Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
випускної кваліфікаційної роботи

магістра
(назва освітнього ступеня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень ***магістр***
(назва освітнього ступеня)

на тему: Методи протидії інформаційно-психологічному впливу в кіберпросторі

Виконавець: студент **II** **курсу, групи** **КБм-21**

Плужник Артем Леонідович
(підпис) (прізвище ім'я по-батькові)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Володимир НАКОНЕЧНИЙ	
Нормоконтроль	Сергій ДАКОВ	

Київ 2024

Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 року

ЗАВДАННЯ
на виконання випускної кваліфікаційної роботи

спеціальності *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

студенту **КБм-21** **Артем ПЛУЖНИК**
(група) (Ім'я, ПРІЗВИЩЕ)

Тема випускної кваліфікаційної роботи
Методи протидії інформаційно-психологічному впливу в кіберпросторі

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень процес інформаційно-психологічного впливу в кіберпросторі, що здійснюються російською федерацією в умовах повномасштабної воєнної агресії проти України

Предмет досліджень система протидії інформаційно-психологічним операціям на державному, міжнародному та громадянському рівнях з метою гарантування інформаційної безпеки України

Мета полягає у вивченні особливостей інформаційно-психологічних та операцій, здійснюваних Російською Федерацією щодо України, в удосконаленні методів протидії цьому впливу під час повномасштабної воєнної агресії з метою надання рекомендацій для удосконалення цієї системи на різних рівнях

Вихідні дані для проведення роботи теоретичні засади, нормативно-правові акти, аналітичні дані, методологічні інструменти, технічні засоби та інформаційні ресурси

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна полягає в удосконаленні існуючих методів захисту від маніпуляцій та дезінформації, що враховують взаємодію психологічних і технічних аспектів кібербезпеки

Практична цінність полягає у розробці ефективних методів і рекомендацій для виявлення та нейтралізації інформаційно-психологічного впливу в кіберпросторі, що можуть бути використані фахівцями з кібербезпеки, організаціями та урядовими структурами для захисту інформаційних систем та підвищення рівня інформаційної безпеки

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

робота виконана у повному обсязі відповідно до теми

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	17.11.2023 – 29.01.2024
Огляд літератури та збір вихідних даних	30.01.2024 – 12.02.2024
Вивчення існуючих методів протидії інформаційно-психологічному впливу	13.02.2024 – 26.02.2024
Розробка методів і інструментів для аналізу та протидії інформаційно-психологічному впливу	27.02.2024 – 04.03.2024
Оцінка ефективності запропонованих методів і технологій	05.03.2024 – 19.03.2024
Формулювання практичних рекомендацій	20.03.2024 – 25.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	26.04.2024 – 12.05.2024
Подача пакету документів на розгляд ЕК	13.05.2024 – 17.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Ефективність вимірюється покращенням показників безпеки, зменшенням інцидентів кібератак та збільшенням готовності до реагування на нові виклики в галузі кібербезпеки

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Володимир НАКОНЕЧНИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Артем ПЛУЖНИК
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.

Термін подання випускної кваліфікаційної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Пояснювальна записка: 102 с., 9 рис., 87 джерел.

Об’єкт дослідження: процес інформаційно-психологічний впливу в кіберпросторі.

Мета роботи: удосконалення методів протидії інформаційно-психологічному впливу в кіберпросторі з метою підвищення рівня кібербезпеки та захисту інформаційних систем.

Методи дослідження: системний підхід, методи порівняння, структурний та кореляційно-регресійний аналіз для дослідження та розробки методів протидії інформаційно-психологічному впливу в кіберпросторі..

У теоретичній частині дана характеристика методам протидії інформаційно-психологічному впливу в кіберпросторі.

У роботі проаналізовано походження терміну «інформаційно-психологічна операція» та його зв'язок з «інформаційною війною»; вивчено різновиди та методи таких операцій щодо безпеки людини, суспільства та держави.

Досліджено теми та зміст інформаційно-психологічних операцій, які проводила Росія стосовно України; проаналізовано способи їхньої реалізації та фактори, які впливають на систему протидії РФ.

Визначено основні принципи інформаційної безпеки України у боротьбі з інформаційно-психологічними операціями; проаналізовано державну інформаційну політику в умовах воєнної агресії РФ.

Досліджено співпрацю з міжнародною спільнотою у протидії інформаційно-психологічним операціям Росії, а також проаналізовано моделі системи інформаційного протиборства та сформульовано практичні рекомендації з удосконалення системи протидії на рівні громадської участі.

Практичне значення роботи полягає в тому, що вона спрямована на розробку конкретних стратегій та методів протидії інформаційно-психологічному впливу в кіберпросторі, що можуть бути використані для захисту інформаційних систем, підвищення обізнаності користувачів та зменшення ризику кіберзагроз.

Результати здійснених у випускній кваліфікаційній роботі досліджень можуть бути використані організаціями, урядовими структурами та іншими зацікавленими сторонами у зміцненні кібербезпеки та збереженні інформаційної незалежності.

Наукова новизна полягає в інтегрованому підході до вивчення взаємодії між психологічними та технічними аспектами кібербезпеки та розробці заходів захисту від маніпуляцій та дезінформації в інтернеті.

Подальші напрямки досліджень можуть включати розвиток більш ефективних методів виявлення атак, дослідження впливу технологічних інновацій, а також аналіз ефективності правових механізмів у протидії такому впливу.

Ключові слова: кібербезпека, інформаційно-психологічний вплив, маніпуляція, дезінформація, кіберпростір, захист інформації, технології захисту, психологічні аспекти, комплексний підхід, аналіз взаємодії.

ЗМІСТ

ВСТУП

Важливість дослідження цієї теми випливає з того, що в умовах нинішнього етапу розвитку міжнародних відносин стає все більш актуальною проблема виникнення нових форм військових конфліктів, включно з гібридними війнами. Розвиток технологій та зростання взаємозалежностей країн сприяє збільшенню різноманіття методів ведення війни.

Країни все активніше задіюють недержавні суб'єкти та інформаційні технології для впливу на своїх противників. У цьому аспекті особливо важливими стають інформаційні війни та інформаційно-психологічні операції (ІПСО), які разом із військовими діями мають руйнівний вплив на тріаду національної безпеки, що охоплює людину, суспільство та державу.

Розвиток інформаційних технологій і соціальних мереж, а також глобалізація загроз на національному та міжнародному рівнях, що полегшує обмін інформацією, зумовлюють більш глибокий і багатогранний підхід до питань безпеки. Відтак, забезпечення інформаційної безпеки є ключовою і невід'ємною функцією держави в сучасних умовах.

Значення досліджень у сфері інформаційних війн та різноманітність їхніх проявів і стратегій, як у науковому, так і в практичному аспектах, підкреслюється тим, що сучасні держави активно застосовують інформаційно-психологічні операції з метою впливу на думки, переконання та процеси прийняття рішень суперника, маючи на меті досягнення власних політичних, економічних, військових та інших цілей.

Інакше кажучи, відбувається всебічний вплив на інформаційне середовище інших країн. Усвідомлення того, як застосовувати технології, соціальні мережі та ЗМІ, а також володіння цими навичками можуть слугувати потужним інструментом для впливу на думки та поведінку громадян, використання інформації у власних інтересах, а також для створення ефективної системи протидії ворожим інформаційно-психологічним операціям.

Необхідність створення ефективної системи протидії, яка б діяла на всіх рівнях і забезпечувала побудову "імунної" системи проти різноманітних методів та засобів інформаційно-психологічних операцій, набуває великої ваги для України при теперішніх обставинах, ніж будь-коли до цього.

Крім того, поглиблений аналіз особливостей та інструментів протидії інформаційно-психологічному впливу, який здійснює росія проти України, може стати основою для досліджень у таких сферах, як формування політичної свідомості, інформаційна гігієна, розвиток медіаграмотності серед населення, комунікаційні навички для журналістів у мирний час та в період надзвичайних ситуацій, прийняття рішень в міжнародних відносинах і інші дослідження, пов'язані з такими науками, як політологія, соціологія, психологія, кібербезпека та захист інформації тощо.

Вивчення, аналіз і критичний розгляд різноманітних аспектів протидії ІПСО мають велике значення для наукових досліджень у різних галузях, зокрема в міжнародних відносинах. У період активної воєнної агресії проти України, рф використовує комплексний підхід, включаючи широкий спектр засобів, таких як пропаганда, дезінформація, психологічний тиск, шантаж, залякування та інші, з метою впливу на громадську думку та підриву національної безпеки. Крім того, збільшилася кількість цільової аудиторії, для якої необхідно розробляти стратегії протидії негативному впливу з боку росії. Це вимагає прийняття нових рішень на рівнях державного, міжнародного та громадського управління для створення ефективної системи протидії інформаційно-психологічним операціям.

Вивчення інформаційно-психологічних операцій росії проти України має важливе значення для розуміння тактики та стратегії супротивника, захисту національної безпеки, впливу на міжнародну спільноту та запобігання поширенню подібних операцій інших держав в інформаційному просторі України. Таким чином, актуальність цієї теми дослідження обумовлена відповідністю її сучасному контексту безпекової політики, зростанням уваги до різних аспектів інформаційної безпеки у зв'язку з активним розвитком інформаційних технологій, розширенням кола потенційних загроз та інструментів інформаційно-психологічного впливу, а

також потребою у розробці ефективної системи протидії інформаційно-психологічним операціям, особливо у період повномасштабної воєнної агресії рф проти України та перспектив її удосконалення.

Мета дослідження полягає у вивченні особливостей, природи та технологій інформаційно-психологічних операцій, які здійснює російська федерація стосовно України, а також у розробці системи протидії цьому впливу у ході повномасштабної воєнної агресії росії проти України. Метою є також надання рекомендацій з удосконалення цієї системи на державному, громадському та міжнародному рівнях.

Реалізація поставленої мети передбачає виконання низки *завдань*:

проаналізувати сутність та історичний контекст виникнення терміну «інформаційно-психологічна операція»; взаємозв'язок між термінами «інформаційно-психологічна операція» та «інформаційна війна»; різновиди та методи інформаційно-психологічних операцій у контексті забезпечення безпеки людини, суспільства та держави;

дослідити основні теми та зміст інформаційно-психологічних операцій, які проводить росія щодо України; способи реалізації інформаційно-психологічних операцій росії проти України та фактори, які впливають на систему протидії інформаційно-психологічним операціям рф;

визначити основні принципи ІБ України у контексті протидії інформаційно-психологічним операціям; проаналізувати державну інформаційну політику України з метою протидії інформаційно-психологічним операціям під час повномасштабної воєнної агресії рф проти України;

проаналізувати співпрацю України з міжнародною спільнотою у сфері протидії інформаційно-психологічним операціям росії, здійснити аналіз матеріалів іноземних ЗМІ та сформулювати практичні рекомендації щодо вдосконалення системи протидії на міжнародному рівні;

розробити моделі життєздатності системи інформаційного протиборства в кіберпросторі та сформулювати практичні рекомендації з удосконалення системи протидії на рівні громадської участі.

Об'єктом дослідження є комплексні інформаційно-психологічні операції, що здійснюються російською федерацією в умовах повномасштабної воєнної агресії проти України.

Предметом дослідження є система протидії цим операціям на державному, міжнародному та громадянському рівнях з метою гарантування інформаційної безпеки України.

Хронологічні рамки дослідження охоплюють з 24 лютого 2022 року до сьогодення. Даний хронологічний інтервал дослідження обумовлений початком повномасштабної воєнної агресії російської федерації проти України. Важливо зазначити, що нижня межа дослідження є умовною, адже на момент завершення аналізу збройний конфлікт триває.

Методологія дослідження, представлена у кваліфікаційній роботі, базується на специфіці об'єкта та предмета дослідження, обумовлених його метою та визначеними завданнями. Застосування методу синтезу дозволило проаналізувати та оцінити процеси та явища, що стосуються формування інституційних засад інформаційної безпеки України, а також дослідити фактори, які вплинули на її становлення та розвиток. Окрім того, цей метод дав змогу розглянути низку механізмів системи протидії інформаційно-психологічним операціям.

З метою дослідження історичних аналогій та розуміння особливостей та методів проведення інформаційно-психологічних операцій РФ, було застосовано історичний метод. Додатково, для збору та систематизації факторів впливу цих операцій на масову свідомість, використовувались такі спеціалізовані методи: спостереження, контент-аналіз ЗМІ, когнітивне картування, а також соціологічний метод (інтерв'ю) з аудиторією громадської організації. Був проаналізований Індекс медіаграмотності населення та досліджена система протидії інформаційно-психологічним операціям росії на державному, громадському та міжнародному рівнях.

Комплексне застосування зазначених методів дослідження дало змогу ідентифікувати ключові фактори, що позитивно та негативно впливають на систему протидії інформаційним загрозам з боку рф. На основі отриманих даних

розроблено рекомендації щодо вдосконалення механізмів протидії інформаційному впливу на Україну.

Апробація результатів роботи здійснена на:

– VII Міжнародній науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS)», 26 квітня 2024, м. Київ;

– VI Міжнародній науково-методичній конференції «Передові технології реалізації освітніх ініціатив» 7 лютого 2023 року, м. Переяслав.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ МЕТОДІВ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ В КІБЕРПРОСТОРІ

1.1 Інформаційна війна як сукупність інформаційно-психологічних операцій

Протягом останніх десятиліть інформація стала одним з найважливіших інструментів у веденні війни. Її активно використовують для впливу на прийняття рішень опонентів, дезінформації громадськості та формування власного інформаційного поля (інформаційного фронту) на території ворожої держави.

Отже, науковці звернули увагу на появу нових форм війни, де інформація стає зброєю, інформаційний простір − полем бою, а цільовою аудиторією стає населення, що піддається впливу через залякування, шантаж, маніпуляції, залучення емоційного мислення та інше. В контексті гібридної або інформаційної війни терміни "психологічна операція" та "інформаційно-психологічна операція" набувають статусу легітимних елементів військової термінології.

Термін "інформаційно-психологічна операція" (ІПСО) часто ототожнюють з такими поняттями, як пропаганда, дезінформація, фейки, що свідчить про недостатнє розуміння його сутності. Для більш чіткого розуміння ІПСО необхідно розглянути його визначення в широкому та вузькому сенсі. У широкому сенсі ІПСО трактується як комплекс заходів, спрямованих на вплив на свідомість та поведінку людей. Ці заходи можуть включати в себе пропаганду, дезінформацію, фейки, а також інші інструменти інформаційного та психологічного впливу. У вузькому сенсі ІПСО визначається як спланована та цілеспрямована діяльність, що здійснюється з метою досягнення певних політичних, військових або інших цілей шляхом впливу на інформаційне поле та психологічний стан противника. Важливо підкреслити, що ІПСО відрізняється від пропаганди тим, що має чітко окреслені цілі та використовує широкий спектр методів впливу. Пропаганда ж, як правило,

спрямована на маніпулювання суспільною думкою та формування сприятливого для певної сторони іміджу.

Український науковець Михайло Туранський, автор численних праць з питань інформаційної та гібридної війни, визначає ІПСО як систему пропагандистських заходів, метою яких є протидія супротивнику. Ця система, за його твердженням, виступає специфічним видом зброї, аналогічно до традиційних військових інструментів.

У своїй роботі про інформаційно-психологічні війни, зосереджені на російсько-українській війні, Юрій Твердохліб розглядає термін "Інформаційно-психологічна операція" як комплекс заходів та дій з реалізації інформаційно-психологічного впливу, спрямовану як на внутрішню аудиторію, так і на ворожу, з метою формування певної моделі поведінки.

Слід зауважити, що для західної аудиторії досить поширеною є концепція розмежування інформаційних та психологічних операцій у відокремлені категорії. Зокрема, відповідно до документів Міністерства оборони США, інформаційні операції розглядаються як систематичне використання інформаційних можливостей під час проведення бойових дій, співпрацюючи з іншими складовими військової операції з метою впливу на процеси прийняття рішень противником або їх порушення.

Під психологічною операцією розуміється запланована діяльність, що включає комунікаційні та інші засоби, спрямована на досягнення політичних та військових цілей. Це тлумачення досить точно відображає сутність справи, оскільки інформаційно-психологічні операції впливають комплексно, а швидка цифровізація у всьому світі призводить до того, що технології стають засобом впливу не лише на комунікації, а й на поведінку, свідомість та дії населення, взаємно підсилюючи один одного. Згідно зі спільною доктриною союзників з психологічних операцій з 2014 року, психологічні операції розглядаються як заплановані заходи, що використовують методи комунікації та інші засоби для впливу на цільову аудиторію з метою зміни сприйняття, ставлення та поведінки з метою досягнення політичних та військових цілей.

Аналітичний центр "RAND Corporation" США визначає ІПСО як дії, спрямовані на збір тактичної інформації про противника та поширення пропаганди для досягнення конкурентної переваги. Ці операції включають інтеграцію різних інформаційних процесів, спрямованих на вплив на противника, і включають в себе психологічні впливи, заходи інформаційної безпеки, радіоелектронну війну, кінетичні дії та дії в комп'ютерних мережах. Ці заходи спрямовані на психологічний стан противників, їхнє розуміння ситуації та можливостей.

Також до інформаційних операцій входять заходи безпеки процесів прийняття власних рішень, інформації та інформаційних систем у країні [86, с. 85].

Серед ключових принципів інформаційно-психологічних операцій слід зазначити:

забезпечення вірогідності: використання правдивої та перевіреної інформації для підвищення довіри цільової аудиторії;

забезпечення упорядкованості, послідовності та узгодженості: всі заходи включаються до інформаційної стратегії;

розуміння: аналіз цільової аудиторії є ключовим інструментом для здійснення впливу на її сприйняття;

своєчасність та ефективність;

попередня оцінка: для здійснення впливу необхідно отримати інформацію про поточні моделі сприйняття цільової аудиторії, її відносини та поведінку.

Незважаючи на те, що термін "інформаційно-психологічна війна" з'явився порівняно недавно, її корені сягають далекого минулого. Історичні джерела свідчать про використання інформаційно-психологічних методів ще в епоху Олександра Македонського, Чингісхана та давньогрецької цивілізації.

Мета цих операцій завжди була однаковою, хоча характер, стратегії та об’єкти можуть змінюватися. Крім військових стратегій та тактик бою, у книзі «Мистецтво війни» Сунь Цзи містяться вказівки щодо отримання психологічної переваги над противником. Твердження Сунь Цзи про те, що війна ґрунтується на обмані, підкреслює психологічний аспект в бою над фізичним. Крім того, він вказує на те, що перемога у війні без бою є великою цінністю [6, с. 6-16; 36; 46].

Таким чином, держави використовують інформаційний вплив як інструмент, здатний впливати на хід війни або навіть на її результати. Людські ресурси не втрачаються, а використовуються з урахуванням досягнення бажаного результату. Крім того, існує можливість "перетягнути" сили противника на свій бік, використовуючи переконання, шантаж або психологічний тиск.

Інформаційно-психологічні операції використовувалися американськими військами під час війни за незалежність, коли повстанці поширювали листівки з закликами до ворожих солдатів покинути британську армію. Хоча ця кампанія була успішною, лише на початку XX століття вони стали широко використовуваним інструментом в арсеналі держав. Більшість науковців вважають Першу світову війну початком сучасних інформаційно-психологічних операцій, в значній мірі завдяки доступності засобів масової інформації, таких як радіо, сучасні друкарські верстати та революційні методи доставлення повідомлень цільовій аудиторії.

Під час Першої світової війни США провели свою першу організовану військову пропагандистську кампанію, створивши для цієї мети два спеціалізованих агентства. Інформаційно-психологічні операції широко використовувалися всіма сторонами під час Другої світової війни. Радіопередачі стали основним засобом передачі пропаганди ворожим військам. Японія використовувала відому "Токійську троянду" для транслювання музики та пропаганди союзникам. Німецька пропагандистка Мілдред Гілларс, більш відома як "Вісь Саллі", стала важливим інструментом психологічної війни. Інноваційне використання психологічної війни приписується радіопередачам Бі-Бі-Сі, яке почалося незадовго до очікуваного вторгнення Німеччини до Англії [27, с. 270].

На початку 1900-х років для інформаційно-психологічних операцій переважно використовувалися листівки, брошури, газети та радіо. Винахід нових технологій та продуктів показав, що інформаційно-психологічні операції завжди використовували нові технологічні рішення з метою охоплення найширшої аудиторії. Як і в звичайних воєнних діях, інновації та технологічний прогрес призвели до виникнення нових видів інформаційно-психологічних операцій. Зокрема, з появою соціальних мереж у сучасному світі інформаційно-психологічні

операції використовують платформи, такі як Twitter, Facebook, YouTube тощо [27, с. 274].

Незважаючи на те, що з часом змінилися терміни, методи, медіа, ситуації та цільова аудиторія, фундаментальна мета інформаційно-психологічних операцій (ІПСО) залишається незмінною: цілеспрямоване поширення інформації серед іноземної аудиторії з метою впливу на її емоції, мотиви, об'єктивність міркувань та, зрештою, на поведінку іноземних урядів, організацій, груп та окремих людей [13].

Суть поняття "інформаційно-психологічна операція" (ІПСО) полягає в цілеспрямованому впливі на свідомість та поведінку людей з метою досягнення конкретних цілей, що можуть включати зміну геополітичного становища, забезпечення безпеки або інші стратегічні завдання.

Інформаційно-психологічні операції (ІПСО) часто асоціюються з військовою або політичною стратегією, але їх застосування не обмежується лише цими сферами. Корпорації, медіаорганізації та інші групи також можуть використовувати ІПСО для формування громадської думки, впливу на критичне мислення та досягнення власних цілей. Таким чином, концепція "інформаційно-психологічної операції" охоплює широкий спектр заходів, спрямованих на маніпулювання свідомістю людей, підрив легітимності влади та просування стратегічних інтересів.

Незважаючи на значну кількість досліджень, у сучасній науковій літературі, як вітчизняній, так і зарубіжній, ще не існує єдиного комплексного підходу до розуміння поняття "інформаційна війна" (далі – ІВ). Різноманітність дефініцій та методів визначення цього терміну свідчить про його неоднозначність та постійну трансформацію. Проте, багатоваріантність формулювань поняття "інформаційна війна" дозволяє виділити в ньому два основні види: інформаційно-технічну та інформаційно-психологічну.

Український політичний експерт Є. Магда розглядає психологічну війну як один із різновидів інформаційної війни [16, с. 278]. У дослідженнях гібридної війни термін "психологічна війна" вживається ширше, охоплюючи комплекс

інформаційних, дипломатичних, економічних, воєнних, психофізичних, соціально-психологічних, спеціальних та інших заходів. Ці заходи проводяться як у мирний, так і воєнний час з метою зміни у бажаному напрямку психологічних характеристик людини, а також групових норм та суспільної свідомості в цілому [19; 50].

Проводячи порівняльний аналіз термінів "інформаційна війна" та "інформаційно-психологічна війна", дослідник О. Марунченко підкреслює, що в інформаційній війні об'єктом впливу є комп'ютерні системи та інформаційні мережі. Натомість, в інформаційно-психологічній війні до інформаційного аспекту додається психологічний компонент. У цьому випадку об'єктом впливу стає індивідуальна та масова свідомість [17]. Отже, доцільніше використовувати термін "інформаційно-психологічна війна", який слід розуміти як цілеспрямований вплив у вигляді поширення спеціальної інформації, що впливає на психіку та поведінку громадян певної країни або регіону.

Інформаційно-психологічні операції (ІПСО) – це комплекс цілеспрямованих методів та інструментів, що використовуються для впливу на свідомість та поведінку людей за допомогою інформації. Їхніми цілями можуть бути маніпулювання думками, емоціями та поведінкою людей, зміна їхніх переконань, установок та цінностей.

Згідно з В. Горбуліним, основні завдання інформаційних операцій полягають у:

– Збір інформації: Цей метод може включати отримання даних про громадян, підприємства, державні установи, а також збирання інформації про конкретні події, які відбуваються в країні або за її межами.

– Маніпулювання масовою свідомістю: Цей метод може бути спрямований на вплив на думки, почуття чи поведінку громадськості щодо певної теми, політичної партії, діяльності певної держави або іншої суспільно важливої проблеми. Він також може включати дезорієнтацію, дезінформацію та залякування.

– Підтримка певної політичної або соціальної кампанії: Цей метод може бути спрямований на підтримку кандидата чи певної соціальної групи під час виборів або протидію діяльності певної організації.

– Дискредитація опонентів: Цей метод використовується для підриву авторитету та репутації конкурентів, політичних противників або інших осіб, які вважаються загрозою.

– Підготовка до війни або терористичного акту: Інформаційно-психологічна війна може використовуватися для підготовки до збройного конфлікту або терористичного акту. Вона може включати пропаганду, дезінформацію та інші методи, спрямовані на деморалізацію противника, залякування населення та підрив довіри до влади [4, с. 17-20].

Цільові групи інформаційно-психологічних операцій включають окремих осіб (лідерів думок), соціальні групи, населення певної країни (як противників, так і їхніх партнерів), а також тимчасово окуповані території. Перед проведенням інформаційно-психологічної операції відбувається підготовка, під час якої особлива увага приділяється вивченню соціально-психологічних характеристик потенційних об'єктів впливу (цільової аудиторії) та їхніх психологічних профілів.

З цією метою активно використовуються дані соціологічних досліджень, статистика, а також вивчаються стереотипи, менталітет, традиції та забобони цільових груп. Проте, не завжди вдається досягти бажаного ефекту при реалізації інформаційних операцій. Для успішного інформаційно-психологічного впливу та досягнення визначених цілей необхідно провести ґрунтовне дослідження історії, культури та менталітету населення країни противника. Крім того, важливо розуміти, чи існує там свобода слова, як громадяни сприймають дані та факти, які джерела інформації є найбільш популярними, а також ймовірність співпраці з іноземними ЗМІ [22].

Важливо також проаналізувати наявність законодавчої бази, що регулює протидію пропаганді та дезінформації, а також досвід ведення інформаційної війни тією чи іншою державою. У Білій книзі 2007 року, присвяченій діяльності Служби безпеки та розвідувальних органів України, акцентовано увагу на тому, що

інформаційні операції здійснюються в певному ідеологічно орієнтованому соціальному середовищі. Тому для їхнього успішного проведення необхідна адаптація до цього середовища, уникнення створення бар'єрів, які блокують інформаційний вплив, або ж подолання цих бар'єрів для досягнення бажаного результату [1].

Інформаційна війна постає як універсальна модель протистояння, що охоплює всі сфери суспільного життя. Вона представлена широким спектром типів, одним з яких є інформаційно-психологічні операції. Багатогранність терміну "інформаційна війна" підкреслюється фактом її застосування та формалізації багатьма країнами світу протягом різних періодів відповідно до власних наукових концепцій.

Проведення інформаційної війни, паралельно з традиційним збройним протистоянням, трансформувалося в один із ключових інструментів накопичення політичного капіталу світовими лідерами та сприяло підвищенню індексу конкурентоспроможності держави за рахунок активного розвитку інформаційного суспільства. Інформаційна війна може виступати як самостійна форма впливу, не потребуючи введення воєнного чи надзвичайного стану. Яскравим прикладом цього є діяльність терористичних груп у Сирії, які успішно маніпулювали громадською думкою за допомогою пропаганди та психологічного тиску.

У 2016 році росія здійснила спробу втручання у виборчий процес США та країн Європи, які вона вважала ворожими, з метою дестабілізації демократичних інституцій та загострення суспільно-політичної напруги. США мають багатий досвід у веденні та дослідженні інформаційних війн. Під час Другої світової війни в Азії активно використовувалися пропаганда, психологічний тиск та інші методи інформаційного впливу з метою залучення населення до військових дій. Німеччина, яка на той час перебувала під владою Третього Рейху, поєднувала збройну агресію з інформаційною війною, використовуючи газети, листи, брошури, радіо, кіно та масові заходи для маніпулювання свідомістю населення, підтримки нацистського режиму та приховування власних воєнних злочинів.

Інформаційна війна являє собою комплексний підхід до ведення конфлікту, який використовує широкий спектр інструментів та методів, включаючи фейки, дезінформацію, психологічний тиск, пропаганду, кібератаки та інші. Ці елементи є складовими частинами інформаційно-психологічних операцій. Ймовірно, інформаційна війна має більш широке поняття, оскільки вона спрямована не лише на вплив на людей, але й на різні державні установи, новітні технології та канали розповсюдження інформації.

Об'єктом впливу інформаційно-психологічних операцій (ІПСО) є свідомість та поведінка населення [5, с. 87-93]. Ці операції використовують різноманітні методи впливу на психіку та поведінку противника, прагнучи змінити його переконання, емоції, поведінку та реакцію на інформаційні події та факти загалом. Такий тип інформаційної війни можна розглядати як свідомий вплив, оскільки свідомість громадян, зокрема противника, стає головним об'єктом впливу.

Інформаційна війна та інформаційно-психологічні операції (ІПСО) тісно пов'язані між собою і відіграють значну роль у сучасній геополітичній ситуації, чинячи суттєвий вплив на політичні, економічні та соціальні процеси.

1.2 Різновиди та прийоми інформаційно-психологічних впливів

Інформаційно-психологічні операції (ІПСО) являють собою комплекс заходів, спрямованих на вплив на психіку та поведінку людини шляхом використання інформації як інструменту впливу. Ці операції можуть мати як позитивні, так і негативні цілі, зокрема, забезпечення безпеки особистості, суспільства та держави. Залежно від мети та спрямованості, ІПСО поділяються на наступальні та оборонні види. Однак, як зазначає В. Горбулін, у більшості випадків інформаційні операції мають змішаний характер [4, с. 19].

Валентин Петрик пропонує класифікацію інформаційно-психологічних операцій за їх цілями, спрямованістю та націленістю. До основних типів належать:

– Операції, спрямовані проти державних діячів та інших суб'єктів, які приймають рішення в країні. Їх мета – дискредитувати, дезорієнтувати або деморалізувати ключові фігури політичного та військового керівництва.

– Компрометуючі операції. Їх мета – здобути компрометуючі матеріали на посадових осіб, політиків, представників бізнесу або інших осіб, які становлять інтерес для противника.

– Операції, спрямовані на дестабілізацію політичної або економічної ситуації. Їх мета – підірвати довіру до влади, спровокувати масові заворушення, економічні кризи або інші деструктивні процеси [21, с. 73].

За тривалістю проведення інформаційно-психологічні операції поділяються на:

– Короткострокові (1−2 тижні). Їх мета – досягти швидкого ефекту, наприклад, вплинути на результат виборів або зірвати конкретний захід.

– Середньострокові (2−4 тижні). Їх мета – поступово змінювати настрої в суспільстві, формувати нові стереотипи мислення або дестабілізувати ситуацію в певній сфері.

– Довгострокові (понад місяць). Їх мета – досягти глибоких та стійких змін у свідомості людей, сформувати нову ідеологію або систему цінностей [21, с. 71].

Загалом, інформаційно-психологічні операції здійснюються на довготривалій основі з метою непомітного або спланованого впливу на свідомість людини. Кінцевою метою може бути викликання не лише позитивних емоцій на користь ворога, але й, часто, поширення страху та паніки.

На стратегічному рівні інформаційно-психологічні операції реалізуються на глобальному або регіональному масштабах з метою підтримки національної стратегії. До них можуть належати дипломатичні ініціативи, політичні заяви, демонстрації сили та інші заходи, спрямовані на поширення потужного психологічного меседжу (наративу) про наміри та потенційні наслідки агресії.

На оперативному рівні інформаційно-психологічні операції здійснюються в межах чітко окресленої географічної зони з метою підтримки загального плану. Це

може включати реалізація дезінформаційних кампаній, спрямованих на дискредитацію військ противника та виклик страху і паніки серед населення.

На тактичному рівні інформаційно-психологічні операції мають за мету вплинути на сили противника та населення. Це реалізується через навмисне поширення неправдивої інформації щодо мобілізації, поранених чи загиблих; розповсюдження пропаганди, що підкреслює власну могуть та непереможність, а також через перекладання відповідальності за скоєні злочини на ворога [18, с. 188].

Одночасне проведення інформаційно-психологічних операцій на трьох рівнях може призвести до пришвидшення досягнення бажаного результату або створити моральний тиск на одну з цільових аудиторій. Це дає можливість швидше сформувати власний інформаційний фронт або середовище на території противника та його країн-партнерів. Наразі найпоширенішими методами, що використовуються в рамках інформаційно-психологічних операцій, є дезінформація, психологічний тиск, поширення чуток тощо. Їх зазвичай вважають ефективними інструментами пропаганди, інформаційної агресії, маніпулювання та інформаційного тероризму.

Дезінформація являє собою свідоме поширення хибної або неперевіреної інформації з метою введення людей в оману, маніпулювання їхніми переконаннями та думками для досягнення певних цілей, які можуть бути політичними, економічними, соціальними тощо. Петрик В. у своїй праці підкреслює, що дезінформацію можна розглядати як метод, що передбачає введення об'єкта впливу в оману щодо справжніх намірів для спонукання його до запрограмованих дій [21, с.73].

Психологічний тиск являє собою цілеспрямований вплив на особистість або групу людей з метою примусити їх до вчинення певних дій, прийняття певних рішень або зміни поведінки. До форм психологічного тиску належать: переслідування, шантаж, залякування, різноманітні реальні або уявні загрози, терористичні акції та інші подібні дії [3, с. 139].

Поширення чуток являє собою процес передачі непідтвердженої, неперевіреної або неправдивої інформації від однієї особи до іншої. Цей процес

може відбуватися як свідомо, з метою посилення впливу, підтримки певних поглядів або стосунків, так і ненавмисно, через нездатність або недбалість у верифікації фактів.

Поширення чуток має низку негативних наслідків, таких як ескалація конфліктів, спотворення реальності, паніка та підрив довіри між людьми. У контексті війн та конфліктів чутки можуть використовуватися як інструмент інформаційної війни для маніпулювання суспільством та зміни громадської думки.

Сьогодні соціальні мережі та веб-сайти новинних каналів, як регіональних, так і глобальних, слугують основними каналами поширення чуток. Наприклад, під час війни в Україні росія активно застосовує різноманітні методи інформаційно-психологічних операцій (ІПСО), зокрема розповсюдження неправдивої інформації про воєнні злочини українських військових, такі як вбивства мирних жителів та використання забороненої зброї, порушення прав громадян українською владою, а також про успіхи на тимчасово окупованих територіях [52]. Історичний аналіз свідчить про численні прецеденти використання подібних методів ІПСО.

Спостерігаються приклади обмеження свободи слова, жорсткого контролю друку новин та інформації, що суперечить офіційній ідеології, ревізії історії, фінансування рухів, які підтримують агресивну зовнішню політику, а також використання дітей у пропагандистських цілях. Яскравими історичними прикладами такої діяльності є режими Гітлера та Сталіна. Муаммар Каддафі, лідер Лівії, проводив масштабні кампанії з маніпулювання масовою свідомістю, що призводили до формування ворожості та ненависті до інших країн та народів.

Яскравим прикладом тривалого використання ІПСО слугує режим путіна. З початку повномасштабного вторгнення в Україну президент рф постійно погрожує застосуванням ядерної зброї, чинячи психологічний тиск з метою примусити Україну до капітуляції перед російськими вимогами та, за його словами, стримати втручання НАТО. У контексті забезпечення безпеки людини, суспільства і держави, інформаційно-психологічні операції можуть включати різноманітні види та методи. Проте мета таких операцій залишається незмінною: вплив на свідомість,

думку та поведінку цільової аудиторії з метою захисту власних інтересів та безпеки.

Функціонал ІПСО в даному контексті полягає у протидії радикальним переконанням та поглядам, які суперечать загальноприйнятим нормам і цінностям суспільства. Досягається це за допомогою комплексу заходів, таких як: контрпропаганда, створення інформаційної бази з альтернативними переконаннями, кіберзахист та попередження кібератак на державному рівні, фактчекінг та спростування дезінформації, а також програми з підвищення обізнаності та медіаграмотності громадян. Окрім цього, ІПСО здійснює моніторинг та аналіз інформаційного простору противника.

Функціональне призначення інформаційно-психологічних операцій полягає у формуванні політичної свідомості, зміцненні довіри громадян до державних інституцій та лідерів думок, протидії дезінформаційним кампаніям, а також у мобілізації населення в надзвичайних ситуаціях. Хоча подібні операції застосовуються протягом тисячоліть, поняття "інформаційно-психологічна операція" досі залишається предметом дискусій серед науковців, деякі з яких вважають інформаційну війну сукупністю інформаційно-психологічних операцій.

Загалом, відношення між поняттями "інформаційна війна" і "інформаційно-психологічна операція" полягає в тому, що ІПСО є складовою частиною стратегій і тактик, використовуваних у межах інформаційної війни. Вона слугує інструментом для досягнення більш широких цілей інформаційної війни, зокрема, залучення громадської думки на свій бік, дискредитації опонентів або мобілізації підтримки.

Узагальнено, інформаційно-психологічні операції (ІПСО) визначаються як процес або комплексний підхід, спрямований на вплив на поведінку або психіку цільової аудиторії, такої як населення країни-ворога, країн-партнерів, власних громадян і т. д. Початки концепції ІПСО можна відстежити до Першої світової війни, коли інформаційно-психологічна війна була широко використана. З появою цифрової ери та широкого поширення Інтернету і соціальних мереж використання інформаційно-психологічних операцій стало ще поширенішим і модернізованим.

Сучасні державні та приватні суб'єкти використовують інформаційно-психологічні операції для впливу на громадську думку, дискредитації опозиційних політичних лідерів, порушення стабільності демократичних процесів та перетворення влади в деяких країнах. Негативний вплив таких операцій може мати серйозні наслідки для безпеки людини, суспільства та держави.

Розповсюдження дезінформації, психологічний тиск і поширення чуток можуть спричинити масову паніку, погіршити взаєморозуміння між країнами та іншими суб'єктами міжнародних відносин, збільшити напруження і конфлікти. Проте вони також можуть бути використані для контрпропаганди, розвіювання чуток, запобігання конфліктам і фактчекінгу.

1.3 Виявлення негативних наслідків інформаційно-психологічних операцій

З огляду на недавні слід зазначити, що Інтернет поступово став джерелом загроз для інформаційної безпеки людини, суспільства та держави. Поширення сумнівного та необ'єктивного контенту в глобальній мережі разом із застосуванням технологій інформаційно-психологічного впливу на свідомість громадян може призвести до збільшення невдоволення діючою державною владою, міжнаціональних конфліктів, соціальної агресії та інших негативних наслідків.

У контексті глобалізації, прогрес у сфері інформаційно-комунікаційних технологій сприяє тому, що у сучасних міжнародних конфліктах все частіше використовуються стратегії, які включають широкий спектр політичних, економічних та інформаційних заходів. Ці заходи часто підкріплюються військовою силою і відомі як "гібридні" методи, які дозволяють досягати політичних амбіцій у конфлікті з мінімальним прямим військовим втручанням.

Тролінг, який є однією з виразних форм інформаційно-психологічного впливу в рамках інформаційно-психологічних операцій, полягає у створенні та поширенні в мережі Інтернет провокативних дописів. Ця діяльність має на меті

загострення соціальних конфліктів через порушення етичних стандартів комунікацій у цифровому просторі.

Для звичайного користувача Інтернету відстеження тролінгу зазвичай не складає труднощів. Однак складніше розрізнити між випадковим чи несвідомим спотворенням інформації та навмисними маніпуляціями. Обсяги інформації в Інтернеті роблять ручний пошук тролінгу часомістким та вимагають значних зусиль. У зв'язку з цим в області дослідження технологій, що впливають на учасників соціальних мереж, важливим є розробка методів для автоматизації процесу ідентифікації тролінгу.

На основі аналізу наукових праць А. Манойла (2003), О. Литвиненка (2003), Г. Почепцова (2001), О. Поляруша (2008) та С. Расторгуєва (1999), стає зрозуміло, що до сьогодні вчені не прийшли до єдиної думки стосовно визначення інформаційно-психологічного впливу та його основних форм. Дослідження Д. Ланде і Фурашева (2009) фокусуються на розробці алгоритмів для автоматизованої обробки мас-медійних матеріалів, що виявляють інформаційні операції та війни, але поки що не знайшли практичного застосування. Методологічні підходи В. Панченко та В. Полевого (2011), спрямовані на ідентифікацію інформаційно-психологічних впливів у онлайн спільнотах, залишаються лише описовими та не містять конкретної методики впровадження.

Аналіз показав, що на сучасному етапі недостатньо уваги приділяється проблемі визначення інформаційно-психологічних впливів в соціальних мережах. Тому можна зазначити, що розробка методів і засобів виявлення інформаційно-психологічних впливів є актуальною задачею.

В сучасних збройних конфліктах головною зброєю для досягнення політичних амбіцій стала інформація, що є ключовим елементом гібридних воєн. Ці війни характеризуються використанням інформаційно-психологічних впливів, які полягають у цілеспрямованому створенні та розповсюдженні інформації, спрямованої на безпосередній вплив, чи то позитивний, чи негативний, на психіку та поведінку громадян, державного керівництва та військових, а також на загальний стан інформаційно-психологічного середовища суспільства.

Інформаційно-психологічні маніпуляції, здійснювані в інтересах окремих осіб або груп, на шкоду іншим, є особливою формою керування, яка стає небезпечною, коли вона відбувається приховано і приносить вигоду лише її організаторам. Одним з найбільш значущих джерел такого небезпечного впливу, що постійно та все активніше й потужніше діє, є держави, які проводять масштабні психологічні операції проти населення або окремих соціальних груп інших країн, обраних як об'єкти впливу.

Інформаційно-психологічний вплив (ІПВ) має за мету зміну установок особистості. Цей вид впливу спрямований на емоційну сферу свідомості та характеризується нецілеспрямованим сприйняттям та запам'ятовуванням інформації, а також низьким рівнем усвідомлення змісту впливу. Інформація, що поширюється російськими ЗМІ на території України, зокрема у східних областях, є свідомим спотворенням дійсності. Механізм ІПВ ґрунтується на маніпуляції свідомістю мас шляхом впровадження дезінформації.

Деструктивний інформаційно-психологічний вплив (ІПВ) ґрунтується на комплексі заходів, спрямованих на маніпулювання свідомістю людей. До цих заходів належать:

– Широке поширення дезінформації: фейкові новини, відредаговані відео, брехливі або перекручені факти.

– Умисне приховування правди: обмеження доступу до достовірної інформації, роблячи людей схильними до дезінформації.

– Інформаційний шум: бомбардування людей великою кількістю інформації, що ускладнює розрізнення правди і брехні.

Ці дії штучно загострюють соціально-політичну та безпекову напругу в Україні, що може призвести до дестабілізації суспільства, зростання екстремізму та загрози територіальній цілісності держави.

Деструктивний інформаційно-психологічний вплив (ІПВ) реалізується шляхом проведення інформаційно-психологічних операцій (ІПО). В роботі "Операції інформаційно-психологічної війни" (2005) автори В. Вепрінцев, А. Манойло, А. Петренко та Д. Фролов дають чітке визначення ІПО як комплексу

скоординованих та взаємопов'язаних заходів з маніпулювання інформацією. Ці заходи здійснюються за єдиним планом з метою досягнення та утримання переваги шляхом впливу на інформаційні процеси в системах противника.

З метою досягнення визначених цілей застосовується широкий спектр каналів комунікації, що охоплює як традиційні, так і електронні ЗМІ.

Пріоритетними каналами інформаційно-психологічного впливу (ІПВ) є телебачення, Інтернет та соціальні мережі. У рамках цих каналів використовуються різноманітні методи ІПВ, починаючи від спотворення фактів і закінчуючи відкритою брехнею («фейками»).

У гібридних конфліктах соціальні мережі використовуються як знаряддя бойової діяльності. З урахуванням потенційних інформаційних загроз особливо небезпечним є активний участь тролів у інтернет-спілкуванні. Їх завдання включає провокації та поширення конфліктів, включаючи упокорення чи образи інших учасників дискусії.

Отже, соцмережі являються ефективним інструментом впливу на суспільно-політичні процеси в державі. Тому виявлення негативного інформаційно-психологічного впливу в соціальних мережах в умовах глобалізації інформаційного простору та гібридизації військових конфліктів залишається однією з найбільш актуальних проблем, яка потребує вирішення.

Український ринок програмного забезпечення характеризується наступним чином: 90% ринку зайнято програмним забезпеченням західних фірм, тоді як лише 10% становлять українські розробки. Н На цьому ринку діє понад 200 компаній, що мають певний зв'язок з програмним забезпеченням. Проте більшість з них займаються дистрибуцією програмних продуктів з-за кордону.

За результатами моніторингу забезпечення органів державної влади програмним забезпеченням встановлено, що вони використовують понад 1700 тис. комп'ютерних програм.

Згідно з даними онлайн-опитування про використання програмного забезпечення в органах виконавчої влади, інформація була отримана від 60% центральних органів виконавчої влади, що становить понад 1200 тис. примірників

комп'ютерних програм. Аналіз проведено на основі даних, наданих органами державної влади, які використовують понад 1100 тис. примірників програмного забезпечення, а також даних від обласних державних адміністрацій, де використовується понад 60 тис. примірників.

У роботі органів державної влади використовуються такі програмні засоби інформаційної безпеки, як Putty, Comodo, Symantec та Гриф. Це свідчить про те, що такі органи не використовують програмне забезпечення для аналізу великого обсягу даних у сфері кібербезпеки. На внутрішньому ринку представлено програмне забезпечення для обробки великих обсягів даних (Big Data) з метою генерування звітів, які відображають думки споживачів, клієнтів та конкурентів щодо різних брендів.

Застосування програм для визначення тональності тексту у сфері кібербезпеки наразі не поширене.

Аналіз текстових даних з соціальних мереж, зважаючи на значний обсяг інформації, неможливо виконати вручну. Цей процес автоматизовано за допомогою спеціальних сервісів або програмного забезпечення, доступного як на платній, так і на безкоштовній основі.

Технології обробки природної мови (НМ) давно вийшли за межі нововведень. Розроблено методи синтаксичного та семантичного аналізу текстів, а також модулі для вирішення конкретних завдань у цій галузі. Провідні технологічні компанії (IBM, Microsoft, Google, Apple, Facebook та інші) активно розробляють API-сервіси та інтегрують НМ у свої проекти. Однак вітчизняні компанії практично не інвестують у розвиток цих технологій.

Інформаційні повідомлення, які використовуються для здійснення інформаційно-психологічного впливу, мають емоційне забарвлення, що спрямоване на інформування та стимулювання певних емоцій у цільової аудиторії з метою регулювання її поведінки. Тому для виявлення інформаційно-психологічних впливів необхідно використовувати програми для аналізу емоційного забарвлення повідомлень.

Також більшість наявних програмних засобів розроблені переважно для іноземних мов. Переважна частина призначені для відстеження відгуків про товари, послуги, бренди і особистості, а інші проводять аналіз лише по певних реченнях. У зв’язку з цим, особливу увагу привертає важливість даного дослідження, оскільки поки що немає поширених програмних засобів для автоматичної оцінки тональності текстів на російській мові для виявлення в них інформаційно-психологічних маніпуляцій.

На сучасному етапі важливу роль у процесах комунікації суспільства відіграють соціальні мережі в Інтернеті, які надають учасникам віртуальних спільнот нові можливості взаємодії.

Соціальні мережі в Інтернеті все ширше та активніше використовуються для здійснення інформаційно-психологічного впливу. Ці платформи надають широкі можливості для впливу на формування громадської думки з різних актуальних питань, включаючи політичні, економічні та військові рішення, а також вплив на інформаційні ресурси противника та розповсюдження спеціально підготовленої інформації (дезінформації).

У зв'язку із загальним поширенням віртуальних спільнот, вони стали ефективним інструментом для проведення інформаційних операцій проти окремих осіб, суспільства та держави. Ці процеси в соціальних мережах викликають зростаючий інтерес у наукових дослідженнях, однак темп розвитку теоретичних аспектів значно поступається темпам розвитку самих соціальних мереж.

Для виявлення ознак інформаційно-психологічних впливів часто використовуються методи, що загалом відомі як "аналіз емоційного відтінку тексту".

У роботі використовується термін "аналіз емоційного відтінку тексту" як переклад оригінального терміну "sentiment analysis", який також часто перекладається як "аналіз тональності тексту". Аналіз емоційного відтінку тексту - це завдання автоматичного аналізу думок та емоційно забарвленої лексики, виражених у тексті.

Аналіз тональності текстової інформації за допомогою природної мови поділяють на дві основні групи методів: інженерно-лінгвістичні та ті, що ґрунтуються на основі машинного навчання. Інженерно-лінгвістичні методи використовують спеціальні тональні словники, які попередньо підготували експерти-лінгвісти, а також лінгвістичні правила для аналізу текстових фрагментів.

Методи машинного навчання, серед яких можна виділити метод Байєса, метод опорних векторів, метод k-найближчого сусіда, а також регресію, відіграють критичну роль у визначенні тональності тексту. Ці методи базуються на математичних моделях, які дозволяють автоматично визначати оптимальний набір параметрів для вирішення конкретних завдань. Варто зазначити наявність комбінованих (гібридних) методів, які поєднують в собі елементи інженерно-лінгвістичного аналізу і методи машинного навчання.

В дослідженнях, що стосуються класифікації текстів і різного контенту, все частіше вказується на переваги технологій, що базуються на нейромережевих методах і машинному навчанні. Ці методи автоматично аналізують тексти на природній мові, виявляючи зв'язки між словами та їх категоріями. Вони знижують трудомісткість класифікації та підвищують якість рішень у багатьох подібних завданнях, зменшуючи кількість помилок і труднощі, що виникають при роботі з великим обсягом інформації.

Дослідження методів автоматичного аналізу настроїв у соціальних мережах показали, що найбільш ефективними для виявлення інформаційно-психологічних впливів у текстах є нейронні мережі. Особливістю їх використання є те, що вони не потребують складання словників або обов'язкової попередньої лінгвістичної обробки текстів. Крім того, вони можуть застосовуватися до різних типів даних і здатні класифікувати інформацію за декількома категоріями, що сприяє виявленню різних типів інформаційно-психологічних впливів.

Також для розв'язання цієї задачі можна використовувати інженерно-лінгвістичні методи, метод опорних векторів, дерева прийняття рішень та наївний класифікатор Байєса. Однак метод опорних векторів має свій недолік – він проводить лише бінарну класифікацію, розділяючи дані лише на дві категорії: дані

без інформаційно-психологічних впливів та дані з такими впливами. Слабка сторона наївного класифікатора Байєса полягає у неможливості врахування взаємозв'язку результату з комбінацією слів. Спільним недостатком інженерно-лінгвістичних методів та наївного класифікатора Байєса є необхідність підготовки словників, що потребує тісної кооперації з лінгвістами.

Проте, важливо зауважити, що жоден із методів автоматичної класифікації тексту не може гарантувати абсолютно точних результатів. Помилки цих методів зазвичай пояснюються наступними проблемами: орфографічними помилками у тексті, відсутністю зв'язків у тексті. Щоб підвищити ефективність класифікаторів необхідно автоматично виправляти орфографічні помилки та постійно вдосконалювати навчальні набори та словники.

Висновки до першого розділу

У даному розділі було розглянуто основні аспекти інформаційно-психологічних операцій та методів їх протидії. Виявлено, що інформаційна війна є сукупністю інформаційно-психологічних операцій, спрямованих на вплив на свідомість та поведінку цільової аудиторії. В розділі проаналізовано різновиди та прийоми інформаційно-психологічних впливів, зокрема дезінформацію, маніпуляцію, психологічний тиск тощо. Крім того, розглянуто методи виявлення негативних наслідків інформаційно-психологічних операцій, такі як аналіз впливу на суспільну думку, психологічні наслідки для цільової аудиторії та інші аспекти. Ці дані є важливими для подальшого розроблення стратегій протидії інформаційно-психологічному впливу в кіберпросторі.

РОЗДІЛ 2.
ВИВЧЕННЯ СПОСОБІВ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ В КІБЕРПРОСТОРІ

2.1 Аналіз методів виявлення інформаційно-психологічного впливу в кіберпросторі

Зміна уявлення про світ соціальної частини, яка перебуває в стійкій фазі, майже неможлива [4]. Інформаційні операції є найбільш ефективними, коли вони спрямовані на найбільш вразливі частини соціотехнічних систем, особливо на людську свідомість, змушуючи її перейти у нестійкий стан.

Впливовість інформаційних інструментів значною мірою залежить від урахування психосоціальних особливостей як окремих індивідів, так і цілих суспільств. Ефективне моделювання поведінки людини чи групи передбачає глибоке розуміння їхніх психологічних характеристик та вподобань. В рамках інформаційної війни емоційні компоненти, такі як іронія, сарказм, підозрілість, байдужість та атаки на особистість, використовуються як маніпулятивні інструменти. Окрім цього, застосовуються методи формування інформаційних впливів, які включають:

– збурення ситуації, в результаті чого в країні виник конфлікт;

– деградація, розпад країни з перетворенням її на "недієздатну" державу;

– зміна політичної влади на агресорський режим. Тактики включають:

– виведення людини з рівноваги, щоб змінити її уявлення про світ;

– примусове викликання агресії, що призводить до втрати авторитету;

– компрометація ресурсу шляхом розпалювання агресії всередині спільноти;

– спроба переконати людину, що оточуючі думають так, як хоче агресор;

– поширення думки, що всі навколо віддані агресору, що призводить до заміни громадської думки;

– блокування ресурсу через використання нецензурної лексики та мови ненависті;

– компрометація ресурсу за допомогою фейків та перекручених фактів;

– засмічення інформаційного простору для відволікання уваги від основної теми і дискредитації ресурсу.

Тим часом, ефективність мемів збільшується завдяки багаторазовому розповсюдженню повідомлення, включаючи його різні варіанти [5].

Протидія інформаційно-психологічному впливу в ході ІВ:

Етап 1. Спостереження за інформаційним простором для виявлення ворожих інформаційних мемів.

Етап 2. Встановлення набору інформаційних мемів.

Етап 3. Аналіз можливих ризиків після здійснення інформаційно-психологічних операцій.

Етап 4. Впровадження заходів захисту, таких як блокування облікових записів та повідомлень з явно провокативним змістом, включаючи законодавчі ініціативи.

Етап 5. Стимулювання саморегуляції особистості (фільтрування інформаційних мемів, збереження культурного коду тощо).

2.2 Аналіз стратегій боротьби з інформаційним впливом супротивника в контексті ІВ

Сьогодні інформація стала однією з найнебезпечніших збройних систем. Її вплив на маси надзвичайно великий, і успішне маніпулювання нею може призвести до досягнення будь-якої мети: від знищення опонента до виклику війни чи прибирання конкурентів з дороги. Масштаби руйнівного впливу інформаційно-психологічної війни сьогодні настільки великі, що ставлять під сумнів не лише незалежність переможеної держави, а й сам факт існування її народу як національної спільноти.

Термін "інформаційна війна" вперше був застосований американським експертом Томасом Роном у звіті, який він підготував для компанії Boeing у 1976 році. Звіт мав назву "Системи зброї і інформаційна війна". Рон відзначив, що інформаційна інфраструктура стає ключовим компонентом американської економіки, а водночас є дуже вразливою як у часи війни, так і в мирний час.

Під терміном "інформаційна війна" розуміється комплекс методів та стратегій, спрямованих на цілеспрямований вплив на суспільні відносини, інформаційні ресурси, аналітичні та технічні системи, а також системи формування масової свідомості та психіки окремої особи. Цей вплив здійснюється за допомогою різноманітних передових технологій та інформаційних ресурсів для послаблення моральних і матеріальних ресурсів опонента або конкурента й одночасного зміцнення власних позицій. Інформаційна війна включає в себе пропагандистські впливи на ідеологічному та емоційному рівнях.

В умовах стрімкої інформатизації суспільства та активного впровадження сучасних інформаційних технологій у сфері управління, зокрема військового, а також у зв'язку з розвитком електронних державних ресурсів для роботи міністерств, відомств та виконавчих органів, зростає актуальність питання захисту державної інформації від витоку, несанкціонованого доступу та втручання у вигляді введення хибних даних до державних електронних ресурсів. Ці заходи спрямовані на мінімізацію ризиків інформаційного впливу на різноманітні державні системи управління як у мирний час, так і в умовах воєнних дій.

У рамках інформаційної війни визначаються три основні цілі:

1. Контроль над інформаційним простором та захист власної інформації від ворожих впливів.

2. Використання контролю над інформаційним простором для здійснення інформаційних атак на противника.

3. Підвищення загальної ефективності Збройних Сил за рахунок широкого впровадження військових інформаційних технологій.

Існують різноманітні методи протидії інформаційним війнам та захисту інформаційного простору:

1. Пряме спростування.

2. Виявлення та ліквідація потенційних каналів проникнення інформації.

3. Непряме спростування, що включає:

– Узагальнення сумнівів у джерелі інформації.

– Абсурдизація звинувачень.

– Асоціація джерела інформації з негативними подіями.

– Введення додаткових фактів, які можна легко спростувати.

4. Відволікання уваги.

Можливі стратегії включають:

– Перенаправлення потужностей опонента на інші завдання, наприклад, відбиття інформаційної атаки або відволікання його уваги на інші події.

– Введення нової сенсаційної інформації для зміни уваги аудиторії.

– Зосередження уваги аудиторії на незначних аспектах проблеми, що відвертає увагу від головного.

– Мовчання як відповідь на атаку.

– Мінімізація впливу шляхом наголошення на правдивих фактах.

– Дискредитація шляхом підриву авторитету або іміджу джерела негативної інформації.

Інші можливі варіанти включають:

– Розголошення компромату.

– Публічна похвала з негативним підтекстом.

– Невмотивоване освистування або критика.

– Громадське обурення.

– Публікація нейтральної або позитивної інформації, що переважає негатив.

– Подання ситуації до абсурду, що призводить до імунітету аудиторії до негативного впливу.

Залежно від конкретної операції, інформаційна війна включає різні складові:

– Захист власних соціальних та інформаційних систем від інформаційного впливу противника.

– Боротьба з державними системами управління противника різного призначення.

– Війна у сфері політичної та економічної інформації.

– Психологічна війна.

– Комп'ютерна війна.

– Кібернетична війна.

Глибоке розуміння методології ведення інформаційної війни в сучасному світі, всебічний аналіз напрямків застосування інформаційних інструментів та їх впливу на державні системи управління та різні соціальні структури, а також вивчення особливостей національної культури противника є ключовими факторами для розробки ефективних методів захисту власних інформаційно-технічних та соціальних систем від інформаційної агресії. Ретельне вивчення та впровадження цих методів дозволить мінімізувати негативний вплив інформаційної війни на українське суспільство та державу, а також сприятиме досягненню перемоги у цьому протистоянні.

З урахуванням високого рівня небезпеки, яку несуть суб'єкти інформаційних війн для всіх держав, їх владних органів, державних структур та міжнародних організацій, важливо розробити відповідну нормативно-правову базу, враховуючи всі можливості сучасних інформаційно-телекомунікаційних технологій.

Особлива увага має бути приділена розвитку і впровадженню інформаційно-телекомунікаційних технологій в сфері державного управління, підвищенню кваліфікації органів влади та місцевого самоврядування з метою ефективного використання сучасних управлінських технологій та підтримки конструктивної взаємодії з громадськістю.

Також важливо вирішити проблему низького рівня підготовки кадрів у галузі інформаційно-телекомунікаційних технологій. Для досягнення цього необхідно розробити комплекс заходів з підвищення кваліфікації фахівців у цій галузі.

2.3 Протидія сучасним інформаційно-психологічним впливам

Значним позитивним фактором у формуванні системи протидії інформаційно-психологічному впливу з боку Російської Федерації є співпраця з міжнародними ЗМІ. Проведений контент-аналіз деяких іноземних агенцій (Think Tanks) та видавництв, зокрема «The Wall Street Journal» [20], «The Telegraph» [29], «BBC News» [21] і «The Atlantic Council» [19], показав, що з початку повномасштабного вторгнення ці агенції активно публікують статті англійською мовою, присвячені таким темам, як створення або посилення антипутінської коаліції, злочини російських окупантів, ядерний та інший шантаж з боку росії, реальні результати бойових дій на лінії фронту, дезінформаційні кампанії росії в різних країнах світу та інші.

Аудиторією, на яку спрямовані ці агенції, є українці та міжнародна спільнота. Включення громадян росії до цільової аудиторії надасть їм доступ до точної та правдивої інформації, що позитивно позначиться на формуванні стійкості та свідомості людей. Крім того, майже кожна з цих агенцій створила розділи (комплексні онлайн-видання) на своїх офіційних сайтах, присвячені Україні, зокрема «Ukraine», «War in Ukraine» та «UkraineAlert», де приблизно кожні 2-3 дні з'являються публікації про події в Україні [19; 21; 29; 80].

Важливу роль у протидії дезінформаційній кампанії росії та формуванні зваженого громадського дискурсу відіграють публічні заходи та інформаційні матеріали, що публікуються на платформі Atlantic Council. Цей авторитетний аналітичний центр організовує дискусії за участю американських, європейських та українських лідерів та експертів, де обговорюються актуальні питання, пов'язані з війною в Україні, та спростовуються російські фейки. На сторінках Atlantic Council публікуються статті відомих українських політиків, таких як Олексій Резніков (Міністр оборони України) та Олексій Гончаренко (Народний депутат України), а також експертні оцінки та аналітичні матеріали від Олени Хоменко, Ольги Айвазовської та інших авторів. Додатково, платформа публікує звернення Президента України Володимира Зеленського, його промови та виступи

високопосадовців, зокрема керівника Офісу Президента України Андрія Єрмака [19]. Співпраця з виданням The Wall Street Journal полягає в тому, що кореспонденти та журналісти цього видання самостійно проводять дослідження та документують злочини російських окупантів на території України [20].

Це дозволяє міжнародній громадськості ставитися до новин з ще більшою довірою, мінімізує негативний вплив факторів на систему протидії російській дезінформації і перешкоджає російським журналістам у розповсюдженні своїх наративів через ці видання. В цілому співпраця з міжнародними ЗМІ допомагає об'єднати демократії та протистояти російській пропаганді і імперіалізму. Окрім цього, разом із зусиллями окремих країн, міжнародні організації здійснюють перевірку фактів, щоб протистояти російській дезінформації.

Наприклад, НАТО має свою власну систему для спростування шкідливих російських наративів [20]. Подібно діє проєкт EUvsDisinfo, що входить до складу Європейської служби зовнішніх справ (EEAS). Основне завдання цього проєкту – прогнозувати, вивчати та реагувати на постійні кампанії дезінформації з боку росії, які впливають на Європейський Союз, його члени та регіональні країни [16].

Важливим етапом стало долучення нашої держави у вересні 2022 року до програми "Цифрова Європа". Ця програма спрямована на розвиток цифрових технологій для підприємств, громадян та державних установ. Цей крок важливий для поліпшення системи реагування на ІПСО за допомогою активного впровадження цифрових технологій, штучного інтелекту та кібербезпеки. Цифрові технології та інфраструктура відіграють вирішальну роль у забезпеченні інформаційної безпеки країни [23, с. 147-150; 41].

Фінансова підтримка міжнародної спільноти є надзвичайно важливою, оскільки вона може запобігти поширенню інформаційно-психологічних операцій рф не лише на територію України або тимчасово окуповані території, а й у інформаційному просторі інших країн світу. Протидія впливу росії на країни Африки, Латинської Америки та колишні радянські республіки, а також її участь у міжнародних змаганнях, олімпіадах, кінофестивалях тощо є проблемними аспектами. Як відзначалося раніше, культурні проекти від часів СРСР були

важливим інструментом впливу з метою дискредитації, утисків та поширення власної пропаганди.

Можливості зміцнення міжнародного співробітництва України у протидії інформаційно-психологічним операціям рф включають такі напрями:

– Розширення міжнародної співпраці та обмін досвідом з країнами, які успішно протистоять ІПСО.

– Залучення міжнародних партнерів для підтримки стійкості України, включаючи співпрацю з Європейським Союзом та НАТО.

– Активна взаємодія з аналітичними центрами та ЗМІ за кордоном з метою протидії кремлівській пропаганді.

– Створення або підтримка українських агенцій та видань за кордоном, організація ефірів та власних програм за кордоном.

– Збільшення кількості іноземних медіаканалів в Україні, зокрема локальних медіа.

– Забезпечення Міністерства закордонних справ та Міністерства інформаційної політики можливістю спілкування з закордонною аудиторією та виходу в ефір.

– Припинення розповсюдження інформаційно-психологічних операцій рф за кордоном та відсторонення Росії від участі в міжнародних змаганнях та конкурсах.

– Розвиток культурної дипломатії України для підвищення міжнародного іміджу країни та протидії інформаційно-психологічному впливу рф через реалізацію культурних проектів на міжнародній арені.

Віртуальні спільноти є не лише об’єктами, але й інструментами зовнішнього інформаційного управління, а також ареною інформаційного протиборства на різних рівнях. Вони стали ідеальним засобом для здійснення інформаційно-психологічного впливу на національні інтереси держави та суспільство в цілому в інформаційному та кіберпросторі. Щоб попереджувати та протидіяти розколам у суспільстві, необхідно постійно моніторити наявність негативного інформаційно-психологічного впливу в спільнотах і мати можливість ефективно протистояти йому.

Для виявлення інформаційно-психологічного впливу в соціальних мережах застосовуються різні методи, що базуються на аналізі лексем та машинному навчанні з учителем. Найпоширенішими з них є метод опорних векторів, наївний класифікатор Байєса, дерева прийняття рішень, метод максимальної ентропії та нейронні мережі. Кожен з цих методів має свої сильні та слабкі сторони, які необхідно враховувати при виборі оптимального інструменту для конкретного завдання. Згідно з результатами досліджень, найбільш ефективним методом виявлення інформаційно-психологічного впливу є застосування нейронних мереж у машинному навчанні. Цей метод демонструє високу точність та стійкість до шуму, що робить його цінним інструментом для аналізу даних соціальних мереж.

Застосування цього методу не вимагає попередньої обробки тексту та складання словників. Він дозволяє класифікувати інформацію за кількома різними категоріями безпосередньо. Це дозволяє виявляти різні види інформаційно-психологічного впливу, оновлюючи мережу при отриманні нової інформації, враховуючи оновлення контенту в соціальних мережах.

Досліджено, що, на відміну від нейронних мереж, застосування дерев прийняття рішень для виявлення інформаційно-психологічного впливу обмежено на практиці. Це обумовлено складністю підтримки інкрементного навчання. Можна побудувати дерево рішень для великого обсягу даних. Однак не можливо враховувати нові повідомлення без повторного навчання.

Соціальні мережі стали ключовими платформами для інформаційного протиборства, через них здійснюється вплив на віртуальні спільноти та окремих громадян. Це призводить до проведення інформаційних операцій проти осіб, суспільства та держави. Під інформаційно-психологічним впливом розуміється вплив на свідомість особи та населення з метою зміни їхньої поведінки та/або світогляду. Базовими методами такого впливу є переконання і нав'язування.

Приблизно 80% користувачів довіряють інформації, що публікується в соціальних мережах. Для попередження та протидії збурень серед суспільства необхідно постійно відслідковувати присутність негативного впливу на свідомість віртуальних спільнот.

Проте цей процес є складним і вимагає значних зусиль та часу. Цих обмежень можна уникнути, використовуючи методи машинного навчання та методи на основі аналізу лексики.

Вплив на психологічний стан людей в соціальних мережах досліджується в численних наукових працях [1-5]. Автори цих робіт пропонують різні методи автоматичного аналізу контенту, які дозволяють виявляти ознаки інформаційно-психологічного впливу. До таких методів належать: метод опорних векторів [6], наївний класифікатор Байєса [7, 8], методи, що базуються на аналізі лексем [9], дерева прийняття рішень [9], метод максимальної ентропії та нейронні мережі [10]. Ефективність більшості з цих методів значною мірою залежить від якості словників, які використовуються для класифікації тексту. Тому розробка та постійне вдосконалення словників є важливою складовою частиною досліджень в цій галузі.

Один з найважливіших недоліків полягає в тому, що словники можуть бути створені вручну, що, хоч і просто, вимагає значних затрат часу, як, наприклад, у випадку з General Inquire [7].

Окрім статичних словників, існують напівавтоматичні, що ґрунтуються на динамічно оновлюваних даних, такі як WordNet-Affect та SenticNet [8]. Однак останнім часом дослідники віддають перевагу методам, що базуються на нейронних мережах [11]. Це пояснюється тим, що нейронні мережі, як математична модель обробки природної мови (NLP) та її програмна реалізація, здатні відтворювати принципи роботи біологічних нейронних мереж живих організмів.

Застосування цих методів дозволяє автоматично аналізувати текст, написаний природною мовою, та встановлювати зв'язки між його компонентами для визначення його категорії. Проте, обробка природної мови (NLP) й далі залишається актуальним напрямком досліджень. Це зумовлено складністю природної мови, яка являє собою відкриту багаторівневу систему знаків, що виникає та постійно розвивається в процесі людської діяльності [11].

Згідно зі статистичними даними порталу "The Statistics Portal" (рис. 1) [3], кількість активних користувачів соціальних мереж є вельми значною. Аналіз

гістограми свідчить, що найпопулярнішою з них є Facebook, яка налічує 2,49 мільярда активних користувачів Інтернету за місяць. Це робить цю соціальну платформу потенційно потужним інструментом для поширення антиукраїнської пропаганди.

Соціальні мережі широко використовуються для поширення інформації різного характеру, включаючи політичну пропаганду, пропаганду самогубств серед дітей, а також "позитивну" пропаганду здорового способу життя (див. рис. 2.1). Останній тип пропаганди, на відміну від інших, не має маніпулятивного характеру. Незважаючи на наявність різних форм інформаційного впливу, дослідження переважно зосереджуються на негативних аспектах, пов'язаних з пропагандою.

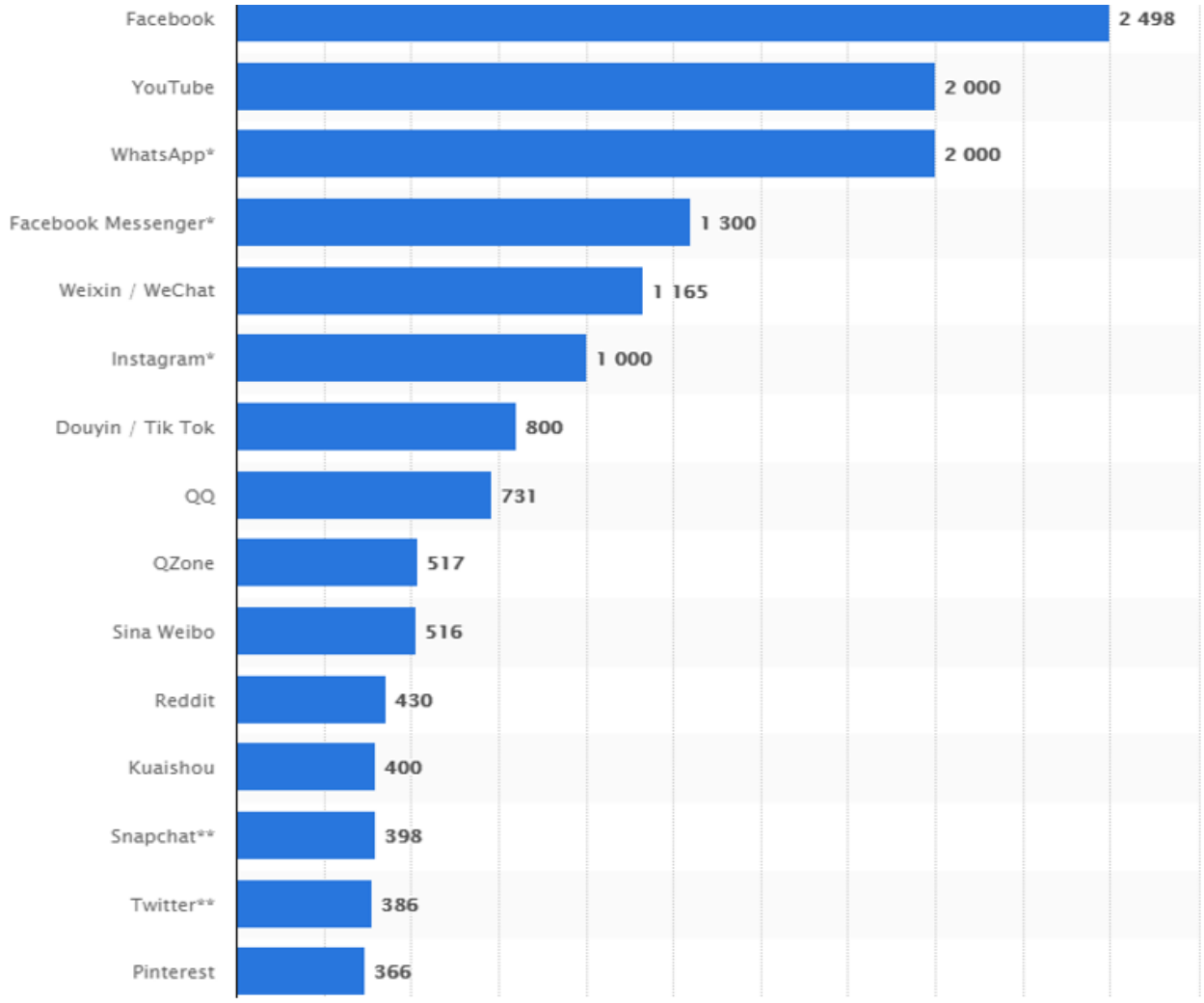

Рисунок 2.1 – Графік, що відображає кількість активних користувачів соціальних мереж (у мільйонах)

Численні віртуальні спільноти використовуються з метою маніпулювання свідомістю користувачів для досягнення власних інтересів. Ці спільноти слугують ключовим майданчиком для формування та поширення інформаційно-психологічного впливу (ІПВ) в соціальних мережах. Віртуальні спільноти представляють собою мережі міжособистісних зв'язків, які забезпечують соціальну взаємодію, підтримку, обмін інформацією, відчуття належності до групи та задоволення різноманітних соціальних потреб [1]. Основним інструментом ІПВ є маніпуляції, які ґрунтуються на ознаках маніпулятивності та прихованих намірах. Ці маніпуляції дозволяють змінювати світогляд людини та впливати на неї, нав'язуючи несправжні факти з метою просування власних інтересів та формування необхідної суспільної думки. До найпоширеніших маніпулятивних ознак в соціальних мережах належать [1], [2], [4]:

– посилання на інші ненадійні джерела інформації;
– повторення ключових слів;
– поширення несправжніх новин, які викликають ажіотаж;
– використання фактів, вирваних з контексту.

На сьогоднішній день існує багато методів автоматичного аналізу тексту для подальшого його категоризування. При використанні таких методів обробки інформації необхідно враховувати специфіку самого тексту. Методи виявлення інтелектуальних власностей можна умовно поділити на дві великі групи: методи, що ґрунтуються на використанні словникового складу, і методи, засновані на машинному навчанні з учителем.

Один із методів аналізу тексту базується на виявленні емоційного забарвлення словникового складу (лексичної тональності). Визначення тональності тексту ґрунтується на оцінці конкретних слів та їх комбінацій за допомогою попередньо складених словників та правил. Цей підхід дещо чутливий до орфографічних помилок чи скорочень, які часто зустрічаються у текстах соціальних мереж.

При лексемно-орієнтованому підході настрій тексту визначається в залежності від полярності слів або фраз у ньому. Цей процес включає такі кроки

[9]: після попередньої обробки тексту перевіряється полярність кожного слова за словниковими значеннями. Якщо слово не знайдено, воно вважається неполярним.

2.4 Загальні приклади ІПСО поширених росією про Україну

Країна-терорист, де чорне називають білим, загарбницька війна представлена як звільнення та мир, а тисячі цивільних жертв в Україні тлумачаться як денацифікація, "звільнення" та підтримка "своїх". Така інформаційна кампанія рф нагадує цитату з роману Джорджа Орвелла "1984" і відноситься не тільки до України, але й до багатьох інших країн світу.

В історичних записах Росія відома своєю активною участю в війнах як на полі бою, так і в інформаційному просторі через мережу Інтернет, телебачення та радіо, розповсюдження чуток. Прикладом цього є війна в Чечні та конфлікт з Сакартвело (російська Федерація надалі називає країну Грузією і використовує пропаганду та дезінформацію для виправдання своїх військових дій), що свідчить про те, як інформація стала зброєю Росії і одним із ключових аспектів у веденні війни. Аргумент Росії, що вона захищає росіян та російської мови за кордоном, є нещодавнім, але нічим не новим.

У 2014 році Росія висунула обґрунтування свого вторгнення на Донбас, стверджуючи, що це було необхідно для захисту етнічних росіян на сході України. Така ж ситуація відбулася і в 2008 році, коли російський уряд звинуватив Тбілісі в етнічних чистках і незаконному видачі російських паспортів для "захисту" росіян у Південній Осетії, так само, як це відбулося на Донбасі [76]. Аналіз наявних даних свідчить про те, що інформаційно-психологічні операції (ІПСО) проти України розпочалися значно раніше повномасштабного вторгнення 2022 року, ймовірно, ще до початку збройної агресії 2014 року. При цьому базові наративи, що становлять основу ІПСО, залишаються практично незмінними, лише адаптуючись, трансформуючись та доповнюючись з часом, формуючи системний вплив.

Досліджується комплексний спектр маніпулятивних практик, що застосовуються в рамках інформаційної війни. До них належать:

– Виправдання збройної агресії, зокрема на тимчасово окупованих територіях, шляхом створення фейкових наративів та дезінформаційних кампаній.

– Перекладання відповідальності за злочини та руйнування на Україну та її партнерів, намагаючись зневірити міжнародну спільноту та приховати власні злочинні дії.

– Протидія консолідації українського суспільства та його євроатлантичному курсу шляхом розпалювання ворожнечі, розколу та дестабілізації.

– Створення ілюзії власної могутності та непереможності агресора, щоб залякати супротивника та деморалізувати українське населення.

– Формування ізольованої соціально-культурної та інформаційної реальності на окупованих територіях, відгороджуючи їх від українського інформаційного простору та нав'язуючи власну пропаганду.

– Поширення дипфейків та дезінформації з метою підірвати довіру населення до законної влади та авторитетних лідерів думок.

Важливо зазначити, що на початковому етапі війни (з лютого до середини літа) українське населення активно поширювало неперевірену інформацію, що свідчить про високий рівень емоційної напруги та схильність до маніпуляцій з боку пропаганди.

З часом населення України набуло навичок критичного аналізу інформації та усвідомило сутність інформаційно-психологічних операцій (ІПСО) [19]. Це підтверджується динамікою зростання інтересу до терміну "Інформаційно-психологічні операції" в Україні протягом 2020-2023 років, що наочно продемонстровано на рис. 2.2 [12].

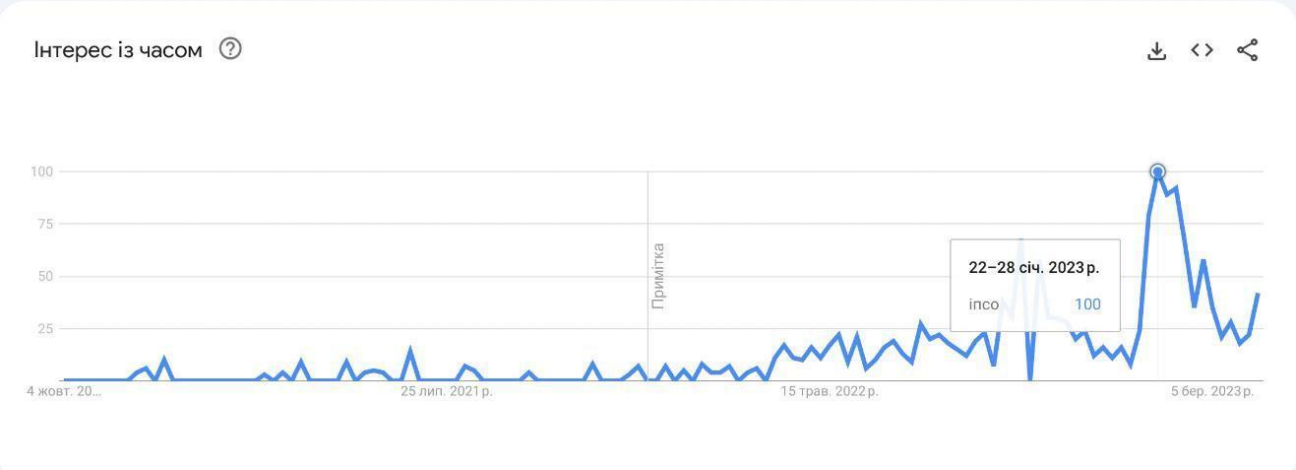

Рисунок 2.2 – Динаміка запитів за останні три роки в українському сегменті Google щодо терміну "ІПСО"

Термін "ІПСО" став досить поширеним і часто вживаним у інформаційному просторі України. І це не випадково. Політолог і експерт з психологічної війни Пол Лайнбарджер зауважував: "Війна завжди починається задовго до початку військових дій та триває певний час після їх завершення.

Традиційна війна полягає у протистоянні армій, однак психологічна війна націлена проти мільйонів цивільних осіб, які не можуть активно протистояти [12]. Це, в свою чергу, відображає тактику інформаційно-психологічних операцій. Психологічний тиск, заснований на впливі на свідомість людини через чутки, фейки, маніпуляції та дезінформацію, які є складовими частинами ІПСО, застосовується комплексно. Він працює під прикриттям "визволення", особливо там, де вже посіяна паніка, і де люди знаходяться в безпритульному становищі, позбавлені базових потреб, які визначені у Піраміді Маслоу: безпеки, харчування, води, моралі, житла і навіть освітлення, майбутнього.

Наративи, чи то реальні, чи вигадані, є історіями, подіями, фактами або враженнями, які розповсюджує росія з метою успішного формування відповідного ставлення до певного об’єкта. Вони представляють собою системне та тривале явище, яке створюється шляхом розповсюдження різноманітних маніпуляцій, вибіркової інформації та виокремлення даних, що підтримують бажане ставлення.

Саме завдяки цим наративам ефективність проведення інформаційно-психологічних операцій значно зросла.

Перед вторгненням рф активно розповсюджувала інформацію з метою деморалізації українців, спровокувати розкол між Україною та її союзниками, зміцнити суспільну підтримку рф та продемонструвати її могутність і непереможність [17].

Заяви включали в себе наступне: збільшення військових сил перед вторгненням було лише частиною навчальних заходів; ретельно пророблені повідомлення, спрямовані на історичний ревізіонізм та намагання позбавити Україну статусу суверенної держави (заявили, що Україна не має історичних підстав для незалежності та була створена росією); твердження про те, що неонацисти проникли до українського уряду; інформація про загрози, які чекають російське населення в Україні, а також про те, що уряд України вчиняє геноцид на тих територіях Донецької та Луганської областей, які незаконно контролюються окупантами з 2014 року; розповсюдження інформації, яка мінімізує розмір вторгнення рф, перекладаючи увагу на можливі воєнні злочини інших країн, включаючи згадки про історичні події, пов'язані з США та країнами Європи [12].

Отже, кілька місяців до розпочаття повномасштабної збройної агресії рф проти України, фейкові наративи про Україну та її союзників, багато з яких були поширені дезінформаційним апаратом кремля, уже активно циркулювали в Інтернеті. Вони включали неправдиві твердження про український геноцид та утиски, спрямовані проти російськомовних українців, а також ствердження, що політичне керівництво України контролюється нацистською ідеологією. Ці маніпуляції та багато інших були використані для виправдання повномасштабного вторгнення рф в Україну.

росія використовує стратегію випаленої землі та ізоляції, перш за все, для російськомовних регіонів України. За словами російських офіційних джерел, рф прийшла захищати ці регіони від нацистів, які, як стверджує російська пропаганда, дискримінують населення за мовою. Ця конструкція наративів працює дуже ефективно, оскільки створює ілюзію про путіна як про сильного лідера, який будує

могутню державу й постійно захищає свій народ від ворогів. російська пропаганда йде по шляху Третього Рейху, який, за допомогою дезінформації, позбавляв населення критичного мислення. Мета наративів російської пропаганди полягає в тому, щоб привести до емоційного мислення українців та зробити їх більш вразливими до пропаганди, спонукати їх сумніватися в чесності власного уряду щодо терористичних актів, масових ракетних обстрілів та загибелей.

Дослідження, що проводилися українськими та американськими науковцями, а також нагляд за урядовими засобами масової інформації на росії, вказують на те, що актуальні дискурси під час конфлікту фокусуються на кількох ключових темах. Серед них поширені теорії змови та конспірологічні версії, особливо в контексті біологічної зброї, а також ідеї про проведення так званих операцій під фальшивим прапором. В цих операціях рф стверджує, що дії, які приписуються їй, насправді є результатом діяльності України, яка намагається відіграти свою роль, приховуючи справжнє джерело відповідальності [21].

Серед найвідоміших неправдивих наративів, які активно розповсюджувала росія перед початком і під час повномасштабної війни, були:

– Україна - штучна держава;

– Сучасна Україна була створена комуністичною росією;

– росія не атакує цивільну інфраструктуру України;

– Україна - маріонетка Заходу;

– В українській політиці та суспільстві процвітає нацизм. Фашизм підтримується українською владою;

– В Україні триває громадянська війна;

– Крим завжди був російською територією і законно ввійшов до складу рф;

– Російськомовне населення Донбасу систематично зазнає геноциду з боку України;

– Україна готує наступальну операцію на Донбасі і загрожує рф вторгненням;

– Українці розробляють біологічну зброю та брудну бомбу, спрямовану проти етнічних росіян;

– Політичні лідери України давно знаходяться за кордоном;

– Україна сфальсифікувала розправу над мирним населенням у Бучі на початку війни;

– росія проявила жест доброї волі;

– Українці торгують західною та американською зброєю;

– Україна підлаштувала напад на лікарню в Маріуполі 9 березня 2022 року [22].

Ці наративи утворюють цілісну семантичну матрицю пропаганди, в якій основні ідеї взаємопов’язані та взаємопідсилювальні. Наприклад, концепція України як штучної держави, що не має реальних інституцій і не може забезпечити основні права та свободи своїм громадянам, призначена для дискредитації країни. Ця ідея створює враження, що російський вплив є необхідним і бажаним, щоб врегулювати "хаос" на території України, на що, як стверджується, місцеве населення і уряд не здатні. Крім того, російська Федерація давно намагається впливати на історичну пам'ять населення, використовуючи як приклад період культа Сталіна, коли відбувався перепис історії. Незважаючи на це, багатовекторність сприйняття історії значно гальмує процес формування національної пам'яті, дезорієнтуючи її, а ворог в цей час намагається маніпулювати історією, щоб змінити свідомість людей [24]. Особливо легко розповсюджувати власні наративи на тимчасово окупованих територіях, де доступ до альтернативних джерел інформації відсутній.

Ці наративи про Україну кремль систематично просував протягом багатьох років, використовуючи всі доступні інструменти. Вони висловлювалися вищими російськими чиновниками, транслювалися на російських телеканалах (як державних, так і приватних, федеральних і регіональних), і розповсюджувалися різними мовами для міжнародної аудиторії.

За успіх російських інформаційно-психологічних операцій проти України відповідають декілька факторів. По-перше, Росія володіє багатим досвідом у таких діях, що вже проявлявся в Сакартвело (Грузії), Чечні та Молдові, і цей досвід застосовується в її взаємодії з Україною. По-друге, у Росії є потужні медіа-ресурси, які служать платформами для поширення дезінформації та пропаганди протягом

багатьох років. Вони використовуються для створення фейкових новин та історій з метою маніпулювання психологією громадян. По-третє, внутрішня політична та економічна нестабільність України, присутність проросійських політиків та їх інформаційних кампаній створюють сприятливу обстановку для здійснення російських інформаційно-психологічних впливів [15; 35].

Незважаючи на активне просування власних наративів та проведення інформаційно-психологічних операцій, російська федерація допустила низку помилок, що призвело до зниження їхньої ефективності. Ігнорування принципів демократії, прав людини та свободи слова спричинило відчуття обмеженості інформаційного простору у частині цільової аудиторії. Слабка доказова база також негативно вплинула на сприйняття пропаганди. Інформація про "краще життя" на тимчасово окупованих територіях Донецької та Луганської областей у складі псевдореспублік не відповідала реальній економічній, політичній та культурній ситуації. Не варто було недооцінювати доступ українців та громадян інших демократичних країн до альтернативних джерел інформації через Інтернет та супутникову систему, що дає змогу їм отримувати різні точки зору та оцінки подій [37, с. 139].

Таким чином, майже щодня, особливо під час повномасштабного вторгнення, росія проводила інформаційно-психологічні операції або поширювала свої наративи про Україну. Особливо активною була дезінформація та чутки, поширювані росією напередодні 9 травня, Великодня, а також під час інформування в Україні про мобілізацію та контрнаступ тощо. Така риторика пов'язана, передусім, з широкою інформаційно-політичною стратегією, що ґрунтується на історичних та культурних цінностях, з метою створення дихотомії "свій чи ворог", де авторитарна росія виступає як "друг", а демократичний Захід - як "ворог".

2.5 Механізми впровадження інформаційно-психологічних впливів росії проти України

Механізми реалізації інформаційно-психологічних операцій росією проти України – це довготривалий процес, який через сформовані меседж-бокси та стратегію інформаційного впливу, комплекс дій, негативно впливає на інтереси держави, громадян і суспільства за межами України, а також затронув усі сфери національної безпеки країни:

– політичну (зовнішньополітичну та внутрішньополітичну);

– інформаційну;

– економічну;

– військову;

– екологічну;

– соціальну;

– науково-технологічну та інші.

Під час повномасштабної війни росія здійснює інформаційно-психологічні операції безпосередньо або агресивно, використовуючи гасла, спрямовані на знищення української культури та просування етнічної асиміляції.

Основними інструментами для здійснення інформаційно-психологічних операцій росією є:

– використання соціальних мереж (YouTube, TikTok);

– вплив на іноземні ЗМІ, включаючи власні канали, що функціонують у різних країнах (RT, Sputnik);

– залучення тролів, блогерів і ботів, включаючи чат-ботів;

– розповсюдження листівок та безкоштовних агітаційних газет;

– проведення face-to-face агітації за участю місцевих колаборантів та активістів "єдиної росії".

Під час видачі грошових виплат, продуктових наборів та російських паспортів вони здійснюють вплив на людей. Інструкції щодо взаємодії з населенням також отримують військовослужбовці держави-окупанта. Крім того,

контроль уряду над внутрішніми мас-медіа (включаючи телебачення, друковані видання та онлайн-ЗМІ), а також інформацією, що потрапляє до громадськості, дозволяє йому заміщати незалежні та фактично обґрунтовані звіти своїми офіційними наративами в основних медіаканалах.

В умовах інформаційної закритості на росії складно об'єктивно оцінити рівень підтримки війни в Україні та рівень довіри населення до офіційних джерел інформації. Це зумовлено відсутністю доступу до надійних даних соціологічних досліджень та незалежних звітів. З одного боку, відомо, що у квітні 2022 року близько 15 400 росіян були заарештовані за участь у антивоєнних протестах, а з іншого боку, матеріали опозиційних та незалежних ЗМІ набирають мільйони переглядів в Інтернеті. Однак, через відсутність вільного та безпечного простору для публічного вираження думок, справжній рівень підтримки війни в Україні серед населення росії залишається невідомим.

На росії спостерігається жорсткий контроль над інформаційним простором, що виражається у відсутності незалежних суспільних мовників та фактичній забороні незалежних ЗМІ. Ці обмеження слугують інструментом маніпулювання наративами про війну в Україні, адже змушують іноземні ЗМІ, що базуються на території рф, самоцензурувати свої репортажі, уникаючи заборонених тем та слів. роскомнагляд, державний орган, що здійснює контроль у сфері інформації, суттєво посилив тиск на ЗМІ, які висвітлюють події, що суперечать офіційній позиції. Так, через два дні після початку повномасштабного вторгнення у 2022 році роскомнагляд оголосив про те, що ЗМІ можуть публікувати інформацію про війну лише з офіційних державних джерел. Окрім цього, було розпочато негайне розслідування щодо 10 ЗМІ за "поширення невірогідної суспільно значущої інформації". Згодом було обмежено доступ до Google News та до платформ соціальних медіа на території рф. Важливо зазначити, що контроль над іноземними компаніями, такими як Google, є значно складнішим завданням, порівняно з вітчизняними аналогами, наприклад, "ВКонтакте" та "Однокласники", які користуються широкою популярністю серед населення і значно більше піддаються впливу з боку держави.

Перефразування тексту в науковому стилі: Через місяць після початку повномасштабної агресії проти України Генеральна прокуратура російської федерації визнала компанію Meta екстремістською організацією, що призвело до блокування доступу до Facebook та Instagram на території рф. Цей крок став наслідком попередніх обмежень, накладених урядом на діяльність Twitter на початку березня 2022 року [55]. Перед забороною попит на віртуальні приватні мережі (VPN), які шифрують дані та приховують місцезнаходження користувача, зріс більш ніж в 20 разів, порівняно зі середньодобовим показником за попередній місяць. Це свідчить про те, що попит на ці платформи на росії залишається високим [55].

Ці рішення щодо обмежень та заборон дозволили росії блокувати доступ до альтернативних джерел інформації для її власних громадян. Це означає, що російське населення не може вільно отримувати інформацію з альтернативних джерел, що створює потенційну можливість впливу на інформаційне середовище України та країн Європи. Оскільки населення не має можливості ефективно протистояти діям власної держави, це створює безперешкодні умови для впливу рф на інформаційне середовище цих країн.

Більше турбот викличуть внутрішні проблеми країни, ніж зовнішньополітичний курс, оскільки зростання цін, мобілізація та відхід великих компаній відбувається відчутно для пересічного громадянина. Страх за власне життя і долю родини переважає над усім іншим. Крім того, вину за сучасну ситуацію на росії малоймовірно буде приписати лише їй самій. Політика "вважати все іноземне ворогом" має свої корені ще від періоду культу особистості Сталіна і подібна до дій Гітлера та навіть Муаммара Кадаффі.

Заборонивши доступ до зарубіжних соціальних мереж, росія активно використовує Telegram – сервіс обміну повідомленнями, створений засновником «ВКонтакте». Цей месенджер став платформою для обміну інформацією між користувачами, а також надає можливість ЗМІ та журналістам працювати без цензури. Із функціями як зашифрованого, так і незашифрованого чату, його

популярність зросла з початком агресії рф проти України. Telegram став джерелом як незалежних новин, так і пропаганди, дезінформації, поширення дипфейків тощо.

При аналізі інформаційно-психологічних операцій важливо враховувати, що використовані наративи та загальні цілі росії залишаються в основному послідовними. Механізми реалізації інформаційно-психологічних операцій, які поширюють неправдивий та оманливий контент, і здатність рф контролювати своє інформаційне середовище, продовжують розвиватися. Ці фактори мають великий вплив на формування системи протидії інформаційно-психологічним операціям росії проти України.

Всі ці чинники взаємодіють між собою, як позитивно, так і негативно, і впливають на систему в цілому. Для більш глибокого розуміння стратегії протидії інформаційно-психологічним операціям росії проти України та для прийняття рішень корисно скласти когнітивну карту (див. рис. 2.3), в якій будуть відображені різні групи впливових чинників (зовнішні, внутрішні, найбільш вагомі), цільовий фактор та умови процесу; каузальний ланцюг подій; визначення каузальної послідовності для досягнення цільового фактору, яке можна побачити на рисунках 2.4 та 2.5.

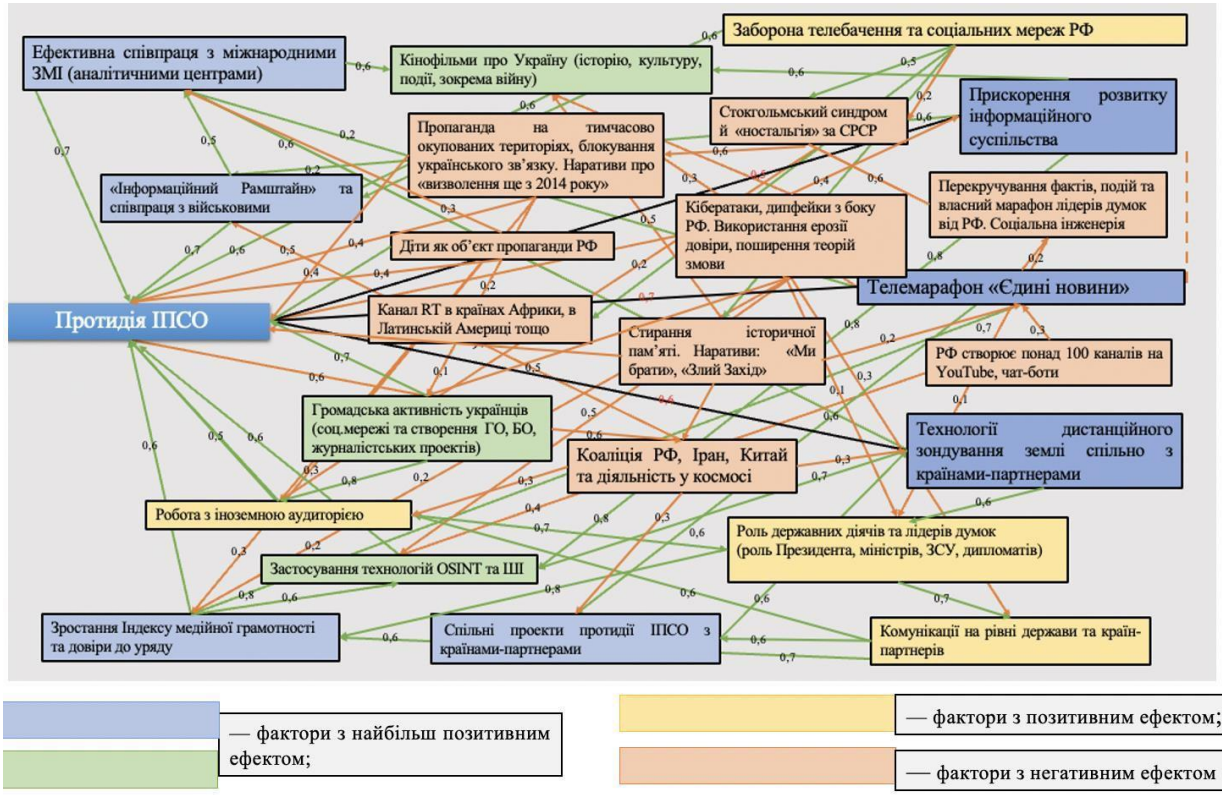

Рисунок 2.3 – Когнітивна карта чинників, що впливають на систему протидії інформаційно-психологічних операцій рф

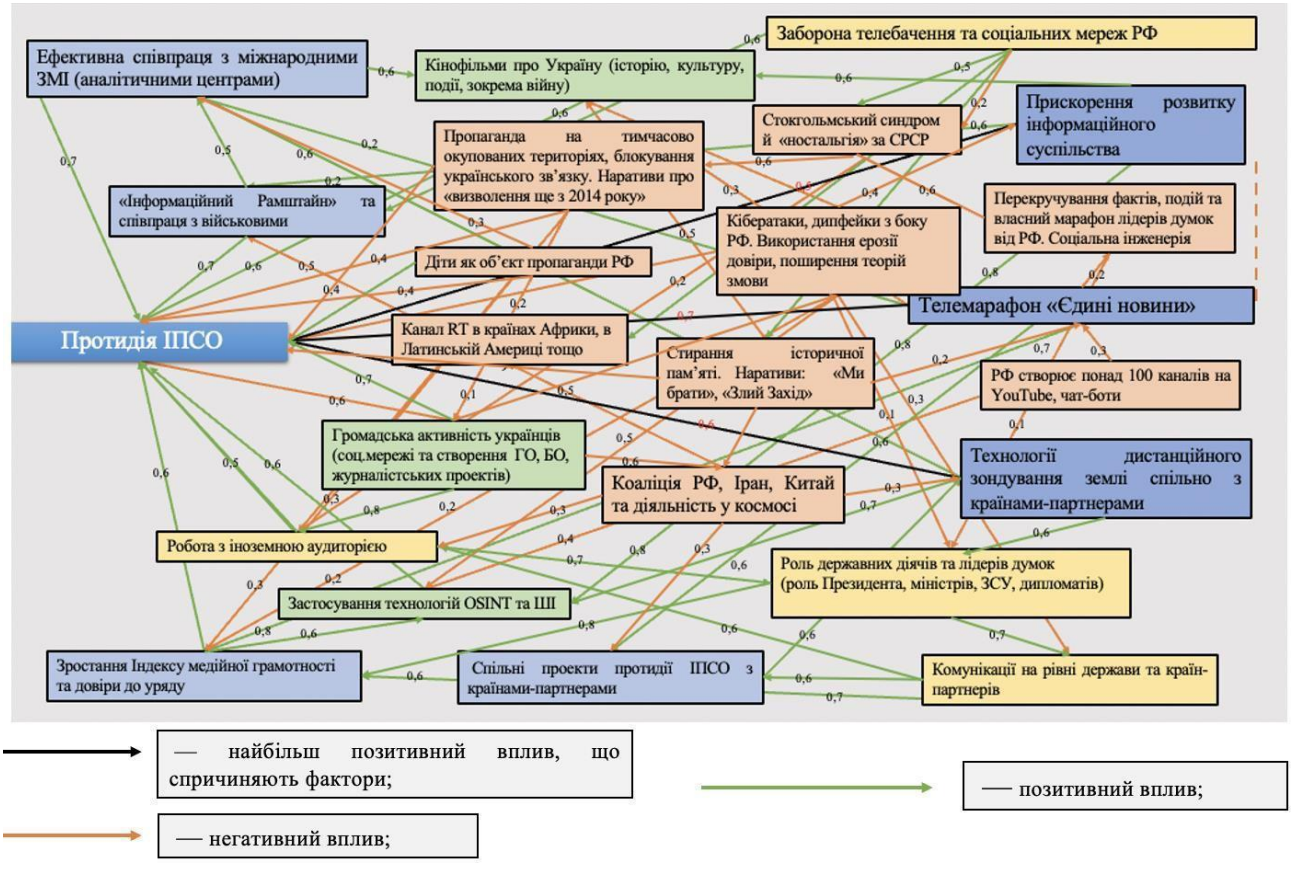

Рисунок 2.4 – Когнітивна карта чинників, що впливають на систему протидії інформаційно-психологічних операцій рф

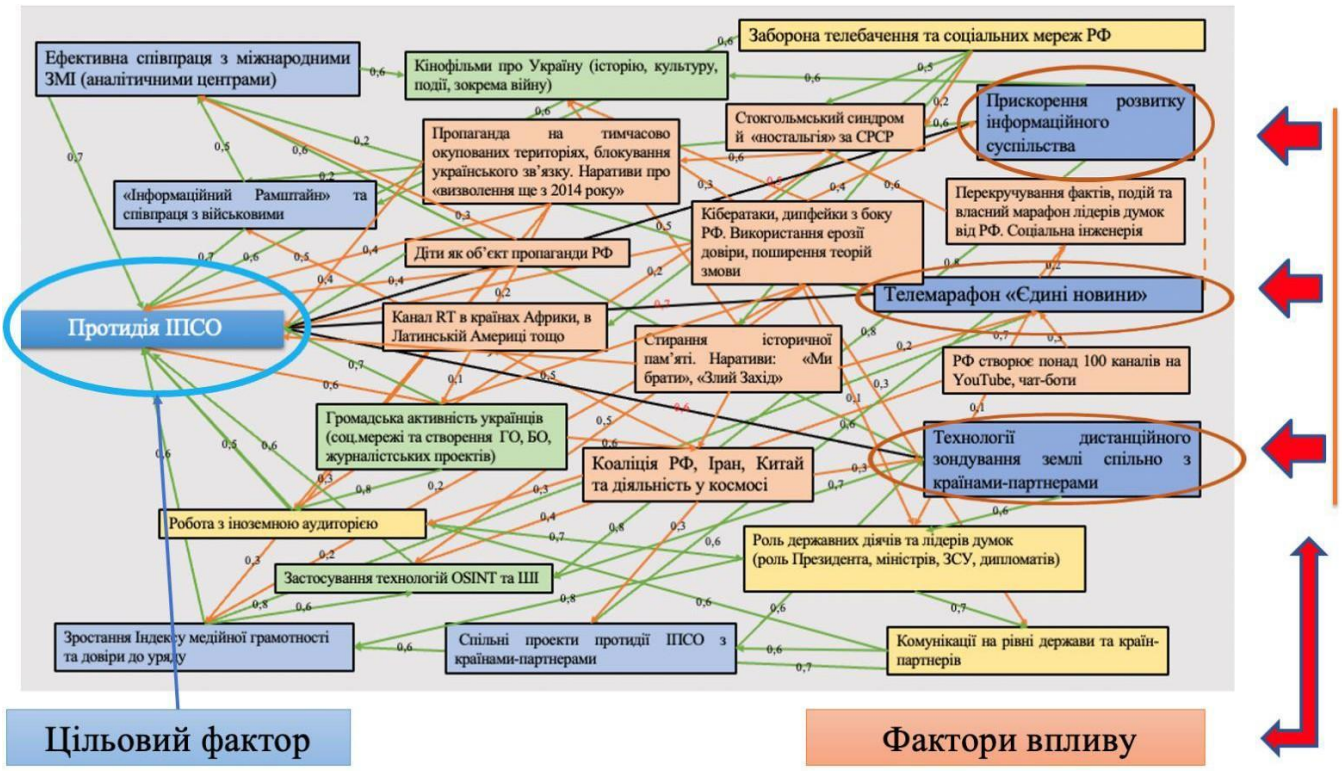

Рисунок 2.5 – Когнітивна карта чинників, що впливають на систему протидії інформаційно-психологічних операцій рф та цільового фактору

До негативних чинників, що впливають на позиції України, належить застосування росією низки методів інформаційної агресії, таких як ерозія довіри, поширення теорій змови, кібератаки та створення дипфейків. Згідно з даними команди безпеки Microsoft, близько 32% деструктивних атак з боку рф були спрямовані безпосередньо на українські урядові організації на національному, регіональному та міському рівнях, а понад 40% – на організації в секторах критичної інфраструктури [22].

Більше того, інформаційно-психологічні операції здійснювані росією стають все більш успішними. Пропаганда зосереджена на виклику стокгольмського синдрому у дорослого населення та молоді – сприяння позитивним емоціям у бік агресора, роз'єднання думок та вірувань у силу росії, а також нав'язливі спогади («ностальгія» за СРСР). Кожен з цих факторів взаємодіє з іншим, утворюючи перешкоди для України у впровадженні успішної та ефективної системи протидії інформаційно-психологічним операціям, що вимагає швидких дій від уряду. Згідно

з результатами когнітивної карти, інформаційно-психологічні операції росії досягають успіху в Україні з декількох причин: соціальна інженерія та історичні зв'язки, впливове інформаційне середовище та медіапростір, а також вплив на міжнародні відносини.

Наприклад, протягом останнього року росія виробила значну кількість відеороликів та кінофільмів, які героїзують терористичні дії в Україні, та поширює їх на тимчасово окупованих територіях, а також серед країн Латинської Америки, Індії, Китаю, африканських країн та навіть в Європі. За даними компанії Newsguard, яка займається оцінюванням довіри до новинних веб-сайтів, з моменту початку повномасштабного вторгнення в Україну рф випустила понад 50 дезінформаційних та пропагандистських фільмів через канали RT, RTD.RT.com, а також платформу YouTube – в середньому один на тиждень [25].

Отже, важливо негайно розпочати формування протидії інформаційній діяльності кремля. Після успішної верифікації результатів аналітичної роботи та побудови когнітивної карти ми можемо зробити висновок щодо факторів, які мають позитивний вплив:

– заборона трансляції російських телеканалів та використання російських соціальних мереж;

– виробництво власних кінострічок, оскільки культура важлива на сучасному етапі; активна робота з іноземною аудиторією;

– використання передових технологій, включаючи нейромережі та штучний інтелект;

– збільшення громадської активності;

– ефективне співробітництво з міжнародними ЗМІ;

– підвищення рівня медійної грамотності населення;

– проведення телемарафону "Єдині новини";

– прискорення розвитку інформаційного суспільства та використання технологій дистанційного зондування Землі у співпраці з партнерськими країнами.

Україна активно вживає різноманітні заходи, проте важливо врахувати негативний вплив факторів з боку росії на систему протидії інформаційно-

психологічним операціям (ІПСО). Особливу увагу слід звернути на заборону російських медіа-каналів за кордоном та зменшення інформаційного впливу росії на тимчасово окупованих територіях, оскільки ці дії негативно впливають на роботу з міжнародною аудиторією та сприяють позитивному іміджу рф.

Висновки до другого розділу

У даному розділі було проведено аналіз методів виявлення інформаційно-психологічного впливу, розглянуто стратегії боротьби з інформаційним впливом супротивника в контексті інформаційної війни. Висвітлено принципи та методи протидії сучасним інформаційно-психологічним впливам, а також наведено загальні приклади інформаційно-психологічних операцій, що поширюються Росією щодо України. Особлива увага приділена механізмам впровадження інформаційно-психологічних впливів росії проти України. Отримані дані є важливим внеском у розуміння та розроблення ефективних стратегій протидії інформаційно-психологічному впливу в кіберпросторі.

РОЗДІЛ 3.
ПЕРСПЕКТИВИ ТА ВДОСКОНАЛЕННЯ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ В КІБЕРПРОСТОРІ

3.1 Інформаційна стратегія України щодо протистояння психологічному впливу в кіберпросторі під час воєнної агресії росії проти України

Система стримування інформаційно-психологічних атак росії включає ряд дій та інструментів, спрямованих на ідентифікацію, перевірку, реагування та нейтралізацію шкідливого впливу на цільові групи, включно з інформаційним простором України та її союзників. Ця система організована за трьома основними рівнями, деталі яких представлені на рисунку 3.1 [2, с. 56-62].

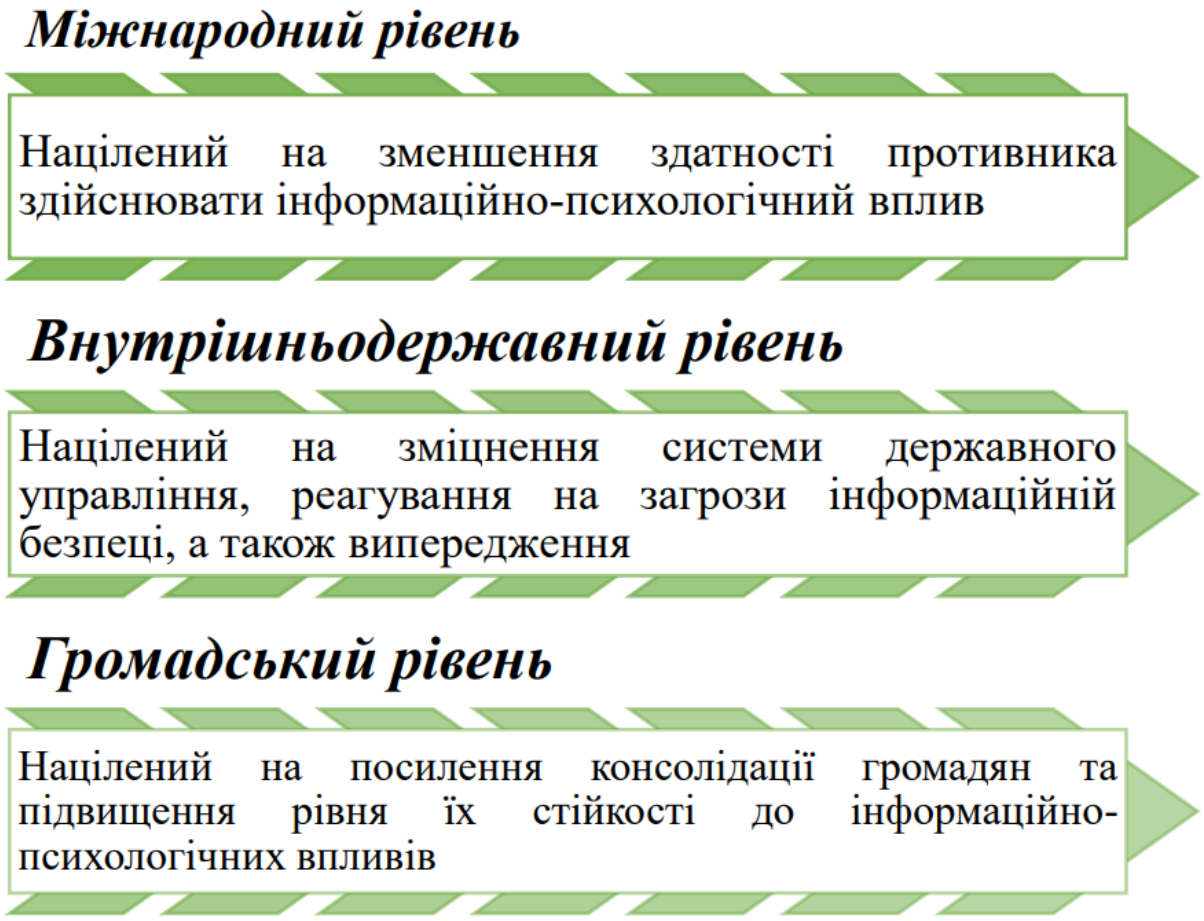

Рисунок 3.1 – Рівні реагування на російський інформаційно-психологічний вплив

На державному рівні формулюється комплексна стратегія протидії інформаційно-психологічним операціям (ІППО), що передбачає комплекс заходів з боку державних органів. Державна інформаційна політика України має на меті захист демократичних цінностей та створення безпечного інформаційного середовища для громадян. В умовах повномасштабного вторгнення російської федерації спостерігається активна реакція українського суспільства на заклики влади до протидії дезінформації та пропаганді. На міжнародному рівні вживаються заходи, спрямовані на мінімізацію здатності противника здійснювати інформаційно-психологічний вплив.

Крім того, активна підтримка та об'єднання перед інформаційними загрозами підтверджують нещодавні соціологічні дані про зростання рівня довіри українців до Президента. Згідно з даними Київського міжнародного інституту соціології за січень 2023 року, рівень довіри до Президента України зросла з 27% у 2021 році до 84% у 2022 [7].

Соціологічне дослідження, проведене Центром Разумкова у лютому-березні 2023 року серед понад 2 тисяч опитаних, підтверджує широку підтримку Президента України, яка складає 83% серед українців [20]. Активна участь Президента, Володимира Зеленського, у брифінгах, соціальних мережах (твіттер-дипломатія) та його вміння чітко, проте швидко і детально комунікувати з аудиторією, включаючи міжнародну спільноту, яка є метою втручання Росії, має важливе значення у протидії інформаційно-психологічним операціям. Поширення правдивої інформації серед внутрішньої та міжнародної аудиторії є одним із ключових інструментів боротьби з інформаційно-психологічними операціями. Крім того, важливим є спростування фейків та дезінформації, що сприяє підвищенню довіри до уряду [10, с. 21].

Крім того, важливо не лише спростовувати наративи росії, але й надавати відповідну інформацію. Наприклад, малоймовірно, що громадяни Німеччини чи України будуть перевіряти новини на кількох джерелах і відстежувати джерела дезінформації. Президент Володимир Зеленський активно шукає військову та дипломатичну підтримку від міжнародної аудиторії та урядів різних країн. Він

інформує їх про ситуацію в Україні через щоденні оновлення у соціальних мережах, звертається до глав держав у онлайн-форматі та під час особистих зустрічей [18].

З метою протидії дезінформаційним кампаніям Росії, Україна вживає комплексних заходів, окрім розширення доступу до об'єктивних новинних джерел. Одним із таких кроків стало обмеження доступу до російських ЗМІ, що мають значний вплив на аудиторію. РНБО України запровадила санкції проти трьох телеканалів, пов'язаних з проросійським політиком Віктором Медведчуком: NewsOne, 112 Україна та ZIK [17].

Вжиті на державному рівні України заходи, окреслені в когнітивній карті, мають низку позитивних наслідків: подолання стокгольмського синдрому та "ностальгії" за СРСР, зменшення кібератак, фейків та дезінформації, стимулювання відновлення історичної пам'яті та розвитку української культури, зменшення інформаційного впливу росії та роблять більш актуальною проблему існування російських пропагандистських каналів в країнах міжнародної спільноти. Ці кроки сприяють не лише захисту власного інформаційного простору України, але й роблять вагомий внесок у боротьбу з глобальною дезінформацією, що становить серйозну загрозу для демократії та міжнародної безпеки.

Для протидії дезінформаційним кампаніям росії Україна вживає рішучих заходів. Зокрема, було створено два спеціалізованих центри: Центр протидії дезінформації при РНБО (ЦПД) та Центр стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України (ЦСКІБ). Ці центри виконують важливу функцію з моніторингу та аналізу інформаційних загроз національній безпеці України. Наприклад, з початку повномасштабного вторгнення у лютому 2022 року ЦПД активно веде роботу з fact-checking та розвінчання неправдивої інформації, що поширюється в Telegram та Twitter. Ця діяльність дає українському уряду офіційний експертний інструмент для протидії ворожим інформаційним кампаніям [13]. Окрім того, у липні 2022 року за ініціативою ЦСКІБ, МКІП та за підтримки посольства Швеції розпочала роботу "Школа протидії дезінформації". Ця програма спрямована на підвищення

рівня інформаційної стійкості та медіаграмотності державних службовців та фахівців у сфері комунікацій [8].

Ці кроки допоможуть в управлінні інформаційним простором, зокрема в поширенні інформації про «Батальйон Монако» (українських політиків та державних службовців, які виїхали за кордон під час воєнного стану). Свобода слова та вільний доступ до інформації є ключовими для демократії. Проте саме такі новини швидко використовуються російськими ЗМІ для проведення інформаційно-психологічних операцій, що сприяють розколу всередині України, підривають довіру до уряду та національної безпеки.

Ця стратегія росії створює хаос серед українського населення через ракетні удари, використовуючи психологічні маніпуляції та наративи, такі як "зрада серед своїх" і "зрадники на Банковій". Додатково, вони генерують дезінформацію, розповсюджуючи міфи про те, що Президент та інші державні посадовці вже давно залишили країну і перебувають за кордоном. У цьому контексті дуже обговорюваною стала ідея створення "Інформаційного Рамштайну" як нового формату міжнародного співробітництва для протидії російській дезінформації та пропаганді. За словами Міністра культури та інформаційної політики Олександра Ткаченка, "Інформаційний Рамштайн" може стати ефективним інструментом інформаційної безпеки України та сприяти ще більш тісній співпраці з партнерськими країнами.

Міжнародна співпраця з протидії інформаційно-психологічним операціям Росії буде реалізована через комплекс спільних заходів та проектів. Партнери визначили чіткі стратегічні цілі, до яких належать протидія ІПСО РФ, налагодження комунікації та співпраці, а також залучення спільного фінансування [38]. Очікується, що це партнерство матиме значний позитивний вплив, адже воно розширить співпрацю з міжнародними ЗМІ, сприятиме розвитку української кіноіндустрії та активізує громадян України.

За О. Ткаченком, "Інформаційний Рамштайн" має складатися з трьох основних напрямків дій:

– посилення геополітичної ролі України та її міжнародної правосуб'єктності;

– адаптація стратегій діяльності відповідно до наявних ресурсів та можливостей учасників, консолідація зусиль державного та приватного секторів;

– запровадження глобальних ініціатив для формування стійкості проти пропаганди та дезінформації [38].

Ще одним важливим кроком у боротьбі з інформаційно-психологічними операціями росії на державному рівні є створення так званої матеріальної бази, яка включає сучасні технології, що дозволяють автоматизовано перевіряти інформацію (фактчекінг), фільтрувати та блокувати її. Компанії з кібербезпеки, супутникові зображення (дистанційне зондування землі або Remote sensing), технологія Open source intelligence (OSINT) та штучний інтелект (ШІ) стають ключовими інструментами в системі протидії інформаційно-психологічним операціям росії [19, с. 595-597].

Дистанційне зондування Землі (ДЗЗ) - це невід'ємний елемент державної інформаційної політики. Ця технологія дозволяє з космосу або з повітря отримувати та аналізувати дані про земну поверхню, що робить її незамінним інструментом для бойової розвідки, моніторингу військових злочинів та інформаційного забезпечення військ [22, с. 119].

З перших днів повномасштабної агресії супутникові знімки стали незамінним інструментом для документування воєнних злочинів росії. Оприлюднені в міжнародних ЗМІ, New York Times, аналітичних центрах та інших авторитетних джерелах, ці дані допомогли спростувати російські фейки про обстріли Бучі, Ірпеня, Маріуполя та інших міст українськими військами, а також сприяли визнанню рф державою-спонсором тероризму. [19, с. 595-598; 9].

Недостатній рівень обізнаності серед загалу щодо розширених функцій пошуку Google, які включають пошук за зображеннями, файлами та документами в Інтернеті та соціальних мережах. Саме завдяки цій технології, що отримала назву OSINT, аналітики та журналісти на державному рівні сьогодні з легкістю розкривають фейкові новини та виявляють канали й джерела поширення інформаційно-психологічних операцій рф. Подібні методи використовувалися ще під час холодної війни: Центральне розвідувальне управління США та Комітет

державної безпеки СРСР збирали інформацію про військові, політичні та економічні можливості своїх опонентів, щоб отримати перевагу в протистоянні [19, с. 595-598].

Зараз технології відкритого джерела інформації (OSINT) із все більшою активністю використовуються в розвідці, доповнюючи звичайні методи з відкритим доступом і вносячи свою частку конспірологічного аналізу. Наприклад, перед початком конфлікту комерційні супутникові знімки та відеоматеріали, розміщені користувачами з росії у соціальних мережах, включаючи TikTok, дозволили журналістам та дослідникам підтвердити звинувачення Заходу щодо готовності рф до вторгнення. Згодом з'явилися докази використання росією забороненої зброї в Нікополі, Марганці, Маріуполі, Мелітополі та інших місцевостях [19, с. 595-600]. Ці факти спонукали міжнародну спільноту до об'єднання проти росії як на полі бою, так і на інформаційному фронті.

Ще одним важливим інструментом у боротьбі проти дезінформації з боку російської інформаційно-психологічної війни є штучний інтелект (ШІ), який дозволяє фільтрувати інформацію, яку не здатні розпізнати люди за її джерелом та емоційним забарвленням. Багато людей вважають, що штучний інтелект сприяє поширенню дезінформації в Інтернеті, автоматизуючи процес створення фейків. Великі ризики виникають у зв'язку зі зростанням популярності чат-ботів, які базуються на потужних мовних моделях, наприклад, ChatGPT від OpenAI, здатні створювати текст, що звучить природно, одним натисканням кнопки, фактично автоматизує створення дезінформації. На жаль, російська федерація та Китайська Народна Республіка спонсорують створення власних чат-ботів. Однак штучний інтелект також може значно зменшити шкоду, завданої дезінформацією [36].

Наприклад, в Україні вже діє чимало проектів з фактчекінгу та блокчейну, які поєднують роботу фахівців і штучний інтелект. Один із таких проектів - Texty, який використовує свої сучасні технології для швидкого аналізу тисяч каналів Telegram, де рф активно проводить Інформаційно-психологічну війну. Detector Media також використовує машинне навчання і штучний інтелект для аналізу масивів даних і прогнозування майбутніх інформаційних кампаній Кремля. Крім того, спільно з

LetsData, українською приватною компанією, що надає послуги зі штучного інтелекту і машинного навчання, Detector Media веде моніторинг дискурсу і документує хроніки дезінформації з боку кремля в режимі реального часу у понад 30 країнах [19, с. 597-600].

Отже, для забезпечення інформаційної безпеки України надзвичайно важливо розробляти власні засоби на базі штучного інтелекту, які допомагатимуть автоматизувати та прискорити процес пошуку дезінформації та її спростування. Серед перспектив удосконалення державної політики України щодо Інформаційно-психологічної війни з боку росії можна виділити наступне:

– Забезпечити оперативне та швидке поширення інформації про застосування Інформаційно-психологічних операцій російською федерацією за допомогою офіційних заяв та висловлювань впливових осіб.

– Провести комплексне вдосконалення правової бази з питань інформаційної безпеки.

– Розробити власні технології аналізу даних для виявлення ІПСО, використовуючи інструменти дистанційного зондування Землі, штучний інтелект, нейромережі та супутникову навігаційну систему для збору незалежної інформації.

– Налагодити надійну та своєчасну систему комунікації між урядом та громадянами.

– Розробити комплексну Національну стратегію використання відкритих джерел інформації (OSINT), яка визначатиме підхід уряду до збору, аналізу та поширення розвідданих.

– Інвестувати в розробку освітніх програм для підготовки наступного покоління висококваліфікованих фахівців з метою забезпечення ефективної протидії інформаційно-психологічним операціям російської федерації.

3.2 Основні принципи забезпечення ІБ України у протидії інформаційно-психологічному впливу в кіберпросторі

Безпека інформації в Україні – це важлива складова національної безпеки, відповідальна за захист національних інтересів, прав людини і суспільства. Це охоплює заходи проти інформаційної агресії, забезпечення кібербезпеки, захист конституційних прав, державної інформації та технологічний захист від негативних впливів, а також протидію інформаційно-психологічним операціям.

За словами професора психології із Бристольського університету С. Левандовського: "Українці ведуть війну XXI століття, яка, наполовину, відбувається в Інтернеті" [44]. Аналізуючи російську інформаційну війну проти України під час широкомасштабної воєнної агресії, можна зазначити, що вона розвивається і поєднує різні складові інформаційно-психологічних операцій: шантаж, дезінформацію, залякування, маніпуляцію, пропаганду, обман тощо.

Припустимо, що це протистояння показало наступне:

– уразливість сфери інформаційної (національної) безпеки України;

– недостатню ефективність захисних механізмів інформації;

– певну нестійкість та складнощі у протидії непередбачуваним інформаційним впливам з боку росії;

– недосконалість заходів на державному рівні. кремль використовує будь-яку новину щодо внутрішніх проблем України як частину інформаційно-психологічної операції, щоб поширити паніку та знизити довіру до влади.

Існують думки, що Україна відстає на інформаційному полі. Заяви про залякування та шантаж створюють уявлення про потужного та непереможного противника, порівнюючи не досягнення країни, а лише дії рф у веденні інформаційно-психологічних операцій. У 2022 році на зустрічі зі студентами факультету міжнародних відносин НАУ Ігор Соловей, керівник Центру стратегічних комунікацій та інформаційної безпеки, наголосив, що Україна не відстає у веденні інформаційної війни з росією, але має ще куди просуватися [11]. На різних рівнях українського суспільства вже запрацювали проекти, які ефективно

протистоять інформаційно-психологічним операціям росії. Головне, щоб всі компоненти працювали узгоджено, поєднуючи свої зусилля через спільні структурні взаємозв'язки.

Основні принципи інформаційної безпеки в Україні включають такі аспекти:

– політичну освіченість населення та медіаграмотність;

– законодавчу регуляцію на державному рівні;

– розвиток критичного мислення та аналізу інформації (вміння розрізняти новини та дані від маніпуляцій та пропаганди);

– захист приватності, даних, свободи слова та преси;

– використання технічних засобів та співпраця з міжнародною спільнотою.

Узагальнено, заходи захисту інформаційної безпеки в Україні можна розділити на дві категорії: законодавчі та інституційні [2, с. 57; 54].

Основний акцент робиться на законодавчих механізмах, зазначаючи, що протягом років незалежності України було прийнято значну кількість нормативно-правових актів, спрямованих на забезпечення інформаційної безпеки та протидію інформаційно-психологічним операціям. Ця законодавча база, яка постійно вдосконалюється, включає в себе такі документи, як Закони України «Про інформацію» [28], «Про доступ до публічної інформації» [25], «Про Концепцію Національної програми інформатизації» [29], «Про захист інформації в інформаційно-комунікаційних системах» [27] та інші.

Ці законодавчі акти постійно адаптувалися та змінювалися відповідно до ситуації в країні. Законодавчий компонент у системі протидії ІПСО має важливе значення, оскільки він є проявом демократії та створює правову базу для протистояння загрозам інформаційної безпеки. Ці закони стосуються вимог до ЗМІ, соціальних мереж, поширення інформації, свободи слова, захисту персональних даних, виборчих процесів та іншого.

Основним документом, який встановлює основні принципи інформаційної безпеки, є Стратегія інформаційної безпеки України, затверджена Указом Президента України від 15 жовтня 2021 року №685/2021 [30].

Стратегія інформаційної безпеки України на період 2021−2025 років виявляє різні загрози та проблеми, які впливають на національну безпеку через інформаційні кампанії. Вона описує, як зовнішні ворожі сили, як державні, так і недержавні актори, застосовують дезінформацію, пропаганду та фальшиві новини для підриву українського суверенітету та безпеки. Документ також пропонує кроки для нейтралізації цих інформаційних атак.

Цей стратегічний документ підкреслює важливість розвитку здібностей України у виявленні, аналізі та контрдії дезінформаційним атакам. Він засвідчує наші попередні заяви, стверджуючи, що ефективне протистояння дезінформації вимагає координованих зусиль на державному рівні, з включенням різних агентств, від військових до розвідувальних та правоохоронних органів.

Заходи стратегій боротьби з інформаційними операціями включають кілька ключових пунктів: створення системи раннього виявлення для моніторингу дезінформаційних акцій; запуск інтегрованого механізму для оперативного втручання у випадках дезінформації; розвиток співпраці з міжнародними установами, урядовими органами та неприбутковими організаціями для боротьби з дезінформацією, а також збільшення кількості проєктів та тренінгів з медійної освіти для підвищення здатності громадськості розпізнавати та реагувати на дезінформацію [30].

Крім того, стратегію можна розширити, включивши зміцнення резистентності населення та зосередження уваги на ключових елементах національної стійкості. Хоча не всі громадяни обізнані з актуальністю питань національної стійкості, що триває вже кілька років, існує необхідність у їхній модернізації та інтеграції в державну стратегію. Такий підхід сприятиме забезпеченню економічної, політичної, соціальної та культурної єдності, підвищенню інформаційної безпеки країни та розвитку критичного мислення серед населення [14]. Підриваючи стійкість громадян через інформаційно-психологічні операції, агресори можуть легко маніпулювати настроями людей та знижувати їхній моральний дух.

Ще одним видом механізмів, спрямованих на забезпечення інформаційної безпеки та протидію інформаційно-психологічним операціям, є інституційні механізми. Ці механізми охоплюють як державні, так і недержавні установи, які займаються формуванням та реалізацією політики в інформаційній сфері нашої країни. На сьогодні серед суб'єктів цієї політики відзначаються:

– Рада національної безпеки і оборони України (РНБО);

– Міністерство інформаційної політики України (МІП);

– Міністерство закордонних справ (МЗС);

– Міністерство оборони України (МО);

– Державна служба спеціального зв'язку та захисту інформації України;

– Кіберполіція [2, с. 56-62; 45].

Діяльність цих органів має вирішальне значення для нейтралізації інформаційних загроз та захисту інформаційного простору України. Одним з вагомих досягнень РНБО у цій сфері стало створення Міжвідомчої робочої групи з протидії пропаганді та дезінформації. Окрім цього, РНБО розробила комплексну законодавчу базу, спрямовану на регулювання діяльності медіа та онлайн-платформ. До цієї бази входять закони про інформаційну безпеку та кіберзлочинність, які чітко окреслюють правила та відповідальність у цій сфері.

Міністерство інформаційної політики України розпочало ряд ініціатив з метою підвищення рівня медіаграмотності та критичного мислення серед населення. Однією з таких ініціатив стало створення спеціалізованого веб-ресурсу для виявлення та спростування фейкових новин і дезінформації. Крім того, Міністерство регулярно організовує прес-брифінги щодо найважливіших подій у зоні конфлікту, сприяючи отриманню українськими та закордонними ЗМІ доступу до достовірної інформації та поширенню об'єктивних фактів. Ці заходи сприяють можливості закордонних ЗМІ здійснювати зйомки репортажів, документувати терористичні акти росії на території України та сприяють розкриттю фейків, які поширюються кремлем та його спецслужбами, передусім перед міжнародною спільнотою.

Міністерство закордонних справ активно займається збільшенням усвідомленості щодо безпекових викликів, що стоять перед Україною, та протидією кампаніям дезінформації за її межами. Для цього був утворений Департамент стратегічних комунікацій, який відповідає за координацію комунікаційних ініціатив України з міжнародними партнерами. Крім цього, Міністерство активно взаємодіє з міжнародними організаціями, такими як Європейський Союз і НАТО, для спільного реагування на кампанії дезінформації та налагодження партнерства. Участь України у Партнерстві НАТО з інформаційної та кібербезпеки, а також в програмі ЄС "Східне партнерство" підтверджує його зобов'язання до спільних заходів зі зміцнення інформаційної безпеки.

Роль Міністерства оборони України у протидії інформаційно-психологічним операціям є ключовою. Цей центральний орган виконавчої влади та військове управління мають визначені повноваження в інформаційній сфері стосовно ЗСУ. Основними завданнями є протидія інформаційним атакам, спрямованим на українську армію, та забезпечення достовірності та передачі інформації через ЗМІ [2, с. 58; 52].

Підрозділ кіберполіції відповідає за розслідування та припинення кіберзлочинів, зокрема тих, що пов'язані з кампаніями дезінформації. Кіберполіція провела кілька значущих розслідувань кібератак і кампаній з дезінформації, що призвели до арешту та судового переслідування осіб, причетних до цих дій. Також були виявлені та нейтралізовані численні хакерські атаки на інформаційні системи України, здійснені російськими хакерами тощо [5, с. 89-90; 81].

Як відзначалося раніше, одним із ключових завдань інформаційно-психологічного впливу росії є атаки на державні веб-сайти, соціальні мережі, ЗМІ та інше, оскільки значна частина молоді отримує новини саме через Інтернет, переглядаючи офіційні ресурси та сторінки від авторитетних осіб, включаючи блогерів, які стають об'єктом кібератак. Все це може мати вплив на політичний простір України, політичну свідомість та підривати критичне мислення громадян, замість цього викликаючи емоційну реакцію.

Таким чином, Росія має значний досвід у проведенні інформаційної війни. Під час повномасштабної воєнної агресії проти України, Росія веде інформаційну атаку на всі сфери національної безпеки України з метою встановлення інформаційної монополії. Це спрямовано на дестабілізацію внутрішньої ситуації, деморалізацію та запобігання консолідації українського суспільства, підрив довіри, залякування та зупинення процесів євроінтеграції в Україні.

Часто рф використовує метод віддзеркалення – перекладає власну провину на жертву – у своїх інформаційно-психологічних операціях проти України. Цей метод ґрунтується на настановах Сталіна та інших державних діячів, які увійшли в історію як тирани.

Протягом останнього року повномасштабної війни та починаючи з 2014 року, Україна активно будує систему, яка здатна швидко реагувати на загрози інформаційної безпеки та передбачати поширення наративів, створених російською федерацією. Ця система ґрунтується на координації та співпраці різних державних органів та громадських організацій. Незважаючи на ці зусилля, загроза інформаційно-психологічних операцій залишається серйозною, і для ефективного протистояння інформаційно-психологічним операціям росії та забезпечення інформаційної безпеки України потрібні постійні зусилля.

3.3 Взаємодія України з міжнародною спільнотою у протистоянні інформаційно-психологічному впливу росії в кіберпросторі

З огляду на масштабне вторгнення Росії на українську територію, ключовою аудиторією для російських інформаційно-психологічних операцій стали громадяни країн Європи, США та інших держав. Протягом цього періоду Україна не лише зміцнювала внутрішні комунікаційні позиції, але й активно співпрацювала з міжнародними ЗМІ та громадськими організаціями, підвищувала імідж країни на міжнародному рівні, користуючись стратегією "м'якої сили".

Необхідність протистояти дезінформаційним кампаніям росії за її межами має декілька причин. По-перше, це пов'язано з великою кількістю українців, які

проживають за кордоном і піддаються психологічному тиску через російські інформаційно-психологічні операції, які порушують міжнародне гуманітарне право та домовленності. По-друге, це заважає об'єктивному ставленню держав до рф та поширенню недостовірної інформації серед іноземних громадян, що може підривати довіру партнерів до України, зокрема у питаннях надання військової допомоги, фінансової підтримки та інших аспектах співпраці.

Центр протидії дезінформації при Раді національної безпеки і оборони України відіграє важливу роль у міжнародному співробітництві з питань протидії інформаційно-психологічним операціям. Цей центр активно залучає держави та міжнародні організації до спільних дій у сфері обговорення, обміну досвідом та розробки системи заходів з нейтралізації негативного впливу інформаційно-психологічних операцій з боку Росії та її союзників. Протягом періоду широкомасштабного вторгнення було організовано різноманітні міжнародні зустрічі та конференції з участю таких країн, як Латвія, Сінгапур, Туреччина, Польща, Фінляндія, Естонія, Румунія, Грузія, Словаччина, Молдова, Японія та інші. Головною метою цих заходів є зміцнення співпраці з міжнародними партнерами для об'єднання зусиль у протидії загрозам інформаційній безпеці на національному та міжнародному рівнях.

Міністерство цифрової трансформації України ініціювало програму Digital4Freedom, яку було представлено під час конференції з післявоєнного відновлення України у Лугано. Цей проєкт спрямований на міжнародних партнерів і спрямований на залучення широкого кола зацікавлених сторін для вдосконалення та розвитку цифрової інфраструктури України [18].

Одним із етапів міжнародного співробітництва у сфері протидії інформаційно-психологічним операціям російської федерації є ініціатива "One Voice" або "Єдиний Голос", також відома як "Інформаційний Рамштайн", про яку ми вже згадували раніше. Ця ініціатива є ефективною на всіх рівнях системи протидії дезінформації. Її дії включають масштабну заборону мовлення російських пропагандистських телеканалів, таких як "Sputnik", "RT/Russia Today", "РТР Планета", "Россия 24", "ТВ Центр − Международный" та інших, як у межах

України, так і в країнах Європейського Союзу. Також передбачається об'єднання соціальних платформ для просування єдиної позиції з метою ліквідації загроз інформаційній безпеці.

Також важливим кроком у спільній боротьбі з психологічними операціями та пропагандою кремля є визнання у лютому 2023 року Службою зовнішніх справ ЄС росії світовим лідером у сфері дезінформації [23. с. 147-150; 74]. Це свідчить про дружні відносини з партнерськими країнами та реальну причетність рф до психологічних операцій.

Ухвалення Верховною Радою України заяви про визнання Чеченської Республіки Ічкерія тимчасово окупованою Росією, а також засудження геноциду чеченського народу стало резонансною подією, яка привернула пильну увагу світової спільноти до злочинних дій Росії в Україні та на інших окупованих територіях [34]. рф продовжує висувати претензії до інших держав, розповсюджуючи пропаганду й виправдовуючи свої дії в Україні, а також залякуючи противників цих наративів. Однак цей важливий дипломатичний крок України допоможе народам, що страждають від колонізації росією, а також країнам, що підтримують рф, побачити реальну сутність країни-агресора.

Спільні заходи України та інших країн світу для протидії дезінформації з боку кремля свідчать про те, що це є однією з ключових стратегічних мет кожної демократичної держави. Наприклад, у вересні 2022 року Україна, Румунія та Молдова узгодили спільну декларацію, в якій зобов'язалися розробити механізм координації зусиль у протидії дезінформації, поширюваної росією [35].

Ключовим кроком у формуванні системи протидії інформаційно-психологічним операціям росії було прийняття заходів Європейським Союзом та такими країнами, як Велика Британія, Канада, США, Австралія та інші. Ці заходи передбачали введення санкцій проти ключових медіа-каналів, які поширюють пропаганду, зокрема, RT та Sputnik [53; 62]. Крім того, Reddit і Telegram повністю заборонили на своїх платформах ЗМІ, які підтримують росію, після відповідного запиту з боку Європейського Союзу; Twitter також припинив розширення державних облікових записів з аналогічних причин [85].

Окрім стратегічних комунікаційних заходів у відповідь на конкретний вміст, міжнародні партнери також активно працюють над спрощенням поширення перевіреної інформації через ЗМІ та соціальні медіа. Наприклад, уряд Великої Британії виділив додаткові кошти для підвищення потужності Всесвітньої служби BBC з метою поширення незалежних, об'єктивних та достовірних новин в умовах посилення пропаганди з боку російської федерації [50].

Деякі держави, такі як Канада та США, активно протистоять російській пропаганді та дезінформації, розміщуючи офіційні наративи на урядових веб-ресурсах і розкриваючи правдиву інформацію щодо цих подій [54]. Така спільна діяльність є важливою для протидії дезінформації, що поширюється через кібератаки на інформаційні мережі, спрямовані на новинні сайти, урядові портали та комунікаційну інфраструктуру в Інтернеті.

Співпраця з міжнародними ЗМІ виявляється важливим і позитивним чинником у боротьбі з дезінформацією та пропагандою, яку поширює росія. Аналіз вмісту деяких зарубіжних агентств (Think Tanks) і видавництв, таких як "The Wall Street Journal" [80], "The Telegraph" [29], "BBC News" [51] та "The Atlantic Council" [49], розкриває різноманітні наративи, які часом протистоять інтересам України, а іноді підтримують її. За даними дослідження, починаючи з 24 лютого 2022 року, ці агентства активно публікують матеріали англійською мовою, які охоплюють створення або посилення антипутінської коаліції; злочини, скоєні російськими окупантами; акти ядерного шантажу та інші спроби тиску з боку кремля; реальні результати бойових дій на фронті; розповсюдження дезінформації росією у різних країнах світу, і т. д.

Аудиторією, на яку націлені агентства, є українці та міжнародна спільнота. Включення громадян росії до цільової аудиторії дозволить їм мати доступ до достовірної та точної інформації, що сприятиме формуванню свідомості та стійкості. Крім того, майже кожне з наведених агентств створило рубрики на своїх офіційних веб-сайтах, які присвячені Україні, зокрема «Ukraine», «War in Ukraine» та «UkraineAlert», де регулярно (кожні 2-3 дні) публікуються матеріали про події в країні. Наприклад, Atlantic Council надає важливу платформу для публічних заходів

з участю американських, європейських та українських лідерів та експертів, де обговорюється важливість прийняття обґрунтованих та невідкладних рішень, а також спростування дезінформаційної кампанії, організованої кремлем.

Платформа Atlantic Council слугує майданчиком для публікацій статей та висловлювань відомих особистостей та авторитетних діячів з України. Серед авторів публікацій - Міністр оборони Олексій Резніков, Народний депутат Олексій Гончаренко, а також громадські діячі та експерти, такі як Олена Хоменко та Ольга Айвазовська. Крім того, на сайті представлені звернення Президента України Володимира Зеленського, цитати з його промов та виступи посадових осіб, зокрема керівника Офісу Президента Андрія Єрмака. Ця різноманітність голосів та думок дає можливість отримати глибоке та багатогранне розуміння поточних подій в Україні [49].

Співпраця України з «The Wall Street Journal» відзначається тим, що журналісти та кореспонденти видання незалежно реєструють події на території України, документують дії російських військ і створюють матеріали про злочини окупантів [80]. Це сприяє підвищенню довіри міжнародного співтовариства до інформації та допомагає у боротьбі з пропагандою рф та спрямовує увагу журналістів на об'єктивне висвітлення подій. Взагалі, співпраця з міжнародними ЗМІ сприяє об'єднанню демократій та протистоянню російській пропаганді та імперіалізму.

Окремі країни прикладають зусилля до боротьби з російською дезінформацією, паралельно з ініціативами міжнародних організацій, які проводять перевірку фактів. Наприклад, НАТО розвиває власну систему спростування шкідливих російських наративів [30]. Аналогічно працює проєкт EUvsDisinfo, який належить до Європейської служби зовнішніх дій (EEAS). Його завданням є виявлення, аналіз та реагування на російські кампанії дезінформації, спрямовані проти Європейського Союзу, його держав-членів та країн регіону [36].

У вересні 2022 року Україна приєдналася до програми "Цифрова Європа", спрямованої на поширення цифрових технологій серед підприємств, громадян та державних структур. Цей крок має важливе значення у контексті підвищення

ефективності заходів у сфері Інформаційної Безпеки та застосування активних методів цифрових технологій, штучного інтелекту та кібербезпеки. Цифрові технології та інфраструктура відіграють ключову роль у забезпеченні національної безпеки та захисту інформації [23].

Фінансова підтримка від міжнародної спільноти має велике значення, оскільки вона може запобігти просуванню інформаційно-психологічних операцій з боку російської федерації не лише на територію України та тимчасово окупованих територій, а й у інформаційному просторі інших країн світу. Важливою проблемою залишається вплив росії на країни Африки, Латинської Америки та пострадянські країни, а також її участь у міжнародних змаганнях, олімпіадах, кінофестивалях та інших подіях. Культурні проекти, які вже з часів СРСР використовувалися для дискредитації, утисків та пропаганди, залишаються значним фактором впливу на аудиторію.

Значимі можливості покращення міжнародного співробітництва України у сфері протидії інформаційно-психологічним операціям росії варто відзначити:

– Розширювати міжнародну співпрацю та обмін досвідом з країнами, які успішно протистоять ІПСО.

– Залучати міжнародних партнерів до підтримки та розвитку стійкості України, зокрема через співпрацю з ЄС та НАТО.

– Активно співпрацювати з аналітичними центрами та ЗМІ за кордоном щодо протидії кремлівській пропаганді.

– Створювати або приєднувати більше українських агенцій та видань за кордоном, організовувати власні ефірні години та вести ефіри за межами країни.

– Збільшувати кількість іноземних медіаканалів в Україні, зокрема локальних видань.

– Забезпечити Міністерству закордонних справ та Міністерству інформаційної політики можливість виходу в ефір за кордоном та спілкування з аудиторією за кордоном.

– Заборонити розповсюдження ІПСО росії за кордоном та відсторонити її від участі у міжнародних конкурсах та змаганнях.

– Розвивати культурну дипломатію України для покращення міжнародного іміджу держави та протидії ІПСО росії шляхом просування культурних проєктів на міжнародну арену.

3.4 Аналіз моделі життєздатності системи інформаційного протиборства в кіберпросторі

Вплив інформації набуває все більшої важливості в сучасному світі, що визначається глобалізацією та переходом до інформаційного суспільства. Цей процес сприяє розширенню використання інформаційних засобів для досягнення різноманітних цілей. Військова, політична та економічна сфери є основними областями застосування такого впливу. Під час воєнних дій важливими аспектами є підтримка населення військовими діями, дезорганізація та деморалізація противника. У політичній сфері акцент робиться на здобутті підтримки населення для влади, ідеологічному впливі. У сфері економіки основною метою є отримання переваги над конкурентами, будь то компанія чи держава. Інформаційно-психологічний вплив є одним з основних методів досягнення цих цілей.

Психоінформаційний вплив (ПІВ) охоплює вплив на свідомість окремої особи або групи людей з метою зміни їхньої поведінки та/або переконань [1]. Це ставить питання забезпечення психо-інформаційної безпеки в актуальний план.

Захищеність психіки людини від негативного впливу деструктивної інформації у свідомість і/або підсвідомість, що може призвести до неадекватного сприйняття дійсності, складає основу інформаційно-психологічної безпеки особи (у вузькому розумінні) [2].

Забезпечення інформаційно-психологічної безпеки стало особливо актуальним в Україні через агресію Росії проти країни. Це породило необхідність формування підтримки територіальної цілісності України серед частини населення, а також збереження високого морального бойового духу військовослужбовців Збройних Сил України.

Основні принципи концепції інформаційного протиборства та війни були сформульовані передовими зарубіжними вченими, зокрема з США та Китаю, але значний внесок у цей напрямок зробили й вітчизняні дослідники.

Українські вчені Р. Грищук, І. Канкін та В. Охрімчук досягли значних успіхів у дослідженні інформаційного протиборства. За їхніми дослідженнями, суб’єктами цього протиборства є вище політичне та військове керівництво держави, органи місцевого самоврядування та саме населення [6].

Зловмисники активно використовують методи інформаційного протиборства, щоб посіяти розбрат і хаос у суспільстві. Ці методи ґрунтуються на глибокому розумінні психології людини та здатні впливати на її емоції, думки та поведінку. Науковці виділяють п'ять ключових характеристик методів інформаційного протиборства. Ця класифікація визначає наступні суб'єкти, на яких спрямоване інформаційно-психологічне протиборство:

- системи для ухвалення політичних рішень;

- механізми формування громадської думки;

- інструменти створення суспільної свідомості (книги, фільми, телевізійні передачі, видані ЗМІ);

- психологічний вплив на психіку людей, що приймають рішення (дискредитація лідерів) та інше [6].

За метою (AE) виокремлюють методи пропаганди та контрпропаганди [6]. Пропаганда спрямована на поширення серед певної групи людей необхідної інформації. Контрпропаганда спрямована на припинення поширення повідомлень у інформаційному просторі.

За джерелами поширення (SD) різні методи проявляються у способах їх втілення [6]. Важливу роль в цьому відіграють засоби масової інформації (ЗМІ): телерадіомовлення та друковані видання. Протягом останнього десятиліття спостерігається надзвичайний розвиток Інтернет-ресурсів. Однак традиційні ЗМІ мають свої переваги. По-перше, це аудиторія: частка населення, яке переглядає телебачення, значно перевищує тих, хто використовує електронні ЗМІ. Іншою

перевагою є те, що телебачення має сильніший вплив на фонове та наведене сприйняття інформації.

При обиранні методів, способів та прийомів впливу важливо враховувати особливості цільової аудиторії (РА) [6]. Важливо враховувати такі характеристики, як вік, соціальний статус та рівень обізнаності аудиторії.

У своєму дослідженні автори розглядають схему «Технологічні аспекти інформаційного протиборства на сучасному етапі», де докладно описані всі аспекти та їх взаємозв'язок (див. рис. 3.2) [6].

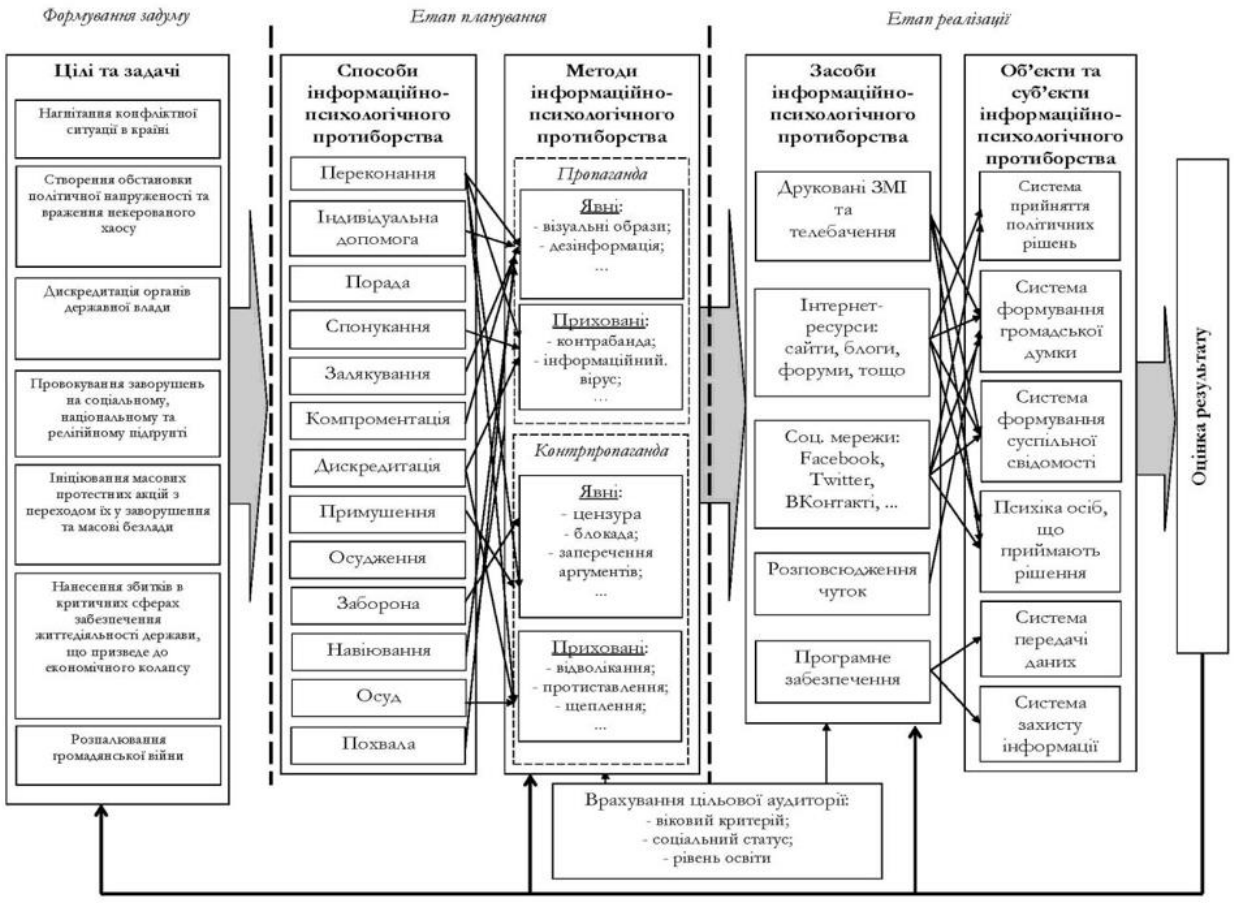

Рисунок 3.2 – Технологічні аспекти інформаційного протиборства на сучасному етапі

Вчені з Австралії, Біл Хатчісон та Мет Уорен, визначили та дослідили тактики інформаційного протиборства, однією з ключових стратегій якого є інформаційно-психологічний вплив. Їх дослідження описує різноманітні режими інформаційних атак, використовуючи модель життєздатності системи

інформаційного протиборства як основу для їх проведення. Це спрямовано на використання методів системного аналізу уразливостей інформаційної інфраструктури у всіх типах організацій. Акцент робиться на процесі атаки, а не на контрзаходах (див. рис. 3.3).

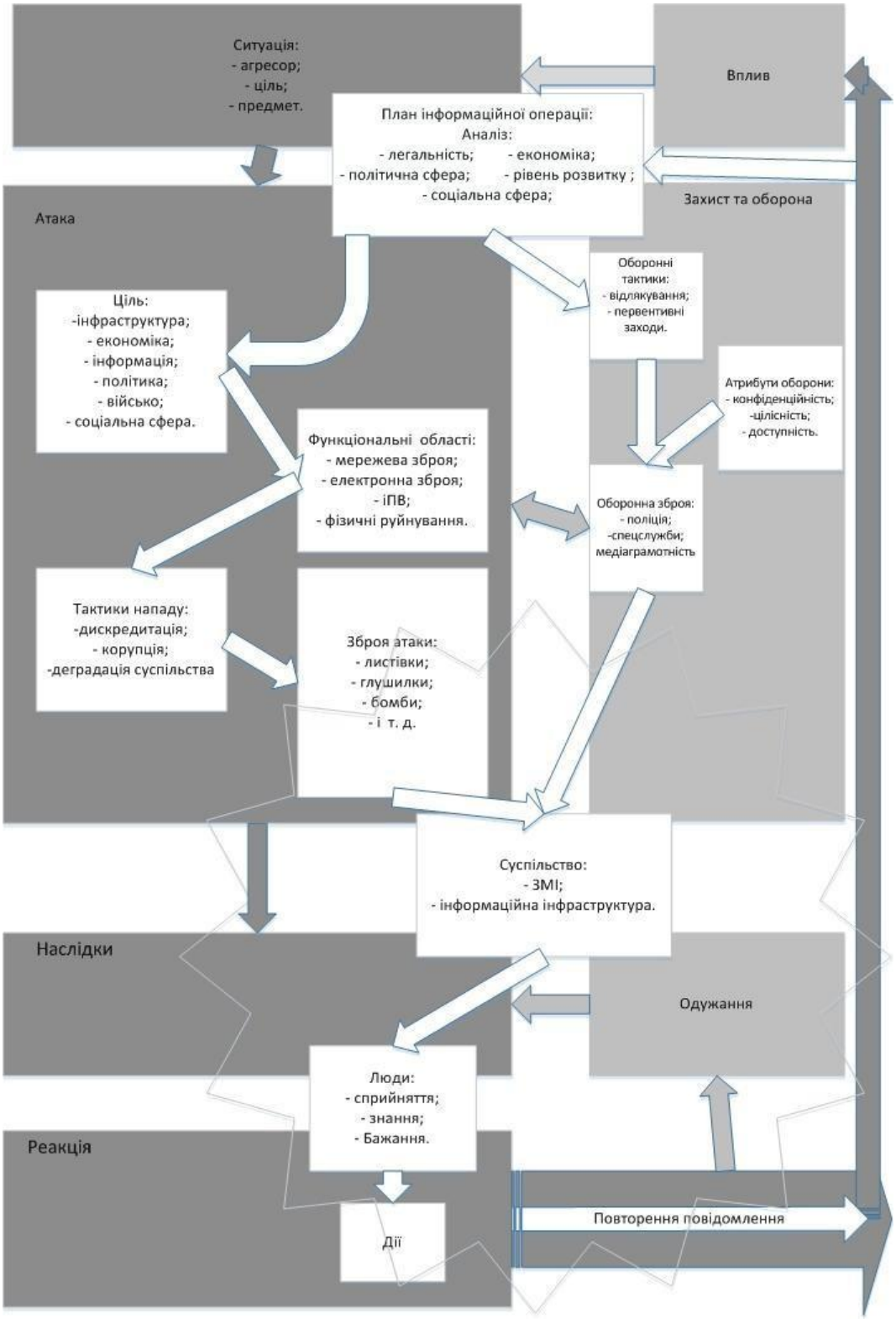

Рисунок 3.3 – Модель життєздатності системи інформаційного протиборства

Існує кілька способів використання інформації або інформаційних систем для проведення інформаційного протиборства. Нижче наведено деякі агресивні тактики, які розроблені дослідниками:

– інформацією можуть маніпулювати або спотворити. З одного боку, це може бути реклама, а з іншого – навмисна дезінформація;

– інформацію можуть перехопити, надаючи зловмиснику уявлення про сильні та слабкі сторони противника;

– інформаційні потоки до цільової аудиторії можуть бути перервані або зупинені, створюючи перевагу для атакуючої сторони;

– цільова аудиторія може бути перенасичена інформацією, що уповільнює обробку та перевірку отриманих даних;

– інформація може бути недоступною або заблокованою для аудиторії;

– порушення інформації або інформаційних потоків призводить до зниження надійності інформаційної системи;

– розкриття конфіденційної та таємної інформації ставить владу в незручне положення [12].

Атаки можуть бути мотивовані організаційними цілями або зловмисними намірами. Напади можуть здійснюватися як колективними організаціями, так і окремими особами. Деннінг ідентифікував п'ять класів ресурсів, які використовуються у інформаційній війні:

- Контейнери: комп'ютери та людські спогади;

- Транспортери: люди та телекомунікаційні системи;

- Датчики: сканери, камери, мікрофони та людські почуття;

- Реєстратори: принтери, людські процеси, що відображають характеристики інформаційного середовища;

- Процесори: мікропроцесори, люди, програмне забезпечення [13].

Кожен з цих елементів або їх складові можуть бути об'єктом атаки. Таким чином, спектр об'єктів може варіюватися від громадської думки до незначного

послання. Дослідники описують життєздатну модель інформаційного протиборства (VSM) Стафорда Біра (див. рис. 3.4) [14].

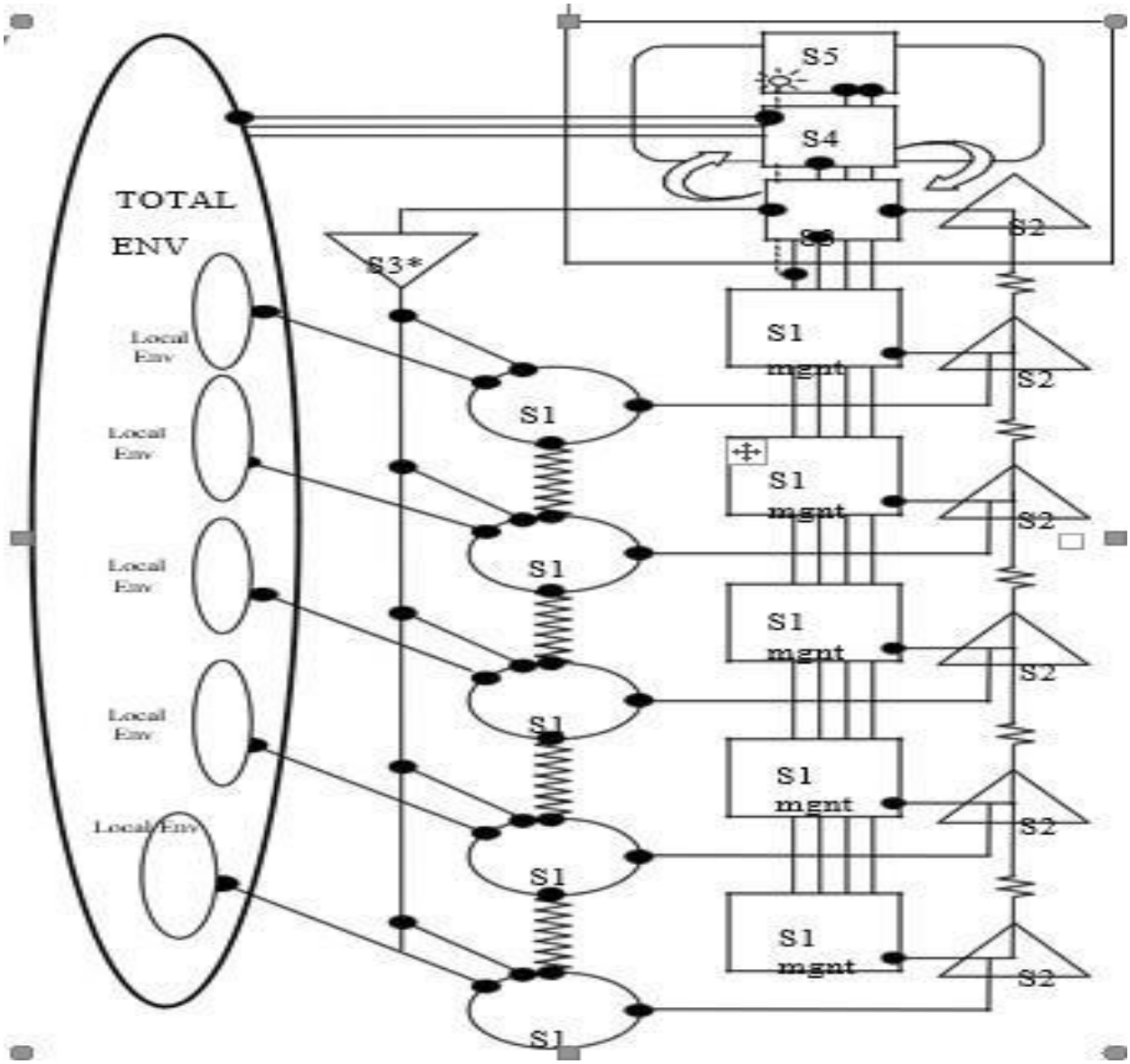

Рисунок 3.4 – Життєздатна модель інформаційного протиборства Стафорда Біра

Модель включає п'ять підсистем з такими функціями [12]:

1. Реалізація (S1) включає напівавтономні блоки, які виконують оперативні завдання у системі. Вони є основою для функціонування системи і взаємодіють з місцевим середовищем та один з одним. Кожен блок має своє власне локальне управління, яке інтегрується з більш широким управлінням вертикальними інформаційними потоками. Вона є складовою частиною роботи організації.

2. Координація (S2) забезпечує координацію S1 так, щоб кожен блок S1 працювала на користь системи в цілому, а не лише на власну. Це може бути досягнуто за допомогою простого графіка або етичних стандартів серед співробітників.

3. Внутрішній контроль (S3) опрацьовує дані з політики "вищого" рівня (S4) і "нижчого" рівня. Цей процес відповідає за контроль на оперативному рівні. Його завдання полягає в реалізації політики.

4. Розвідка та розробка (S4) виступає як фільтр даних з S3 і зовнішнього середовища.

5. Стратегія та політика (S5) визначає напрямок розвитку системи в цілому. Вона відповідає за збалансування внутрішніх і зовнішніх чинників.

Дослідники детально аналізують атаки на кожну з функцій:

Атака на головні активні блоки (S1)

Основні блоки можуть бути пошкодженні наступним чином:

- припинення їх роботи в локальному середовищі;
- відключення від інших підрозділів S1;
- відокремлення від функцій керування.

Дані можуть бути застосованими для спотворення місцевого середовища. Це призводить до погіршання взаємодії між окремими компонентами та значного ускладнення управління ними. Напади спрямовані на зниження ефективності організації шляхом порушення функціонування систем оперативного реагування [12].

Атаки на процес координації (S2)

Атаки на процес координації (S2) націлені на розірвання єдності діючих блоків. Вороги намагаються маніпулювати, замінювати або заперечувати інформацію, щоб зробити цей процес неспроможним ефективно функціонувати.

В результаті такої атаки, діяльність одиниць S1 могла б стати хаотичною, з одиницями, що діють у протиріч одна з одною до стану повного провалу. Один із способів досягнення цього – розповсюдження фальшивих новин, що деморалізує

противника. У таких нападах активно застосовують інформаційно-психологічні методи, що дозволяють адаптувати умови проведення операцій [12].

Атаки на функції управління (S3)

Ключовим аспектом атак на контрольні функції є маніпулювання інформацією, що впливає на сприйняття політичних рішень. Так, інструкції з S1, що відповідають політичним цілям, розробляються у S5. Зміни в інформаційних потоках між S3 і S1 призводять до адаптації функціоналу S4. У результаті цього етапу політика може бути змінена або спотворена.

Метою атак на є S3 перешкоджання або зупинки продуктивної взаємодії між розробкою політики в інформаційному середовищі та її реалізацією. Відповідно, головним завданням є зниження ефективності спілкування між різними сегментами інформаційної системи [12].

Знищення «мозку» і почуття організації (S4 / S5)

Завданням S4 є створення динамічної взаємодії між зовнішнім та внутрішнім середовищами через аналіз та інтеграцію інформації з S5 та S3. Зі свого боку, S5 формулює політику на основі даних, отриманих від S4.

Ці дві функції виступають як інтелектуальне ядро середовища. Основна ціль атаки полягає у формуванні помилкових переконань про внутрішнє та зовнішнє середовища, а саме у розробці політик та стратегій, що не відповідають дійсному стану речей. Конечною метою є руйнування інформаційного ландшафту. S4 може страждати від перевантаження некоректною інформацією, що спричиняє замішання та зниження довіри. Згідно з аналізом, ключові функції S4 включають збір, обробку, аналіз і розповсюдження інформації.

Рівень "Інформація" поділяється на наступні категорії: дані (результати вимірювань та спостережень); інформація (дані, які були упорядковані та проіндексовані); знання (глибоке розуміння інформації); мудрість (ефективне використання знань).

Отже, основною задачею атак є спотворення і маніпуляція інформацією для зміни стратегічних цілей у визначеному контексті. Інформація, спочатку впливаючи на цільову аудиторію, потім стає предметом маніпуляцій вже

встановленим сценарієм. Яскравий історичний приклад – британська дезінформаційна кампанія проти німецьких військ перед висадкою союзників у Нормандії в 1944 році. У більш пізніх етапах агресор мусить саботувати коректне використання стратегічних знань.

Висновки до третього розділу

У даному розділі було розглянуто ключові аспекти і стратегії протистояння інформаційно-психологічному впливу, особливо у контексті воєнної агресії Росії проти України. Проаналізовано інформаційну стратегію України та її основні принципи забезпечення інформаційної безпеки у протидії інформаційно-психологічному впливу в кіберпросторі. Окреслено важливість взаємодії України з міжнародною спільнотою для ефективного протистояння інформаційно-психологічному впливу Росії в кіберпросторі. Проведено аналіз моделі життєздатності системи інформаційного протиборства в кіберпросторі, що є важливим для подальшого вдосконалення стратегій та методів протидії інформаційно-психологічному впливу. Отримані результати є актуальним внеском у розвиток інформаційної безпеки та протидії інформаційним загрозам у кіберпросторі.

ВИСНОВКИ

Під час інформаційної війни однією з головних задач є забезпечення кібербезпеки. Однією з цілей цієї війни є вплив на морально-психологічний стан протилежної сторони, позбавлення її сил і здатності до протистояння, деморалізація.

У ході проведення нашого дослідження встановлено, що система протидії ІПСО рф складається з комплексу заходів на трьох рівнях: міжнародному, внутрішньодержавному та громадському.

Система протидії інформаційно-психологічним операціям в Україні ґрунтується на концептуальних засадах інформаційної безпеки держави. Ці засади охоплюють декілька ключових елементів:

1. Нормативно-правова база: До неї належать Закон про інформацію, Закон про Концепцію Національної програми інформатизації та Стратегія інформаційної безпеки України. Ці документи визначають загальні рамки та принципи протидії ІПСО.

2. Інституційний механізм: Національна система протидії ІПСО в Україні реалізується за допомогою комплексу державних органів. До них належать Рада національної безпеки і оборони України (РНБО), Міністерство інформаційної політики України (МІП), Міністерство закордонних справ (МЗС), Кіберполіція та інші. Кожен з цих органів має чітко визначені функції та повноваження у сфері протидії ІПСО.

3. Активна участь держави та громадян: Ефективна протидія ІПСО потребує не лише зусиль державних органів, але й активної участі громадянського суспільства. Це передбачає підвищення обізнаності населення про загрози ІППО, формування культури кібергігієни та залучення громадян до моніторингу та протидії інформаційним атакам.

Важливо підкреслити, що система протидії ІПСО в Україні не є статичною. Вона постійно розвивається та вдосконалюється з урахуванням нових викликів та

загроз. Це потребує постійного оновлення нормативно-правової бази, удосконалення роботи державних органів та активізації співпраці з громадянським суспільством.

В арсеналі інформаційних війн важливе місце посідають інформаційні операції, які поділяються на два типи: інформаційно-психологічні та інформаційно-технічні. Перші з них спрямовані на людину, маніпулюючи її свідомістю та думками, а другі – на кіберпростір, руйнуючи чи дестабілізуючи інформаційні системи. Стрімкий розвиток соціальних мереж став каталізатором для активізації комунікації в суспільстві. Це, в свою чергу, відкрило широкі можливості для використання інформаційно-психологічних операцій з метою маніпулювання суспільною думкою та свідомістю. Мета інформаційних операцій полягає в конструюванні цілісної картини світу, в якій дії та вчинки, що раніше здавалися б незрозумілими й невиправданими, стають виправданими. Це досягається шляхом формування певного бачення світу, яке змушує людей змінювати свою індивідуальну та суспільну свідомість.

Отже, розглянуті основні мотиви використання інформаційно-психологічних операцій у ході інформаційної війни, показано методи формування інформаційних впливів та їх наслідки. Також запропоновано кроки, спрямовані на зменшення впливу інформаційно-психологічних операцій під час інформаційної війни.

Вчені з багатьох країн широко досліджують процеси та розробляють методи інформаційно-психологічного впливу. У зв'язку зі сучасною ситуацією із інформаційним протиборством, актуальність цих досліджень лише зростає.

Сучасний епоха інформації стрімко змінюється і приносить нові методи ведення інформаційної війни. Необхідно приділяти вагому увагу розробці ефективних стратегій протидії ризикам, з урахуванням гнучкості та непередбачуваності інформаційної зброї, а також концепції інформаційних війн. Крім того, на постійній основі потрібно не лише спростовувати пропаганду та дезінформацію, але й вивчати успіхи супротивника на інформаційному фронті, щоб працювати на випередження та уникнення зростання інформаційних загроз і їх впливу на громадян та державу.

Вивчивши теоретико-методологічні основи феномену інформаційно-психологічних операцій, можемо зазначити, що вони є складовою частиною інформаційної війни, спрямованою на вплив на свідомість і поведінку суспільства. Водночас, інформаційна війна - це більш широке поняття, оскільки включає в себе не лише інформаційно-психологічні операції, а й кібератаки та інші інформаційні загрози для держави в цілому. ІПСО можна використовувати як для створення сприятливого інформаційного поля, так і для поширення дезінформації, що негативно впливає на емоційний стан, думки та поведінку цільової аудиторії.

Під час нашого дослідження було визначено, що інформаційно-психологічні операції, проведені рф, є довготривалою системою заходів, спрямованих на використання інформаційних і комунікаційних технологій та психологічних методів для впливу на громадську думку та поведінку. Вони можуть застосовуватися як у надзвичайних ситуаціях, під час воєнного стану, так і в мирний час. Інформаційно-психологічні операції зазвичай є комплексними і включають різноманітні методи, такі як пропаганда, дезінформація, стратегічна комунікація, медіа-кампанії, розповсюдження листівок та проведення психологічної оцінки тощо.

Проте мета таких операцій залишається незмінною: впливати на свідомість, думку та поведінку цільової аудиторії з метою захисту власних інтересів та безпеки. У контексті забезпечення безпеки людини, суспільства та держави інформаційно-психологічна операція працює у зворотному напрямку: вона використовується для протидії радикальним переконанням та поглядам, контрпропаганди, попередження кібератак на державному рівні, роботи на випередження, спростування, фактчекінгу тощо.

З історичної аналогії випливає, що інформаційно-психологічні операції рф ґрунтуються на політичних стратегіях Гітлера та Сталіна, які активно використовували пропаганду та дезінформацію для впливу на населення. Виявлено, що протягом повномасштабного вторгнення не було жодного дня, коли рф не проводила інформаційно-психологічні операції або не поширювала свої наративи про Україну.

Було визначено, що кремль послідовно, комплексно і на довгостроковій основі просуває п’ять основних наративів про Україну як країну, що, за його думкою, не має суверенітету, контролюється Заходом і є, за його твердженнями, фашистською державою, де відбувається громадянська війна. Ці наративи спрямовані на три аудиторії: російську, міжнародну, українську. Окрім того, розробляється окрема стратегія спрямована на населення тимчасово окупованих територій. Мета подібних кампаній – дестабілізація держави України, запобігання розширенню впливу України, НАТО та ЄС, а також відволікання уваги від власних внутрішніх проблем у державі.

Під час аналізу реалізації інформаційно-психологічних операцій Росією проти України ми виявили, що для досягнення своїх цілей через такі операції Росія здійснює контроль над інформаційним простором. Російська влада використовує різні методи проти журналістів та громадян, обмежуючи доступ до соціальних медіа в межах Росії, забороняючи їх використання та цензуруючи "некоректний" контент, і так далі.

Використовуючи метод когнітивного картування, ми з’ясували, що рф намагається здійснювати інформаційно-психологічні операції в усіх сферах національної безпеки України. Найбільш негативними факторами впливу на інформаційне середовище та загалом систему протидії російських інформаційно-психологічних операцій є:

– пропаганда, спрямована на поширення стокгольмського синдрому, зокрема на тимчасово окупованих територіях;

– поширення переконань, спрямованих на виклик відчуття приниження через те, що Україна нібито покинула українців, не планує деокуповувати території і т. д.;

– дозвіл на ефіри, телебачення та соціальні мережі російських медіа закордоном;

– стирання історичної пам’яті;

– використання дітей як об’єкту або суб’єкту власних інформаційно-психологічних операцій.

Виключення цих факторів впливу може зменшити ризик появи інформаційних загроз в інформаційному середовищі України та її партнерів.

Під час дослідження було виявлено, що система протидії інформаційно-психологічним операціям росії включає комплекс заходів, які реалізуються на трьох рівнях: міжнародному, внутрішньодержавному та громадському. Основою для формування цієї системи є концептуальні засади інформаційної безпеки України щодо протидії інформаційно-психологічним операціям.

Це означає наявність законодавчої бази, до якої входять такі акти, як Закон про інформацію, Закон про Концепцію Національної програми інформатизації, Стратегія інформаційної безпеки України, а також інституційні механізми, що охоплюють Раду національної безпеки і оборони України (РНБО), Міністерство інформаційної політики України (МІП), Міністерство закордонних справ (МЗС), Кіберполіцію та інші, а також активну участь держави та громадян.

У дослідженні висвітлено, що орієнтація державної політики України у сфері протидії інформаційно-психологічним операціям спрямована на захист національних інтересів, збереження суверенітету, територіальної цілісності, а також на забезпечення прав і свобод громадян.

У боротьбі з дезінформаційними атаками росії Україна залучає низку дієвих інструментів. Серед них: Центр протидії дезінформації при РНБО (ЦПД), який здійснює моніторинг інформаційного простору, виявляє та спростовує фейки, а також координує діяльність з протидії дезінформації на державному рівні; Центр стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України (ЦСКІБ), який розробляє та реалізує стратегію інформаційної безпеки України, а також проводить інформаційно-просвітницькі кампанії з питань протидії дезінформації; регулярні виступи, брифінги та зустрічі Президента України, який активно спілкується з громадськістю та світовою спільнотою, доносячи правдиву інформацію про ситуацію в Україні та спростовуючи російські пропагандистські наративи. Незважаючи на наявність у законодавстві України чіткої нормативно-правової бази, спрямованої на протидію

інформаційно-психологічним операціям росії, система інформаційної безпеки країни все ж таки потребує певних вдосконалень.

На рівні держави важливо швидко реагувати на інформаційні загрози. Це включає розробку технологій аналізу даних, використання власних засобів дистанційного зондування Землі, ШІ та супутникової системи навігації. Також потрібно формувати комплексну Національну стратегію відкритих джерел інформації (OSINT).

Аналіз показав, що обмін інформацією та даними розвідки щодо пропаганди та дезінформації рф є критичним напрямком у взаємодії України з міжнародними партнерами. Україна налагодила партнерські зв'язки з іноземними урядами та структурами для ефективного обміну цією інформацією та координації дій щодо протидії цим викликам. Окрім того, міжнародна підтримка України зростає, зокрема через фінансову та технічну допомогу в областях розвитку цифрових технологій та протидії дезінформації.

Дослідження підтвердило необхідність інтенсифікації міжнародної співпраці, зокрема через подальше розширення ініціативи «Інформаційний Рамштайн». Важливо зміцнювати зв'язки з аналітичними центрами та засобами масової інформації за кордоном, щоб ефективніше протистояти російській пропаганді. Крім того, необхідно залучати до цих зусиль все більше вітчизняних агенцій та видавництв, які діють за межами країни, розширювати присутність в Україні іноземних медіаканалів, додатково блокуючи канали поширення інформації від російських інформаційно-психологічних операцій за кордоном і запобігати участі Росії в міжнародних конкурсах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Syuntyurenko, O. V. "Network technologies for information warfare and manipulation of public opinion." Scientific and Technical Information Processing 42.4 (2015): 205-210.

2. Voitovych O., Holovenko V. Research of social networks as a source of information in warfare : Inżynier XXI wieku projectujemy przyszlosc, monografia [pod red: Jacek Rysiński] - Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016 . 111-119.

3. Дудатьєв А. В., Войтович О. П. Інформаційна безпека соціотехнічних систем: модель інформаційного впливу. Інформаційні технології та комп'ютерна інженерія. – Режим доступу : https://itce.vntu.edu.ua/index.php/itce/article/view/657/401

4. Dudatyev A. V. , Voitovych O. P. Моделі інформаційної підтримки управління комплексною інформаційоною безпекою. Радіоелектроніка, інформатика, управління 2017. № 1. С. 107-114.

5. Dudatyev, Andrey V. "Complex Method of Informational-Psychological Operations Counteraction." Journal of Automation and Information Sciences 49.1 (2017)

6. Шаравов И. К вопросу об информационной войне и информационном оружии // Зарубежное военное обозрение – 2012. – Вип. №10. – С. 3-5. 2. Кормич Б. А. Правові засади політики інформаційної безпеки України : монографія / Б. А. Кормич. – Одеса : Юридична література, 2013. – 472 с.

7. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К.: КНТ, 2016. – 280 с.

8. Історія інформаційно-психологічного протиборства : підруч. / [Я.М. Жарков, Л.Ф. Компанце- ва, В.В. Остроухов В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. Ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 212 с.

9. Інформаційна безпека: Підручник / [Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін.]; за заг. ред. Є.Д. Скулиша. – К. : КНТ, 2010. – 776 с.

10. Бєльська Т. В. Інформаційно-психологічна війна як спосіб впливу на громадянське суспільство та державну політику держави / Т.В. Бєльська. – Технології та механізми державного управління. – 2014. - №3. – С. 49-56.

11. Гріга В. С. Характеристика базових складових інформаційного протиборства/ В. Гріга, А. Гі- зун, І. Іванченко// Матеріали Другої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації». – Одеса, 2016. – С. 22- 25.

12. Бурячок В. Л. Можливість забезпечення захисту від інформаційно-психологічного впливу на основі універсального методу онтологій / В.Л. Буря- чок, А.А. Шиян // Сучасний захист інформації. – 2013. - №4. – С.57-67.

13. Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі / Р.В. Грищук, І. О. Канкін, В. В. Охрімчук // Захист інформації. – 2015. – Том 17. – № 1 – С. 80–86.

14. Van Niekerk B. The Information Warfare Life Cycle Model / B. Van Niekerk, M.S. Maharaj // SA Journal of Information Management – 2011. - Vol 13. - № 1–9 p.

15. Cox L. Planning for psychological operations: a proposal / L. Cox. – Air Command and Staff College, Maxwell Air Force Base, Montgomery, Alabama, 1997. – 89 p.

16. Pew R.W. Modeling Human and Organizational Behavior: Application to Military Simulations / Richard W. Pew and Anne S. Mavor. – Washington, D.C. : National Academy Press, 1998. – 418 p.

17. CEPA [Електронний ресурс]. – Mode of Access URL: http://infowar.cepa.org/ – Дата звернен- ня: 14.11.16.

18. Jormakka J. Modelling Information Warfare as a Game / Jorma Jormakka, Jarmo V. E. Mölsä // Journal of Information Warfare. – 2005. – Vol 4 (2). – №12. – 25 p.

19. Hutchinson B. Information Warfare: Using the Viable System Model as a framework to attack or- ganizations / B. Hutchinson, M. Warren. // Australa- sian Journal of Information Systems. – 2012. - Vol 9. -№ 2. – 10 p.

20. Denning D.E. Information Warfare and Se- curity / D.E. Denning. - Reading : Addison-Wesley, 1999. – 544 p.

21. Beer S. The Viable System Model: its prove- nance, development, methodology and pathology /S. Beer; Espejo R, Harnden R. (eds.). – Chichester, John Wiley & Sons, 1984. – PP. 211-270.

22. Johnson L. S. Toward a Functional Model of Information Warfare / L. S. Johnson // Center for the Study of Intelligence. CIA. – 8 p.

23. В. Грига. Информационно-психологи- ческая безопасность общества, как средство сохране- ния народа/ В. Грига, С. Гнатюк, А. Гизун// Безпека інформації. – 2015. – Том 21, 2. – С. 179-191.

24. Мороз А., Поліщук К. Роль сучасних технологій у системі протидії засобам застосування ІПСО рф в широкомасштабній війні проти України // Scientific Collection «InterConf», (152), С. 594-602. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/3223.

25. Оцінка громадянами ситуації в Україні та дій влади, довіра до соціальних інститутів (лютий − березень 2023 р.) // Разумков Центр. URL: https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-sytuatsii-v-kraini-ta-dii-vlady-dovira-do-sotsialnykh-instytutiv-liutyi-berezen-2023r.

26. Петрик В. Сутність і особливості проведення спеціальних інформаційних операцій та акцій інформаційного впливу // Сучасні інформаційні технології у сфері безпеки та оборони. 2019. № 3(6). С. 71−75.

27. Піддубний О. Що таке постправда? // Piddubny. com. URL: http://piddubny.com/scho-take-postpravda.

28. Поліщук К. Спільні дії ЄС та України у боротьбі з дезінформацією, як один із основних аспектів системи протидії ІПСО в період широкомасштабної воєнної агресії рф // Дипломатія в міжнародних відносинах: ретроспекція і

сучасність. Збірник матеріалів Всеукраїнської науково-практичної конференції з міжнародною участю. К. : НАУ, 2023. С. 147−150.

29. Поліщук К. Що таке ІПСО? // Ukrainian Women's Battalion. URL: https://www.instagram.com/p/Cri3ngvN_TC/?igshid=NTc4MTIwNjQ2YQ==.

30. Про доступ до публічної інформації : Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

31. Про захист інформації в інформаційно-телекомунікаційних системах : Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр - Text.

32. Про інформацію : Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650 // База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/2657-12.

33. Про Концепцію національної програми інформатизації : Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.182 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/75/98-вр - Text.

34. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 15.10. 2021. № 685/2021 // База даних «Законодавство України» / ВР України. URL: https://www.president.gov.ua/documents/6852021-41069.

35. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» : Указ Президента України №152/2022 // База даних «Законодавство України» / ВР України. URL: https://www.president.gov.ua/documents/1522022-41761.

36. Рачкевич М. Вийти з-під культурної тіні Росії: як Україна просуває культурну дипломатію // Радіо Свобода. URL: https://www.radiosvoboda.org/a/kulturna-dyplomatiya-ukrainskii-instytut/31117518.html.

37. Росія використовує культуру як зброю проти України // Армія Inform. URL: https://armyinform.com.ua/2022/12/08/rosiya-vykorystovuye-kulturu-yak-zbroyu-proty-ukrayiny/.

38. Ростислав Хотин Чому Україна визнала Чечню окупованою Росією і чи означає це визнання незалежності Ічкерії? // Радіо Свобода. URL: https://www.radiosvoboda.org/a/ukrayina-rosia-chechnya-nezalezhnist-ichkeria/32091704.html. (дата звернення: 02.05.2023). 35. Спільне комюніке 15 вересня 2022 // Посольство Румунії в Україні. URL: https://romania.mfa.gov.ua/news/spilne-komyunike-15-veresnya-2022-odesa.

39. Ткаченко О. «Інформаційний Рамштайн» – початок єдиного інформаційного фронту країн-союзників // Українська правда. URL: https://www.pravda.com.ua/columns/2022/09/30/7369845/.

40. Туранський М. О. Інформаційно-психологічні операції в гібридній війні: історіографічний аспект // Вісник Черкаського університету. 2018. С. 111−121.

41. Україна приєдналася до програми «Цифрова Європа»: що це означає // Економічна правда. URL: https://www.epravda.com.ua/news/2022/09/5/691138/.

42. Цикало К. Застосування технологій дистанційного зондування землі у військовій справі. Політ. Сучасні Проблеми Науки. Міжнародні відносини: Тези доповідей XXII Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених, Київ, 2022, Національний авіаційний університет / Редакційна колегія М.Луцький [та ін.]. – К.: НАУ, 2022. – 337 с.

43. Чередник Л. Діяльність українських масмедіа під час російсько-української війни // Бібліотекознавство. Документознавство. Інформологія. 2022. № 2. С. 75−81.

44. Abrams Z. The role of psychological warfare in the battle for Ukraine // American Psychological Association. URL: https://www.apa.org/monitor/2022/06/news-psychological-warfare.

45. Across Russia, journalists detained, threatened over coverage of Russia’s invasion of Ukraine // CPJ. URL: https://cpj.org/2022/02/across-russia-journalists-detained-threatened-over-coverage-of-russias-invasion-of-ukraine/.

46. Al-Khatib T. Hearts and Minds: History of Psychological Warfare // Seeker. URL: https://www.seeker.com/hearts-and-minds-history-of-psychological-warfare-1769783167.html.

47. Allyn B. Telegram is the app of choice in the war in Ukraine despite experts' privacy concerns // NPR. URL: https://www.npr.org/2022/03/14/1086483703/telegramukraine-war-russia. 48. Anual Media Consumption Survey // USAID. URL: https://internews.org/wp-content/uploads/legacy/2020-10/2020-Media-Consumption-Survey-FULL-FIN-Eng.pdf.

48. Atlantic Council // Atlantic Council. URL: https://www.telegraph.co.uk/.

49. BBC Gets Emergency Funding to Fight Russian Disinformation // GOV. UK. URL: https://www.gov.uk/government/news/bbc-gets-emergency-funding-to-fight-russian-disinformation. (дата звернення: 01.04. 2023). 51. BBC News // BBC News. URL: https://www.bbc.com/news.

50. Cadier A. Russia-Ukraine Disinformation Tracking Center // NewsGuard. URL: https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/.

51. Compliance with Professional Standards in Online Media. The 1st Wave of Monitoring in 2021 // Institute of Mass Information. URL: https://imi.org.ua/en/monitorings/compliance-with-professional-standards-in-online-media-the-1st-wave-of-monitoring-in-2021-i38434.

53. Countering disinformation with facts - Russian invasion of Ukraine // Government of Canada. URL: https://www.international.gc.ca/worlв-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng.

54. Demand for VPNs in Russia skyrockets by 2,000% after the Kremlin bans Instagram // Euronews. Next. URL: https://www.euronews.com/next/2022/03/15/demand- for-vpns-in-russia-skyrockets-by-2-000-after-the-kremlin-bans-instagram.

55. Disinfo Database: Ukraine // EU vs Disinformation. URL: https://euvsdisinfo.eu/disinformation-cases/.

56. Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses // OECD Policy Responses on the Impacts of the War in Ukraine. URL: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde.

57. Encyclopedia Britannica // Encyclopedia Britannica. URL: https://www.britannica.com/.

58. Fratus M. Killer vampires, demon dolls, and sauerkrast: a brief history of American PSYOPS // Black Rifle Coffee Company. URL: https://coffeeordie.com/craziest-american-psyops/.

59. Helmus T. The Ukraininan army is leveraging online influencers. Can the U.S. Military? // War On Rocks. URL: https://warontherocks.com/2023/03/the-ukrainian-armyis-leveraging-online-influencers-can-the-u-s-military

60. Joint Chief of Staff. Joint Publication 3-13. Information operations // Joint Chief of Staff. URL: https://irp.fas.org/doddir/dod/jp3_13.pdf.

61. Lawson H., Deka K., Funanakoshi M. Tracking Sanctions against Russia // Reuters Graphics. URL: https://graphics.reuters.com/UKRAINECRISIS/SANCTIONS/byvrjenzmve/.

62. Matyushenko Y. Zelensky Approves Regulation on Center for Countering Disinformation // Unian. Net. URL: https://www.unian.info/politics/center-for-counteringdisinformation-zelensky-approves-regulation-11413858.html%5d.%20%D0%94%D0%BE.

63. McCarthy L. Why Putin uses Russian law to crack down on dissent // The Washington Post. URL: https://www.washingtonpost.com/politics/2022/04/07/autocratsrussia-kremlin-protest-fines-jail/.

64. Misinformation Monitor: February 2023 // NewsGuard. URL: https://www.newsguardtech.com/misinformation-monitor/february-2023/. (дата звернення: 03.05.2024).

65. Morrish L. Fact-Checkers Are Scrambling to Fight Disinformation With AI // WIRED. URL: https://www.wired.co.uk/article/fact-checkers-ai-chatgpt-misinformation#intcid=_wired-uk-bottom-recirc_ba2a4245-0b76-4fce-85a8-fd94e5a166f7_similar2-3. (дата звернення: 01.05.2023).

66. Mouton F., Pillay K., Van't Wout C. The Technological Evolution of Psychological Operations Throughout History // Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance. 2016. P. 266−278.

67. Narula S. Psychological Operations (psyops): A Conceptual Overview // Strategic Analysis. Vol. 28. No.1. P.177–192.

68. NATO Standardization Office. Allied Joint Doctrine for Psychological Operations AJP 3-10.1. Brussels: North Atlantic Treaty Organization // NATO Standardization Office(NSO). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_d ata/file/450521/20150223AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf. (дата звернення: 03.05.2024).

69. NATO-Russia: Setting the Record Straight // North Atlantic Treaty Organization. URL: https://www.nato.int/cps/en/natohq/115204.htm. (дата звернення 03.05.2024).

70. Nevmerzhytskyi I. Procedure and Principles of Information and Psychological Operations in the North-Atlantic Alliance (Based on NATO Documents) // Challenges to national defence in contemporary geopolitical situation. 2020. P. 176−181.

71. Paul M. A. Linebarger. Psychological Warfare // Project Gutenberg. URL: https://www.gutenberg.org/files/48612/48612-h/48612-h.htm. (дата звернення: 03.05.2024).

72. RAND Corporation // RAND Corporation. URL: https://www.rand.org/. (дата звернення: 03.05.2024).

73. Report on EEAS Activities to Counter FIMI 2022 // The European External Action. URL: https://www.eeas.europa.eu/eeas/2022-report-eeas-activities-counter-fimi_en. (дата звернення: 03.05.2024).

74. Russian Government Orders Media Outlets To Delete Stories Referring To 'Invasion' Or 'Assault' On Ukraine // Radio Free Europe/Radio Liberty. URL: https://www.rferl.org/a/roskomnadzor-russia-delete-stories-invasion/31724838.html. (дата звернення: 03.05.2024).

75. Seskuria N. Russia Is Reenacting Its Georgia Playbook in Ukraine // Foreign Policy. URL: https://foreignpolicy.com/2022/02/22/russia-ukraine-invasion-georgia-2008- south-ossetia-tskhinvali. (дата звернення: 03.05.2024).

76. Since Russia invaded Ukraine in February 2022, almost all independent media have been banned, blocked and/or declared “foreign agents” // Reporters without borders. URL: https://rsf.org/en/country/russia. (дата звернення: 03.05.2024).

77. Song T. Information/Psychological Warfare in the Russia-Ukraine War: Overview and Implications // Institute of Foreign Affairs and National Security. URL: https://www.ifans.go.kr/knda/ifans/eng/pblct/PblctView.do?menuCl=P11&pblctDtaSn=14 006&clCode=P11. (дата звернення: 03.05.2024).

78. The Telegraph // The Telegraph. URL: https://www.telegraph.co.uk/. (дата звернення: 03.05.2024).

79. The Wall Street Journal // The Wall Street Journal. URL: https://www.wsj.com/. (дата звернення: 03.05.2024).

80. Thompson J. and Graham T. Russian Government Accounts Are Using a Twitter Loophole to Spread Disinformation // The Conversation. URL: http://theconversation.com/russian-government-accounts-are-using-a-twitter-loophole-to- spread-disinformation-178001. (дата звернення: 03.05.2024).

81. Tom Burt The hybrid war in Ukraine // Microsoft. URL: https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/. (дата звернення: 03.05.2024).

82. Tracy J. 100 years of subterfuge: the history of Army psychological operations// U.S. ARMY. URL:

https://www.army.mil/article/199431/100_years_of_subterfuge_the_history_of_army_psy chological_operations. (дата звернення: 03.05.2024).

83. Tsykalo K. The value of historical memory for the formation of public policy // Polit. Challenges of Science Today. International Relations: Abstracts of XXII International conference of higher education students and young scientists, Kyiv, 2022, National Aviation University / Editorial board Lutskyi M. [and others]. – K.: NAU, 2022.– 337 p.

84. Ukraine War Resource Hub // EU DisinfoLab. URL: https://www.disinfo.eu/ukraine-hub/. (дата звернення: 03.05.2024).

86. Vejvodová P. Information and psychological operations as a challenge to security and defence // Vojenské rozhledy. 2019. Nº 3. P. 83–96.

87. Wahlstrom A. The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine // MANDIANT. URL: https://www.mandiant.com/resources/information-operations-surrounding-ukraine. (дата звернення: 05.04.2023).