європи починається війна. Так, з самого початку захоплення перших адміністративних будівель – це війна, згідно з нормами міжнародного права, незважаючи на те, що деякі її називали «спецоперація Росії з анексії Криму та Севастополя, а також на Сході України.

Ця війна призвела до того, що росія поставила себе поза міжнародним правом і цивілізованими рамками міжнародного життя. І чим далі тягнеться ця війна, тим більше міжнародних організацій та окремих держав усвідомлюють справжню катастрофу, яка утворилася в результаті російської агресії [50, с. 100].

Слід наголосити, що «гібридна» війна проти України підтвердила також відсутність дієвості міжнародних глобальних і регіональних безпекових інститутів (ООН, ОБСЄ, ЄС, Ради Європи, СНД) у врегулюванні міжнародних конфліктів і локальних воєн та, як результат, спостерігаємо втрату ними міжнародного авторитету. Багато особливостей та новітніх підходів Росії у військовій сфері виявив конфлікт на Сході України [42, с. 22].

Яку мету несе руйнування української державності?

По-перше, продемонструвати своїм громадянам катастрофічні наслідки будь-якої активності та гарантувати йому підтримку «сильної руки»;

По-друге, створити для внутрішньої аудиторії образ ворога в особі українського націоналізму та західного експансіонізму, який його підтримує;

По-третє, знешкодити загрозу внутрішньої опозиції В. Путіну — як ліберальної, так і націоналістичної;

По-четверте, перехопити геополітичну ініціативу у Заходу, який зазнав кризу тотожності та політичної спроможності.

Вкотре українсько-російський конфлікт показав, що будь-яку країну, навіть європейську, можна розхитати і довести до межі розпаду. І, навпаки, відбудувати цілісність і стабільність країни, яка стала жертвою «гібридної» агресії - дуже важке завдання та вимагає неабияких зусиль майже всього світового співтовариства [41, с. 322].

Війна на Донбасі стала класичним прикладом «гібридної» війни, що характеризується використанням місцевих кримінальних груп, нерегулярних збройних формувань, а також регулярних збройних сил Росії. Крім того, Кремль офіційно спростовує свою участь у збройному конфлікті та не несе формально правової відповідальності за агресію проти України.

Отже, збройний конфлікт на Донбасі є класичним проявом «гібридної» війни, яка може спонукати досліджувати цей сучасний феномен та сприяти збільшенню міжнародних зусиль щодо його протидії. Варто наголосити, що «гібридні» війни Росії застосовують багато інструментів, починаючи від розповсюдження панічних чуток до мобілізації потенціалу церкви, політичних органах чи застосування так званої м'якої сили.

Особливістю російсько-української війни стало також ефективне використання меметичної зброї. Меметична війна може розглядатися як цифрова версія психологічної війни, більш відомої, як пропаганда. Якщо пропаганда і громадська дипломатія є традиційними формами меметічної війни, тоді тролінг і психологічні операції — її партизанські версії. Меметична зброя і війни, які чиняться за її допомогою є окремим випадком сучасних технологій і є різновидом операцій, що відносяться до сфери мережевих війн.

Меметічна зброя застосовується в соціальних мережах, флешмобах, блогах для виробництва і поширення мемів. Вона діє тут і зараз дуже ефективно. За допомогою меметічної зброї, тобто із застосуванням всіх можливих мереж

повторення мемів, організатори цих процесів досягають значних результатів, які наприклад, зміна політичних режимів, падіння, здавалося б, доволі стійких, існуючих багато десятиліть в режимі надзвичайного стану державних вертикалей [25, с. 63].

«Гібридні» загрози являють собою різні ступені небезпеки Україні та країнам ЄС. По-перше, в Україні «гібридна» війна вже стала довершеним фактом із активним залученням російських військових, найманців та військової допомоги через ділянку кордону, що є неконтрольованою.

По-друге, всупереч Україні, майже всі країни ЄС розташовані на найнижчих позиціях у рейтингу «Fragile States Index» за сумою показників, які можуть спричинити дестабілізацію. Зазначимо, що ефективні державні інституції та низький рівень структурного насильства в цих країнах значно знешкоджують «гібридні» загрози з Росії.

По-третє, міцні історичні зв'язки українських політичних вершків та фінансово-промислових груп з російським керівництвом створили умови для вразливості України до «гібридних» загроз з боку Росії, які в 2014 р. перетворились у «гібридну» війну.

За словами експертів, Україні та Європі необхідно створювати комплексні стратегічні підходи у протидії російській «гібридній» агресії, добирати гнучкі та ефективні механізми реагування, зміцнювати єдність європейських країн у протидії зовнішнім загрозам [49, с. 140].

В зв'язку з тим, що «гібридні» війни та «гібридні» загрози являють собою асиметричні виклики національній безпеці, то й держави мають відповідати на них асиметрично.

Українська практика показала, що «гібридна» війна загрожує, насамперед, слабким країнам, нездатним протистояти гібридним загрозам з боку країн, які мають значно вищі військові та економічні ресурси. Отже, ефективним засобом протидії «гібридним» загрозам є створення ефективних державних інституцій,

які здатні гарантувати безпеку, права і свободи громадян та представляти інтереси суспільства.

Ще одним кроком у протидії «гібридним» загрозам є збільшення інформаційно-аналітичних потужностей органів державної влади, які мали б змогу своєчасно реагувати на ймовірні виклики та об'єктивно оцінювати їх небезпеку. Вагомим асиметричним методом протидії «гібридним» загрозам може бути розвиток політичної культури та освіти. Завдяки цьому з'явиться можливість попередити посилення маргінальних груп, які здебільшого служать інструментом втілення цілей держави-агресора [27, с. 92].

Отже, з усього вище сказаного випливає - по-перше, росія почала війну, щоб задовільнити свої власні хворобливі амбіції та «залякати» своєю могутністю інші країни Європи. По-друге, самопроголошення нейтральною державою без надійних міжнародних гарантій незалежності та територіальної цілісності - це є міною уповільненої дії, яка, як тільки прийде її час, і може вибухнути.

По-третє, лише об'єднання зусиль усіх європейських держав. США та інших демократичних держав світу є гарантією заборони домінування держав, для яких основне — право сили, а не сила права.

Інформаційна кампанія проти України, яку розгорнула Російська Федерація являється досить глибокою і багаторівневою агресією. Вона включає багато факторів, які спрямовані на те, щоб ослабити Україну в політичному, економічному, військовому, інформаційному плані для того аби все світове співтовариство виключило українське питання з порядку денного. Для того аби окупувати Україну повністю і в подальшому знищити усі деморалізовані намагання супротиву.

Для ефективної протидії інформаційній війні потрібно регулярно вживати заходи протидії. Велика роль у вирішенні цього завдання відводиться засобам масової інформації. Саме факти, які висвітлюють медіа, акценти на певні явища чи аспекти протистояння, формують думку аудиторії про конфлікт, стимулюючи

до потрібної реакції. Засоби масової інформації надають можливості перетворити маленький конфлікт на велике протистояння або, навпаки, – проігнорувати серйозну проблему. Саме від ставлення медіа до події, їхньої упередженості, значною мірою залежить перебіг самого конфлікту. Велику роль у протидії інформаційній війні відіграє громадськість, особи з активною життєвою позицією, які через мережу Інтернет доносять інформацію відмінну від тієї, яка нав'язується суспільству ззовні.

Найбільш складним та часовитратним, проте достатньо ефективним методом протидії інформаційній віні, на мою думку, є підвищення у суспільства аналітичних здібностей, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій.

На мою думку, в Україні має бути створений відповідний центр, що виконуватиме аналіз інформації по всім можливим пунктам : від джерела походження до змісту та «чистоти», достовірності. Лише в такому випадку відбуватиметься координація діяльності волонтерів з моніторингу медіа-ресурсів на предмет наявності матеріалів, які містять згубний інформаційний вплив, а також здійснення такої діяльності працівниками центру.

Необхідно на законодавчому рівні прийняти закон щодо кримінальної відповідальності за поширення не правдивої інформації на території України.

Виходячи з наведеного, можна зробити висновок, що протидія інформаційній війні та інформаційному тероризму є одним з напрямів забезпечення інформаційної безпеки як складової частини національної безпеки держави. Механізми протидії зазначеним загрозам мають бути високотехнологічними та мати системний характер.

Головний виклик сьогодні полягає в тому, як здійснити систематичні кроки для відповіді на російську інформаційну війну. Дослідження показує, що стратегія росії є гібридною та гнучкою, має безліч облич та безліч вимірів, для брехні і агресії. Крім того, вона має унікальну здатність трансформуватись під форми

демократичних наративів та інструментів, і навіть під національні форми. Вона використовує демократію проти неї самої. І саме це робить її такою унікальною, а боротьбу проти неї – такою складною. Але у часи, коли інформацію дедалі більше використовують як інструмент у війні, ми не маємо жодної іншої альтернативи як боротися проти неї, позбавити зброї зловмисні впливи, приборкувати агресора.

Можемо прийти до наступного висновку - спроби росії впливати на громадську думку через перегляд і переписування історії під час війни в Україні охоплюють досить широкий і різноманітний спектр діяльності як у внутрішньому, так і в міжнародному середовищі. Ця діяльність продовжує залишатися одним з основних інструментів інформаційно-психологічних операцій в арсеналі російських пропагандистів.

У ході дослідження було з’ясовано, що українське ЗМІ відіграє ключову роль у формуванні суспільної думки, особливо в умовах воєнного стану та інформаційного протистояння. Вплив ЗМІ на громадян виявляється як у здатності мобілізувати суспільство, підтримувати моральний дух, так і в потенційній небезпеці поширення недостовірних або емоційно забарвлених повідомлень. На разі, сучасний інформаційний простір України характеризується високим рівнем конкуренції між офіційними джерелами, незалежними медіа та соціальними мережами. Це створює сприятливе середовище для появи фейків — особливо щодо втрат на фронті, просування українських чи ворожих військ, а також оцінки міжнародної підтримки. Тож, важливим завданням українського суспільства є розвиток медіаграмотності, уміння фільтрувати інформацію, перевіряти джерела та критично сприймати новини. Підвищення рівня обізнаності громадян у сфері інформаційної безпеки сприятиме зміцненню національної стійкості до дезінформації.

РОЗДІЛ 5. РОЗВИТОК ІНФОРМАЦІЙНОЇ СИСТЕМИ

5.1. Виклики та загрози інформаційного простору

На сьогоднішній день, інформаційний простір України зазнає багаторівневу еволюційну загрозу: масштабні дезінформаційні кампанії, атаки на журналістів і медіа структуру, кібероперації, «інформаційне вичавлювання» (зливи/псевдоджерела), а також міжнародна маніпуляція (кампанії впливу в ЄС/США). Саме ці загрози посилюють соціальну поляризацію, знижують довіру до інституцій і створюють ускладнення при доступі громадян до перевіреної інформації [51, с. 56].

Варто виділити такі основні види загроз для інформаційної безпеки:

1. Несанкціонований доступ. Така загроза може призвести до розповсюдження, зміни або видалення важливих конфіденційних даних. Тому компаніям варто постійно оцінювати ситуацію з приводу інформаційної безпеки на наявність вразливостей.
2. Шахрайство. Застосування ненадійних додатків призводить до того, що конфіденційна інформація стає доступною злочинцям, які використовують її для наживи.
3. Витік інформації. Загроза, під час передачі даних через недостатньо захищені канали може призвести до дискредитації інформації.
4. Кібертероризм. Масштабні загрози, які завдають суттєвої шкоди не лише компанії, а й цілій державі.
5. Інформаційні операції з елементами «зливів» і псевдодокументів. Фейкові зливи та підміна контексту справжніх документів яскраво підривають довіру до інституцій.
6. Фізичні та кібер-атаки на журналістів і медіа структуру. Цілеспрямовані удари по базам журналістів, кібератаки на ЗМІ направлені на залякування та тиск закрити матеріали. Все це значно ускладнює фронтове висвітлення подій.

7. Маніпуляції через міжнародний інформаційний простір. Ціль: просунути антиукраїнські сценарії в ЄС та США, щоб ослабити і підірвати зовнішню підтримку, міжнародну солідарність, створювати сумніви щодо санкцій та допомоги [43].

У найближчі роки українській інформаційній системі доведеться зіштовхнутися з низкою структурних, технологічних, соціальних та інституційних викликів:

1. Технологічні виклики

2. Штучний інтелект і неправдивий контент.

Швидкий розвиток технологій штучного інтелекту надає не лише нові ресурси, але й створює загрозу масового поширення фейкових зображень, аудіо та відео, які навіть експертам складно розпізнати.

Уже сьогодні ми бачимо відео з підробленими заявами політиків, військових чи дипломатів.

Поширення таких фейків може викликати паніку, призвести до дестабілізації суспільної довіри або вплинути на міжнародну репутацію України. [54, с. 138].

Як бачимо, інформаційна система України постійно підпадає під кібератаки на урядових порталах, медіа, критичну інфраструктуру. Український медіаринок і надалі перебуває роздробленим: саме бізнес-групам належать приватні медіа, що впливає на незалежність редакційної політики. Це є фундаментом ризику для політичних маніпуляцій і нерівного доступу до правдивої інформації [52, с. 59].

Ефективним було б саме розробка державою нової моделі співпраці державних і незалежних ЗМІ, яка буде гарантувати баланс між свободою слова і безпекою.

Незважаючи на те, що Україна має потужний Центр стратегічних комунікацій, все ще відчувається нестача єдиної довгострокової інформаційної концепції, яка б визначала:

- цілі державної комунікації у мирний і воєнний час;

- чітку систему координації між силовими структурами, МЗС, медіа і громадськими організаціями;
- алгоритми реагування на інформаційні кризи.

Без такої тактики навіть правильна інформація може подаватися частково із зниженою ефективністю.

3. Соціально-психологічні виклики

3.1. Втома від війни та інформаційне перенасичення

Після кількох років війни українці стикаються з явищем інформаційної втоми — емоційним вигоранням, байдужістю, зниженням інтересу до новин.

В результаті , створюються прогалини, які заповнюють маніпулятори й фейкові джерела, що пропонують легку, емоційно забарвлену інформацію. Звідси висновок - підтримувати психологічну стійкість населення, поширювати культуру усвідомленого споживання новин.

3.2. Поляризація суспільства

Інформаційна війна Росії активно використовує розбіжності між регіонами, соціальними та віковими групами.

Тому такі теми, як мови, релігії, мобілізації чи економічних труднощів найчастіше стають основою для маніпуляцій.

Українська інформаційна система має навчитися формувати сюжети єдності, не замовчувати проблеми і забороняти ворогам використовувати їх у своїх цілях.

4. Освітні та кадрові виклики.

4.1. Низький рівень медіаграмотності серед населення

Незважаючи на те, що ситуація все-таки покращується, велика частина населення досі не вміє аналізувати інформацію, відрізняти факт від судження, фейк — від сатири.

Найуразливіші групи — мешканці сільських районів, люди старшого віку, учні без доступу до якісної освіти.

Варто зробити медіаграмотність обов'язковим елементом шкільної та університетської програм.

4.2. Професійна підготовка журналістів

Не секрет, що українські журналісти нерідко працюють у надскладних умовах, не маючи жодного захисту чи доступу до сучасних аналітичних інструментів. Тому слід оновити систему журналістської освіти, роботи з даними та психології інформаційних війн, впровадити навчання з кібербезпеки, OSINT, фактчекінгу.

5. Міжнародні та геополітичні виклики

5.1. Інформаційна війна поза межами України

Російська федерація завзято діє у європейському, американському та азійському інформаційному просторі, при цьому просуває меседжі про "втому від України", "корупцію у владі", "марність допомоги".

Україна може значно послабити підтримку союзників, якщо не вибудує системну інформаційну дипломатію.

5.2. Конкуренція з глобальними інформаційними гравцями.

Українські меседжі часто втрачаються серед інформаційних потоків великих міжнародних медіа.

Слід звернути увагу на присутність України у світовому інформаційному полі — через культурну дипломатію, мультимедійні платформи, співпрацю з аналітичними центрами.

6. Нормативно-правові виклики.

У зв'язку з недостатнім оновленням законодавства щодо регулювання онлайн-платформ, боротьби з дезінформацією та захисту персональних даних, питання балансу між свободою слова та інформаційною безпекою залишається

відкритим. В цьому випадку варто виробити гуманістичну, але ефективну модель інформаційної політики, яка захищає суспільство і тим самим не порушує демократичні принципи [53, с. 252-254].

Висновки

Наразі українська інформаційна система перебуває у стані глибоких змін, водночас виступаючи інструментом оборони, освіти й державотворення.

Головними викликами найближчих років стануть:

- технологічна адаптація до нових форм дезінформації (ШІ, фейк);
- зміцнення незалежних медіа і фактчекінгових центрів;
- підвищення медіаграмотності всіх груп населення;
- розвиток інформаційної дипломатії на міжнародному рівні;
- створення цілісної державної стратегії комунікації.

Щоб Україні не лише протистояти інформаційним атакам, а й трансформувати власний інформаційний простір на потужний інструмент зміцнення державності та демократії, варто поєднати технологічні рішення, правові інструменти та просвітницьку роботу.

5.2. Розвиток інформаційної системи України та майбутні зміни

Наразі, інформаційна система України знаходиться в стані активного трансформаційного розвитку, спричиненого одночасно двома чинниками — зовнішньою агресією Росії та внутрішньою потребою у цифровізації держави. Сучасні події продемонстрували, що інформаційна сфера є як елементом комунікації, так і інструментом безпеки, оборони, управління та міжнародного впливу [50, с. 91].

1. Цифровізація державного управління

За останні роки значний прорив у напрямі цифрової трансформації здійснила Україна.

Платформа «Дія» стала символом трансформації державних послуг у цифровий формат, що дало можливість громадянам взаємодіяти з владою онлайн, при чому знижуючи корупційні ризики та підвищуючи прозорість.

Здійснення електронного документообігу, відкритих даних та кіберзахисту державних реєстрів є маневром до створення міцної інформаційної інфраструктури.

У майбутньому очікується інтеграція цих систем у єдиний національний цифровий контур, який буде сумісним зі стандартами ЄС [38, с. 154].

2. Посилення кібербезпеки

Повномасштабна війна довела, що інформаційна система держави має бути захищеною і від технічних атак, і від інформаційно-психологічних операцій (ІПСО).

Саме тому розвиток інформаційної безпеки України окреслює :

- створення національної системи кібероборони;
- розвиток центрів реагування на кіберінциденти (CERT-UA);
- зміцнення співпраці з НАТО та ЄС у сфері кіберзахисту;
- впровадження стандартів безпеки у приватному секторі.

Актуальним було б створення у майбутньому окремого кібервійська, яке б координувало оборону інформаційного простору на рівні із Збройними силами.

3. Боротьба з дезінформацією та пропагандою

Наразі інформаційна система України стикається з масштабними кампаніями дезінформації з боку РФ [38, с. 193].

Тому стратегічні напрямки розвитку такі:

1) формування державних і громадських аналітичних центрів фактчекінгу,

2) розробка законодавчих механізмів протидії фейкам із збереженням свободи слова,
3) організація національної медіаграмотності населення через освіту, ЗМІ та соціальні мережі.

Можемо сказати, що цілеспрямованим було через певний час побачити єдину платформу перевіреної інформації, що буде збирати офіційні дані, повідомлення від органів влади та спростування фейків.

4. Інтеграція до європейського інформаційного простору

Майбутнє України в інформаційній сфері суцільно пов'язане з євроінтеграційними процесами.

Це означає:

- пристосування українського законодавства до Директив ЄС про цифрові послуги та захист персональних даних (GDPR),
- збільшення участі українських медіа в європейських платформах,
- розвиток партнерських програм у сфері кібербезпеки, штучного інтелекту та цифрових комунікацій.

Завдяки такому зближенню, гарантовано і підвищення якості інформаційного середовища, забезпечення включення України у єдиний цифровий ринок Європи [2, с. 94].

5. Розвиток медіа та громадянського суспільства

Варто зазначити, що інформаційна система майбутнього — це не лише технології, а й людський капітал.

Ключовим напрямом стане:

1) підтримка незалежних ЗМІ,
2) процвітання освітніх програм з журналістики, комунікацій та кіберетики,

3) посилення ролі громадських організацій у моніторингу інформаційних загроз.

Це дасть можливість створити відкритий, демократичний та стійкий інформаційний простор.

Отже, розвиток інформаційної системи України — це стратегічний напрям державного розвитку, який визначатиме як безпеку, так і конкурентоспроможність країни у глобальному світі. Майбутнє українського інформаційного простору — це синтез технологій, демократії, медіаграмотності та національної свідомості, які разом створюють базу для стійкої, незалежної й захищеної цифрової держави.

На мою думку, Україна потребує єдиного стратегічного документа, який би визначав:

1) цілі, інструменти та пріоритети у сфері міжнародних комунікацій;
2) механізми протистояння ворожим інформаційним впливам;
3) способи поширення правдивого іміджу України за кордоном.

Це має бути щось на зразок державної доктрини “інформаційної дипломатії”, що поєднує зусилля Міністерства закордонних справ, Міністерства культури, СБУ, Центру стратегічних комунікацій, провідних ЗМІ та громадських ініціатив.

Її основна мета — створити та закріпити єдину інформаційну позицію України у світі.

2. Реформа державних комунікацій

В наш час комунікація між державними структурами нерідко фрагментована.

Саме тому слід створити:

- Центральне агентство стратегічних комунікацій, яке узгоджуватиме роботу всіх держорганів у медіапросторі;

- єдину систему швидкого реагування на інформаційні атаки, що керуватиметься принципом “інформаційної оборони”;
- професійну школу державних спікерів і комунікаторів, які будуть мати можливість ефективно представляти позицію України в міжнародних медіа.

3. Поглиблення міжнародного співробітництва

Щоб Україні стати активним учасником міжнародних ініціатив у сфері кібербезпеки та інформаційної політики, необхідно :

1) приєднатися до Європейського альянсу з протидії дезінформації (EDMO);
2) приймати участь у програмах НАТО StratCom;
3) створити регіональний центр інформаційної безпеки у Києві, який міг би співпрацювати з партнерами у Центральній та Східній Європі.

За таких умов Україна могла б перетворитися з об’єкта на суб’єкт інформаційної політики, комплектуючи стандарти та ініціативи для інших.

4. Розвиток публічної дипломатії та іміджевих проєктів.

На мою думку, одним із пріоритетів розвитку має стати просування України у світі через позитивні наративи, такі, як:

- підтримка україномовних медіа за кордоном;
- формування міжнародного телеканалу українського мовлення (аналог BBC World або DW);
- комунікація в активній позиції через культурні, наукові, освітні проєкти;
- створення бренду Ukraine – strong, smart, free.

Це дасть змогу боротися не лише з фейками, а й з глибшими стереотипами про Україну, які тривалий час вирощувалися російською пропагандою.

5. Освітня реформа: медіаграмотність, як частина національної безпеки.

Оскільки від рівня критичного мислення громадян залежить стійкість усієї інформаційної системи, тому вважаю за потрібне :

1) включити медіаграмотність і цифрову етику до шкільної програми;
2) сформували національний освітній центр медіабезпеки при МОН;
3) створювати та удосконалювати курси для держслужбовців, журналістів і дипломатів з аналізу інформаційних загроз.

Така реформа, на мою думку, допоможе сформувати інформаційно відповідальне суспільство, яке буде здатне самостійно протидіяти маніпуляціям.

6. Впровадження штучного інтелекту в системі моніторингу.

Не секрет, що на сьогоднішній день майбутнє належить технологіям.

Україна має інвестувати у створення AI-платформи для моніторингу дезінформації, яка автоматично відстежуватиме фейки у соцмережах та новинних сайтах, встановлюватиме джерела їх походження та, що наразі є вкрай важливим, прогнозуватиме інформаційні атаки.

Оскільки такі системи вже використовують у США, Франції та Естонії, то і їх впровадження допоможе Україні діяти на випередження, а не лише реагувати.

7. Захист цифрового суверенітету

На моє переконання, Україні варто мати власні державні дата-центри, розташовані у безпечних регіонах, національну соціальну платформу або мережу, що дадуть можливість комунікувати у разі блокування глобальних ресурсів та, звичайно, систему резервного збереження державних баз даних у країнах-партнерах ЄС. Як підсумок, це питання є дуже актуальним - і є не лише з питань технології, технології, а й дипломатії, оскільки забезпечує стійкість держави в умовах війни чи глобальних кібератак.

8. Підтримка незалежних медіа та громадянського суспільства.

Мої спостереження призвели мене до переконання, що без вільної журналістики неможливо побудувати сильну інформаційну державу. Для цього варто:

1) сформували державний фонд підтримки незалежних медіа, який буде фінансуватися прозоро через грантову систему;
2) забезпечити захист журналістів від переслідувань та тиску;
3) підтримувати ініціативи з перевірки фактів і громадського моніторингу.

Таким чином, можна сміливо сказати, що фундаментом демократичного суспільства є баланс державної безпеку та свободи слова.

9. Дипломатичне просування українських наративів.

На мою думку, Україні слід активніше використовувати дипломатичні місії. Варто зазначити, що майбутнє української інформаційної системи має спиратися на три головні принципи:

-стратегічність,

- відкритість,

- безпеку.

Реформам слід поєднувати державний контроль за критичною інфраструктурою з максимальною свободою громадянського суспільства та міжнародним партнерством.

Як майбутній дипломат, я бачу Україну не тільки як державу, що обороняється від інформаційної агресії, а як лідера у формуванні нової культури правди, прозорості та відповідальної комунікації у світі.

ВИСНОВКИ

Отже, тема Інформаційної війни в Україні є надзвичайно важливою, адже інформація – це основна зброя у протидії держав світу в боротьбі за світове панування у глобальному інформаційному просторі. Сам простір розглядається як сукупність інформаційних ресурсів, технологій, комунікаційних мереж і соціальних взаємодій, що забезпечують обмін даними та знаннями в сучасному суспільстві.

Дослідження цього підрозділу вказують на те, що інформаційний простір на разі розвивається під впливом технологічного процесу, соціальних процесів та політичних факторів. Зрозумівши його структуру дозволить ефективніше використовувати інформаційні ресурси та забезпечувати інформаційну безпеку всередині нашої країни. Без сумніву можна сказати, що інформаційна складова національної безпеки держави відіграє важливу роль, адже в ній присутні певні ризики та загрози (кібертерорризм, кіберзлочинність, агресивна пропаганда та поширення антидержавних гасел, обмеження доступу населення до публічної інформації).

Проаналізувавши роботу українських ЗМІ (журналістів, редакцій, новинних пабліків), я з’ясувала, що вони відіграють ключову роль у сприйнятті інформації. Медіа допомагають людям орієнтуватися в інформаційному просторі, пояснюють складні події простими словами, завдяки ним формується суспільна думка, рівень довіри до державних інституцій. В умовах війни українські медіа також виконують функції інформаційного щита — спростовують фейки, підтримують моральний дух населення та забезпечують доступ до перевіреної, достовірної інформації. Багато соціальних мереж, такі як : Телеграм, ТікТок, Фейсбук допомагали українцям дізнатися актуальні новини про ситуацію в країні. Короткі репортажі в Ютуб давали розуміння масштабів трагедій. Я перекрнана, що саме від ставлення медіа до події, їхньої упередженості, значною мірою залежить перебіг самого конфлікту. Велику роль у протидії інформаційній війні відіграє громадськість, особи з активною життєвою позицією, які через

мережу Інтернет доносять інформацію відмінну від тієї, яка нав’язується суспільству ззовні.

На мою думку, досі серйозною загрозою для національної безпеки є дезінформація. Вона поширюється через соціальні мережі, новинні платформи та різні канали комунікації, що значно ускладнює її виявлення та протидію. З початку повномасштабного вторгнення росії в Україну, в Інтернеті активно ведеться інформаційна війна. Основна її ціль — деморалізувати українців, зменшити силу, психологічно вплинути на людей : посіяти паніку, навести страх та заплутати. Останнім часом мережами Інтернету ширяться фейки про всі глобальні події на світовій арені, аби ввести людей в оману, маніпулювати їхніми емоціями або змінити погляди.

Цілями у війні росії з Україною є створення перешкод європейському та євроатлантичному курсу України, руйнування української державності, повернення росії сферу впливу. У планах Кремля було : зруйнувати єдність європейського співтовариства, заплямувати базові цінності ЄС, посилити вплив і контроль на континенті, зафіксувати порядок та новий устрій в Європі за російським сценарієм.

Якщо проаналізувати цілі, які переслідує Кремль, можна зробити такі висновки : по-перше, не допустити членства в ЄС і НАТО країн, які створені на теренах колишнього СРСР — Грузії, Молдови та України в першу чергу. По-друге, знищити євроатлантичну та європейську єдність і здобути залежні від Москви режими в більшій кількості європейських країн, а також задовольнити лояльність США. По-третє, здобути доступ до дешевого обладнання з промислових об’єктів.

Стратегічні завдання російської гібридної агресії – це руйнування базових європейських цінностей, які об'єднують країни ЄС, вплив на громадські думки та хаос, формування впливової проросійської думки в європейському колі, підтримка та просування розбіжностей між європейськими державами. Отже,

інформаційна кампанія проти України, яку розгорнула Російська Федерація являється досить глибокою і багаторівневою агресією. Вона включає багато факторів, які спрямовані на те, щоб ослабити Україну в політичному, економічному, військовому, інформаційному плані для того аби все світове співтовариство виключило українське питання з порядку денного. Для того аби окупувати Україну повністю і в подальшому знищити усі деморалізовані намагання супротиву.

Для ефективної протидії інформаційній війні потрібно регулярно вживати заходи протидії. Я рахую, що раціонально буде прийняти або оновити попередній національний закон про кібербезпеку, встановити кримінально-правову відповідальність за кібератаки, посилити санкції проти зловмисників і хакерів, запровадити обов'язкову планову сертифікацію кіберзахисту для органів влади й операторів критичної інфраструктури, ввести вимоги до захищеного зберігання та шифрування персональних даних.

Також можна створити національні програми підвищення медіа-грамотності і навчальні кампанії про види фейків та боротьбу з ними, ознайомлення всіх держслужбовців з базами даних та методами захисту електронної інформації (паролі, ключі, коди).

Проте, українська практика показала, що «гібридна» війна загрожує слабким країнам, нездатним протистояти цим загрозам з боку країн, які мають значно вищі військові та економічні ресурси. Порівняємо, наприклад Естонію та Україну, які постраждали від росії. Спільним для них є те, що росія застосовувала проти обох - кібератаки, інформаційний тиск, пропаганду та спроби погіршити внутрішньополітичну ситуацію. Для протидії цьому тиску, обом державам довелося активно розвивали власні системи кіберзахисту, інформаційної безпеки та стратегічних комунікацій. Відмінне – масштаби тиску росії. Україна переживає війну в повному її прояві, в той час як Естонія просто втратила допуск до баз даних, отримала хакерські атаки. Українцям доводиться вести боротьбу,

як на фізичному фронті зі зброєю та кровопроливтям, так і в Інтернеті, в той час як естонці зіштовхнулися лише з кіберзагрозою та витоком даних.

Порівняємо також досвід Ізраїля та України стосовно питань ведення боротьби гібридної війни. Спільним для цих країн є те, що обидві перебувають у стані тривалої небезпеки й вимушені будувати власну систему безпеки, де інформаційна, психологічна та кіберскладові мають таке ж значення, як і військова. Ізраїль, так само як і Україна, протидіє пропаганді, дезінформації, спробам вплинути на громадську думку та маніпуляціям у медіапросторі. Обидві держави поєднують роботу розвідки, армії, аби оперативно реагувати на загрози й мінімізувати наслідки інформаційних атак. Але є і купа відмінностей, наприклад: Ізраїль десятиліттями будує систему безпеки, де ключову роль відіграють високотехнологічні розвідструктури, жорстко контролює інформаційне середовище та постійне моніторить цифрові канали у режимі реального часу. Україна ж формує свою сучасну систему інформаційної безпеки вже під час повномасштабної агресії, коли доводиться реагувати не лише на пропаганду та кібератаки, а й на реальні військові операції росії.

Отже, з усього вище сказаного випливає - по-перше, росія почала війну, щоб задовільнити свої власні хворобливі амбіції та «залякати» своєю могутністю інші країни Європи. По-друге, лише об’єднання зусиль усіх європейських держав. США та інших демократичних держав світу є гарантією заборони домінування держав, для яких основне — право сили, а не сила права.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Іноземні видавництва та статті :

Alodat, A. M. (2023) Social media platforms and political participation: a study of jordanian youth engagement. MDPI. Отримано з: https://www.mdpi.com/2076-0760/12/7/402log2013.pdf

Anti-Western narratives in Russian propaganda. Riga : NATO StratCom COE, 2022. 68 p.

Cyber Operations in the Russia-Ukraine War: White Paper. Cambridge : Google Threat Analysis Group, 2022. 27 p.

Destroying the Myth of Russian Invincibility — дослідження Джона С. Гаррела, видане у січні 2024 р., аналізує хід війни та розвіює міфи про "непоборність" російської армії. https://www.penandswordbooks.com/9781399031769/the-russian-invasion-of-ukraine-february-december-2022/

Detecting and Defeating Disinformation. Riga : NATO StratCom COE, 2021. 72 p.

Disinformation during the Russia-Ukraine War. London : BBC News Analysis, 2022. URL: https://bbc.com/news

Giles K. Moscow Rules: What Drives Russia to Confront the West. London : Chatham House, 2019. 256 p.

Global Risk Report 2023: Digital Threats. Geneva : World Economic Forum, 2023. 117 p.

Helmus T., Bodine-Baron E., Radin A. et al. Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. Santa Monica : RAND Corporation, 2018. 145 p.

How Russia Uses Telegram for Propaganda. Washington : The Washington Post Investigations, 2023. URL: https://washingtonpost.com

Kremlin Information Operations in Europe. London : The Guardian Investigations, 2023. URL: https://theguardian.com

Overreach: The Inside Story of Putin's War on Ukraine — журналістський і історичний, виданий у 2022 році.р https://en.wikipedia.org/wiki/Newsweek

Paul C., Matthews M. The Russian "Firehose of Falsehood" Propaganda Model. Santa Monica : RAND Corporation, 2016. 12 p.

Polyakova A., Fried D. The Kremlin's Trojan Horses 3.0. Washington : Atlantic Council, 2023. 54 p.

Pomerantsev P. This Is Not Propaganda: Adventures in the War Against Reality. London : Faber & Faber, 2019. 288 p.

Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. New York : Farrar, Straus and Giroux, 2020. 513 p.

Russia's Cyber Tactics and the Global Cyber Threat. New York : Microsoft Threat Intelligence Center, 2022. 32 p.

Seely R. A War of Words, A War of Wires: Russia's Information War. Washington : CEPA, 2022. 34 p.

The Information War in Ukraine: Media, Censorship and Narratives. London : Reuters Institute for the Study of Journalism, 2023. 57 p.

The Russia-Ukraine War: Disinformation, Cyber Operations and Media Manipulation. Brussels : EUvsDisinfo, 2022. 41 p.

The Russo-Ukrainian War. https://www.amazon.com/Russo-Ukrainian-War-Serhii-Plokhy/dp/1802061789?utm_source=chatgpt.com

Українські дослідження та офіційні документи :

Бабенко А. М. Мережі Інтернет як об'єкт регіонального дослідження в контексті профілактики злочинності / Матеріали конференції «Боротьба з інтернет-злочинністю». Донецьк, 2013.

Бабенко А. М. Мережі Інтернет як об'єкт регіонального дослідження в контексті профілактики злочинності / Матеріали конференції «Боротьба з інтернет-злочинністю». Донецьк, 2013.

Бабенко А. М. Мережі Інтернет як об'єкт регіонального дослідження в контексті профілактики злочинності / Матеріали конференції «Боротьба з інтернет-злочинністю». Донецьк, 2013.

Баранов О. В. Інформаційна політика держави : навч. посіб. — К. : НАДУ, 2014. — 298 с.

Баровська А. В. Інформаційна війна: теорія і практика. — К. : НУОУ ім. І. Черняховського, 2018. — 212 с.

Баровська А. Інституційне забезпечення державної комунікативної політики : досвід країн Європи : аналітична доповідь. Режим доступу : http://niss.gov.ua/articles/1730

Біловус Л. І. Український інформаційний простір: перспективи. Тернопіль: Західноукраїнський національний університет, 2019. 275 с.

Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту: навчальний посібник. Київ: Ліра-К, 2024. 554 с.

Бондар Ю. В. Поле битви – інформаційний простір. К.: МАУП, 2006.152 с.

Буньківська О. В. Вплив інноваційних інформаційних технологій на функціонування національного інформаційного простору. К.:КНУКіМ, 2008. 261 с.

Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. (за заг. ред.). Інформаційна та кібербезпека: соціотехнічний аспект : підручник. — (навч. посібник/підручник), 2019 р.

Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. (за заг. ред.). Інформаційна та кібербезпека: соціотехнічний аспект : підручник. — (навч. посібник/підручник), 2019 р.

Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. (за заг. ред.). Інформаційна та кібербезпека: соціотехнічний аспект : підручник (навч. посібник/підручник), 2019 р.

Віднянський С., Мартинов А. Російсько-українська війна та міжнародне співтовариство: монографія. К.: Інститут історії України НАН України, 2023. 264 с.

Вплив тіньових інформаційних технологій на інформаційну безпеку суб'єкта господарювання / А. Марущак, О. Скіцько // Безпека інформації. 2018. 69-74 с. Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2018_24_1_12

Гончаренко Р. Як війна Росії проти України змінила настрої у країнах G7. // DW. 21 червні 2022.URL: https://www.dw.com/.uk/ryzyk-1-yak-viina-rosii-proty-ukrainy-zminyla-nastroi-u-krainakh-g7/a-62202115

Горбулін В. П. Стратегічне планування у сфері національної безпеки. — К. : НІСД, 2010. — 320 с.

Горбулін В. П., Литвиненко О. В. Світова гібридна війна : український фронт. — К. : НІСД, 2017. — 496 с.

Горовий В.М. Правові перспективи національного розвитку. Режим доступу : http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/#sthash.AgJjKJa4.dpuf

Гурлєва Т. С., Журавльова Н. Ю. Довіра до себе як важливий атрибут стресостійкості особистості в умовах інформаційної війни: взаємозв’язок понять. Вчені записки ТНУ імені В.І. Вернадського. Серія: Психологія. 2022. Том 33 (72), № 4. 76–82 с.

Гуцалюк М. В. Організація захисту інформації : [навч. посібн.]. К. : Альтерпрес, 2012. 224 с.

Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: навч. посіб. Х. : Фоліо, 2002. 285 с.

Державна політика : підручник / Нац. акад. держ. упр. при. Президентові України; ред. кол. : Ю. В. Ковбасюк, К. О. Ващенко, Ю. П. Сурмін та ін. Київ : НАДУ., 2014. 448 с.

Державна служба фінансового моніторингу України. Кіберзлочинність. URL: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf

Довгань О.Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації // Правова інформатика. 2013. 79-88 с.

Дорошкевич А. С. Гібридна війна в інформаційному суспільстві. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія. Харків : Право, 2015. № 2(25). С. 21–28.

Дубов Д. В. Інформаційний простір України: трансформація, безпека, розвиток. — К. : НІСД, 2013. — 368 с.

Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

Інформаційна безпека держави у контексті протидії інформаційним війнам" /Навчальний посібник // За загальною редакцією доктора технічних наук, професора, заслуженого працівника народної освіти України генерал-полковника В. Б. Толубка. К.: НАОУ, 2004. 177с.

Інформаційна безпека України: сучасні виклики, загрози та механізми протидії. Науковий журнал «Соціальні технології». Львів: Національний університет "Львівська політехніка", 2016. С. 45-60.

Інформаційна війна – зброя масового знищення. Електронний ресурс : https://www.pravda.com.ua/rus/articles/

Інформація [Електронний ресурс] / Матеріал з Вікіпедії – вільної енциклопедії Посилання: http://uk.wikipedia.org/wiki.

Кириченко В. В. Особистість у сучасному інформаційному суспільстві. Житомир : Вид-во ЖДУ імені Івана Франка, 2020. 245 с.

Ковтух Є. В. Кібербезпека у публічному секторі: монографія. – Харків: Харківський національний університет внутрішніх справ, 2019. 320 с.

Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

Концепція національної безпеки України : схвалена Постановою Верховної Ради України від 16 січ. 1997 р. № 3/97-ВР. Відомості Верховної Ради України. 1997. № 10. Ст. 85.

Кормич Б.А. Інформаційна безпека : організаційно-правові основи. Навч.посібник. – К. : Кондор, 2004. 128 с.

Кормич Б.А. Інформаційна безпека : організаційно-правові основи. Навч.посібник. – К. : Кондор, 2004. 128 с.

Курс адміністративного права України: підручник/ за ред. О. В. Кузьменко. 3-тє вид., допов. Київ: Юрінком Інтер, 2018. 904 с.

Ліпкан В. А. Інформаційна безпека України : навч. посіб. — К. : КНТ, 2011. — 348 с.

Ліпкан В. А. Інформаційна безпека як складова національної безпеки України // Інформаційні технології в економіці, менеджменті і бізнесі: Проблеми науки, практики і освіти: Зб. наук. праць VIII Міжнар. наук.-практ. конф.Ч. 2. К.: Вид-во Європ. ун-ту, 2003. С. 443 – 453.

Ліпкан В. А. Інформаційна безпека як складова національної безпеки України // Інформаційні технології в економіці, менеджменті і бізнесі: Проблеми науки, практики і освіти: Зб. наук. праць VIII Міжнар. наук.-практ. конф.— Ч. 2. — К.: Вид-во Європ. ун-ту, 2003. — С. 443 – 453.

Ліпкан В. А. Національна та міжнародна безпека. — К. : Знання України, 2006. — 640 с.

Ліпкан В. А. Теоретичні основи та елементи національної безпеки України. К.: Текст, 2003. 600 с.

Лойшин А., Ясенко С., Косарецький Є., Бойко Р. Сутність ключових понять у сфері міжнародної допомоги, наданої для зміцнення обороноздатності України. Міжнародне співробітництво у воєнній сфері. 2023. № 3 (76). С. 46–57.

Лук'янчук Р. В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції [електронний ресурс : https://ippi.org.ua/luk%E2%80%99yanchuk-rv-suchasni-vikliki-povyazani-iz-rozvitkom-kriptoindustrii-st-72-81], 2015.

Лук'янчук Р. В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції [електронний ресурс : https://ippi.org.ua/luk%E2%80%99yanchuk-rv-suchasni-vikliki-povyazani-iz-rozvitkom-kriptoindustrii-st-72-81], 2015.

Лук'янчук Р. В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції [електронний ресурс : https://ippi.org.ua/luk%E2%80%99yanchuk-rv-suchasni-vikliki-povyazani-iz-rozvitkom-kriptoindustrii-st-72-81], 2015.

Магда Є. В. Гібридна війна: вижити і перемогти. Харків : Віват, 2015. 304 с.

Марущак А.І. Питання ефективності діяльності державних органів у сфері захисту інформаційного простору України — Марущак А.І. // Журнал Інформація і право, 2017, № 4(23) / с. 89-92.

Марущак А.І. Питання ефективності діяльності державних органів у сфері захисту інформаційного простору України. Марущак А.І. Журнал Інформація і право, 2017, № 4(23) с. 89-92.

Міжнародні санкції як інструмент стримування російської агресії проти України : аналіт. доп. / [А. Бобровицький, Н. Гавриленко, А. Гончарук, І. Ус, Г. Широкий, Р. Юлдашев] ; за заг. ред. М. Паламарчука. Київ : НІСД, 2023. 76 с. (Серія. «Міжнародні відносини»). DOI: https://doi.org/.10.53679/NISSanalytrep.2023.10

Новаківський І.І. Засади формування інформаційного простору структурних бізнесоболонок. Режим доступу: http://ena.lp.edu.ua

Новіцький Є. В. Проблематика правового регулювання інформаційної та кібербезпеки в сучасній світовій політиці: міжнародно-правовий аспект. Київ: Інститут міжнародних відносин, 2017. 310 с.

Олійник О.В. Стан забезпечення інформаційної безпеки в Україні. Юридичний вісник. 2012. 59-65 с.

Онищенко О.С. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.] ; НАН України, Національна бібліотекака України ім. В.І. Вернадського. К., 2014. 198 с.

Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту: навчальний посібник. Львів: Новий Світ-2000, 2023. 678 с.

Остроухов В. В., Присяжнюк М. М. та ін. Інформаційна безпека: підручник. Київ: Ліра-К, 2021. 412 с.

Панченко В.М. Співвідношення понять : інформаційна та кібернетична безпека. Інформаційна безпека людини, суспільства, держави. 2013. 20-24 с.

Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект. Дніпро: Дніпровський державний університет внутрішніх справ, 2021. 280 с.

Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Електронний ресурс. Режим доступу: http://www.justinian.com.ua/article.php?id=3222

Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Електронний ресурс. Режим доступу: http://www.justinian.com.ua/article.php?id=3222

Пилипчук В.Г. Системні правові проблеми формування інформаційного суспільства : зб. наук. ст. та тез ; наукове повідомлення за матеріалами міжнародної науково-практичної конференції. Х. : НДІ державного будівництва та місцевого самоврядування, 2012. 214 с.

Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину / стаття — Інформаційна безпека людини, суспільства, держави. https://www.researchgate.net/publication/311660245_Cyberterrorism_development_history_current_trends_countermeasures).

Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину / стаття — Інформаційна безпека людини, суспільства, держави, №2 (2), 2009, с. 80. (https://www.researchgate.net/publication/311660245_Cyberterrorism_development_history_current_trends_countermeasures).

Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину / стаття — Інформаційна безпека людини, суспільства, держави, №2 (2), 2009, с. 80. (https://www.researchgate.net/publication/311660245_Cyberterrorism_development_history_current_trends_countermeasures

Почепцов Г. Г. Інформаційні війни. — К. : Видавничий дім «Києво-Могилянська академія», 2015. — 496 с.

Почепцов Г. Г. Теорія комунікації. — К. : Видавничий дім «Києво-Могилянська академія», 2009. — 422 с.

Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. К. : Вид.дім Києво-Могилянська академія, 2015. 497 с.

Почепцова В. Сучасні інформаційні війни / В. Почепцова. – К. : Вид.дім ―Києво-Могилянська академія‖, 2015. – 497 с.

Про забезпечення функціонування української мови як державної : Закон України від 25 квіт. 2019 р. № 2704-VIII. Відомості Верховної Ради України. 2019. № 21. Ст. 81.

Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) : Указ Президента України від 15 трав. 2017 р. № 133/2017. Офіційний вісник Президента України. 2017. № 14. Ст. 392.

Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

Про Національну програму інформатизації : Закон України від 4 лют. 1998 р. № 74/98-ВР. Відомості Верховної Ради України. 1998. № 27–28. Ст. 181.

Про основи національної безпеки України : Закон України від 19.06.03 р. // Відомості Верховної Ради України (ВВР). 2003. № 39. 351 с.

Про основи національної безпеки України: Закон України. Офіційний Вісник України. 2003. № 29. 143 с.

Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лют. 2017 р. № 47/2017. Офіційний вісник Президента України. 2017. № 5. Ст. 122.

Про рішення РНБО України щодо застосування санкцій до російських медіа : Указ Президента України від 28 квіт. 2017 р. № 107/2017. Офіційний вісник Президента України. 2017. № 9. Ст. 245.

Радзієвська О. Г. Проблеми негативних інформаційних впливів на дитину в Україні в умовах збройного протистояння. Запоріжжя: Запорізький національний університет, 2020. 200 с.

Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни: монографія. Одеса: Одеський національний університет імені І. І. Мечникова, 2020. 350 с.

Сапольскі Р. Біологія поведінки. Причини доброго і поганого в нас / пер. з англ. Любенко. Київ : Наш Формат, 2021. 672 с.

Снігир О. Інформаційна безпека в умовах гібридної війни. — К. : Центр Разумкова, 2016. — 48 с.

Стратегія кібербезпеки України : схвалена Указом Президента України від 26 серп. 2021 р. № 447/2021. Офіційний вісник Президента України. 2021. № 18. Ст. 550.

Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи. Львів: Львівський національний університет імені Івана Франка, 2018. 290 с.

Український інформаційний простір: Науковий журнал Інституту журналістики і міжнародних відносин Київського національного університету культури і мистецтв. Ч. 1. К.: КНУКІМ, 2013. 314 с.

Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Київ: Інститут проблем інформації, 2022. 150 с.

Чаплінська Ю. Кіберкультура та кібербезпека в умовах війни: психологічний практикум : практичний посібник / Юлія Чаплінська ; Національна академія

педагогічних наук України, Інститут соціальної та політичної психології. – Київ, 2023. 80 с.

Чаплінська Ю. Кіберкультура та кібербезпека в умовах війни: психологічний практикум : практичний посібник / Юлія Чаплінська ; Національна академія педагогічних наук України, Інститут соціальної та політичної психології. – Київ, 2023. 80 с.

Чаплінська Ю. Кіберкультура та кібербезпека в умовах війни: психологічний практикум : практичний посібник / Юлія Чаплінська ; Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Київ, 2023. 80 с.