МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет міжнародних відносин

Кафедра журналістики

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

Васильченко В’ячеслав Миколайович

_____

«___» _____ 2021 р.

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

РОЗРОБКА ТЕЛЕГРАМ-КАНАЛУ ЩОДО ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВІЙНАМ “INFO BREAKER”

Виконавець: Несін Дмитро Анатолійович _____

Керівник: канд. філол. наук, доц.

Букіна Наталія Валеріївна _____

Нормоконтролер: канд. пед. наук, доц.

Остапчук Світлана Сергіївна _____

Київ – 2022

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

ЗМІ – засоби масової інформації

СРСР – Союз Радянських Соціалістичних Республік

США – Сполучені Штати Америки

НАТО – Організація Північноатлантичного договору

ООН – Організація Об'єднаних Націй

ПАРЄ – Парламентська асамблея Ради Європи

ЄС – Європейський Союз

ІП – інформаційний простір

ІО – інформаційні операції

ІМ – інформаційні можливості

ІС – інформаційна стійкість

ПСО – психологічні операції

ЗСУ – Збройні сили України

РЕВ – радіоелектронна війна

ВСТУП

Актуальність теми. На сучасному етапі розвитку суспільства спостерігається процес повсюдної інформатизації та виникнення всесвітнього інформаційного простору. Поряд із позитивними явищами глобальної інформатизації, чіткіше проявляються обриси нових проблем. Насамперед, це стосується сфери інформаційної безпеки та інформаційних війн. Не можна стверджувати, що ці проблеми виникли лише в умовах глобальної інформатизації, але виникнення єдиного світового інформаційного простору дозволило перетворити його на ще одне поле протистояння міжнародних суб'єктів. Використовуючи свою інформаційну перевагу, окремі держави чи їхні союзи здійснюють інформаційне протиборство з менш сильними суперниками.

Ефективність здійснення влади у будь-якій державі значною мірою залежить від його інформаційного забезпечення. Без інформації неможливо і уявити позитивно функціонуючу політичну структуру, розвиток масової політичної свідомості, взаємодію суб'єкта та об'єкта політики. У процесі інформаційно-комунікативної дії у свідомості народу формується образ державної влади, її політичних інститутів та лідерів. І керуючі функції держави здійснюються з найбільшим потенціалом та найменшими енергетичними витратами лише тоді, коли досить добре розвинена система інформаційних зв'язків між державою, громадянським суспільством та особистістю.

Необхідність дослідження цієї теми викликана тим, що у наш час міждержавні і міжнаціональні конфлікти дедалі частіше протікають в інформаційному полі. На наш погляд, це пов'язано із загрозою масового, у найгіршому разі – тотального знищення людей через можливість застосування зброї. Наслідком переходу основної маси міждержавних конфліктів від відкрито-озброєної стадії до потайно-інформаційної є збільшення психологічного тиску на індивідуумів. При цьому тиск чиниться з кількох сторін. Наприклад, якщо одна з держав намагається впровадити вигідні для себе настрої в іншій, а це, у

свою чергу, викликає захисну реакцію у відповідь, то в результаті громадяни другої держави стають точкою докладання серйозних зусиль з боку представників влади обох конфліктуючих сторін.

Проблематика інформаційних війн носить міждисциплінарний характер. Як науковий напрямок вона має кілька аспектів, зокрема, управлінський, економічний, організаційно-технічний, психологічний, правовий, культурологічний та інші. Однак останнім часом, коли в геополітичному просторі світу інформаційні технології та інформація в цілому набули визначального значення, політичний аспект вивчення інформаційних війн відіграє головну роль.

Для України інформаційна політика є додатковим потужним ресурсом у здійсненні модернізації країни та вирішенні багатьох поточних внутрішніх та зовнішніх проблем. Однак у цій сфері Україна не має стратегічного доробку на кілька років. Тому від політичної та наукової еліти України вимагається негайне прийняття рішень щодо формулювання державної стратегії, заснованої на справжніх інтересах суспільства, створення системи реалізації інформаційної політики та проведення конкретних заходів.

Цілком очевидним є той факт, що відставання країни в галузі технологій інформаційної політики не може сприяти успіху у вирішенні поставлених завдань. Ліквідувати відставання в цій галузі, як на теоретичному, так і на практичному рівні, можна лише при вивченні світового досвіду суб'єктів протиборства в інформаційній сфері.

Не секрет, що наша держава є учасником подібних конфліктів. Причому часто вона займає далеко не вигідну собі позицію, що негативно позначається на менталітеті її громадян. Для того, щоб знизити рівень психологічного тиску в ході таких конфліктів, необхідний, перш за все, ретельний аналіз ситуації, що складається зі знання закономірностей процесів, що відбуваються і вироблення адекватних заходів із мінімізації негативних наслідків.

У таких умовах «мирні» інститути (засоби масової комунікації) є провідниками різних ідеологій та зброєю у війнах нового покоління – «інформаційних», які, своєю чергою, можуть розглядатися як реалізація

конфліктів ідеологій. З'являються сучасні терміни: «інформаційні війни», «стратегії інформування», «інформаційна безпека» та ін., але поки що відсутні дефініції цих понять, як наукові, так і правові.

Ступінь наукової розробленості теми дослідження. Наукові знання про інформаційні війни та супутні їм процеси є комплексом результатів досліджень політологів, істориків, соціологів, філософів, психологів, правознавців, теоретиків засобів масової інформації та ін. Інформаційні війни тісно пов'язані із загальною природою масової комунікації, конфліктологією властивостями політичних відносин, поведінкою особистості, соціальних груп та суспільства в цілому, впливом засобів масової інформації (далі – ЗМІ). Тому як наукова проблема ця тема розглядалась переважно опосередковано – через призму суміжних галузей знання, що перебуває у полі дослідницької уваги зарубіжних і вітчизняних учених досить давно.

Положення, що лягли в основу вивчення теми роботи, вироблялися зарубіжними вченими початку XX століття. Насамперед, це результати досліджень таких соціологів, як Г. Лассуел, П. Лазарсфельд про вплив засобів масової комунікації на громадську думку. Актуальними є питання захисту від інформаційної агресії. Останнім часом інтерес до проблеми інформаційної безпеки поширився на академічні кола, свідченням чого є перелік дисертацій на дуже близькі до проблематики інформаційної війни теми. Теоретичні аспекти пострадянської інформаційної війни розглядали такі вчені, як І.І. Завадський, Н.І. Панарін, Г.Г. Почепцов, С.П. Расторгуєв та Д.А. Швецов. З погляду маніпуляції свідомістю особистості інформаційну війну розглядав Г.В. Грачов. Питання громадської думки розглядали такі учені, як Б.А. Грушин, В.А. Полторак та Ю.П. Сурмін.

Мета та завдання дослідження. Мета роботи – виявлення витоків і закономірностей розгортання «інформаційних війн» у контексті інформаційних процесів, що реалізуються на міжнародному та національному рівні, та вироблення практичних рекомендацій для створення телеграм каналу з метою інформаційного протиборства України.

У дослідженні були поставлені такі завдання:

- дослідити поняття, сутність та ознаки інформаційної війни;
- розглянути історичні засади наукових досліджень в галузі інформаційної війни;
- дослідити становлення проблеми інформаційної війни у XX ст.
- проаналізувати сучасний стан та перспективи розвитку інформаційної війни в сучасному інформаційному суспільстві;
- розробити телеграм канал «Info Breaker» як метод протидії інформаційній війні.

Об'єктом дослідження є протиборство суб'єктів інформаційного впливу у світі.

Предмет дослідження – особливості розробки телеграм-каналу «Info Breaker» на тему протидії інформаційним війнам.

Методи дослідження. Методологічною основою дослідження є принципи сучасної теорії політичної науки. У роботі використано такі методи дослідження як:

– індукції та дедукції – для зіставлення окремих наукових понять і категорій (інформаційна війна, інформаційне протиборство тощо);

аналогії та компаративістики – для поглибленого дослідження теоретичних, організаційних засад проведення інформаційної війни;

– тлумачення – для аналізу та розкриття змісту основних категорій інформаційного права, які характеризують понятійно-категоріальний апарат дослідження;

– історичний – для розгляду причин та передумов виникнення інформаційних війн;

– системно-структурний – для аналізу стану та перспектив розвитку проведення стратегій інформаційних війн.

Наукова новизна дослідження полягає в отриманих таких основних результатах:

1) вивчення причин виникнення інформаційних конфліктів;

2) виявлення специфіки поняття інформаційної війни;

3) систематизація методів здійснення зовнішньої інформаційної агресії;

4) визначення тенденцій зміни світового порядку у сфері інформаційного впливу;

5) вироблення рекомендацій щодо зміцнення становища України у глобальному інформаційному просторі.

Апробація. Основні теоретичні висновки та положення дослідження доповідалися здобувачем на науково-методологічному семінарі «Права людини: відображення у медіа просторі» (Київ 2022).

Публікації. Основні положення дипломної роботи було викладено в публікаціях: Несін Д. А. «Висвітлення конфліктів у медіа» (Київ 2022) (готується до друку).

Практичне значення результатів дослідження. Проведений аналіз послужить теоретичною та методологічною основою для подальших досліджень ідеологічних, політичних та соціально-філософських аспектів виникнення та здійснення інформаційної агресії насамперед на молодіжну аудиторію. Подані в роботі висновки будуть корисними при експертизі та прогнозуванні ідеологічної ситуації у міжнародному та вітчизняному інформаційному просторі.

Структура роботи. ВКР складається зі вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг дослідження становить 68 сторінок, список використаних джерел містить 51 найменування.

РОЗДІЛ 1
ІНФОРМАЦІЙНА ВІЙНА: ПОНЯТТЯ, ОЗНАКИ, ІСТОРІЯ ВИНИКНЕННЯ

1.1. Поняття, сутність та ознаки інформаційної війни

Інформаційні війни можуть загрожувати як усьому людству, так і окремій особистості. На сьогоднішній день термін «інформаційна війна» трактується по-різному. Насамперед це пов'язано з варіаціями перекладу словосполучення «information warfare». Його переводять і як «інформаційна війна», і як «інформаційне протиборство», і як «інформаційно-психологічна війна». Існує цілий ряд прийомів та методів визначення терміну «інформаційна війна».

Наприклад, дослідник Ю. О. Горбань першими інформаційними війнами вважав міфи, так як війська кожного завойовника слідкували за розповідями про їх жорсткість, що досить сильно підривало моральний дух противника [10, с.136].

У 1976 році Т. Рон у своїй доповіді «Системи зброї та інформаційна війна» вперше вжив поняття «інформаційна війна». Т. Рон звертав особливу увагу на те, що інформаційна інфраструктура є ключовим аспектом американської економіки і, в той же час, вона стає вразливою метою як у військовий, так і мирний час. Але, на думку М. І. Рибак, вперше термін «інформаційна війна» був вжитий 1967 року А. Даллесом у книзі «Таємна капітуляція». Книга присвячена таємним переговорам між США та Великобританією з одного боку та рейх-фюрером СС Гітлером – з іншого. Пізніше це поняття часто вживається у пресі [33, с.66].

Наприклад, Р.Чирва вважає, що інформаційна війна – це комплекс заходів щодо інформаційного впливу на масову свідомість для зміни поведінки людей і нав'язування їм цілей, які не входять до їх інтересів, а також захист від подібних впливів. У роботі ми визначаємо поняття «інформаційна війна» як свого роду конфлікт репутацій між різними коаліціями [45, с.8]. У рамках інформаційної війни неявна агресія виявляється більш суттєвою, ніж фізична агресія, хоча у

моменти відкритих збройних зіткнень обидва види агресії взаємно доповнюють одна одну.

Неявна агресія за визначенням реалізується через інформаційні канали ЗМІ. Інформація як втілення загрози та маніпуляції з метою досягнення конкурентної переваги над опонентом постає фундаментальною зброєю та метою інформаційної війни. Визнається необхідність дослідження оборонних взаємин між військовим керівництвом та цивільним населенням у процесі підготовки інформаційної війни.

Позначені взаємовідносини, у свою чергу, націлені на оптимальне поєднання захисту демократичних цінностей (свободи вираження поглядів достовірність особистого життя) та заходів, необхідних для захисту проти зовнішньої інформаційної загрози. Зазначена проблема гостро стоїть перед різними державами, оскільки інформаційні технології продовжують поширюватися в світі, що стрімко глобалізується.

З урахуванням комунікативної сфери інформаційної війни зазначені феномени дефінуються певним чином. Наприклад, у межах моделі, запропонованої М.Х. Боїсотом, дані асоціюються з самим об’єктом, різними його станами, подіями, до яких залучено об’єкт, який виявляє ті чи інші свої характеристики. Події та об’єкти мають свої специфічні характеристики. Опис цих показників і є даними. Знання, навпаки, характеризує суб’єкта (індивіда чи групу індивідів). Воно є набором взаємодіючих образів думки, мислень щодо даних, активованих конкретною подією [50, с.12].

Інформація – як сукупність даних, «відфільтрованих» суб’єктом у межах наявного в нього знання, визначає зв’язок між суб’єктом та наявними в нього даними. У певній ситуації знання використовують із опорою на певний контекст. У контексті інформаційної війни кожен з представлених вище елементів може відчувати інтегровані та динамічні атаки з боку протиборчої сторони (тобто впливу може зазнавати один або відразу всі елементи). Зокрема, якщо мішенню постають дані, то атакуюча дія може набувати наступних форм:

- відмова в отриманні даних: атаки на системи, що містять дані, стирання даних;

- фізичне знищення накопичувачів даних;
- крадіжка даних з подальшим їх маніпулюванням для реалізації цілей, що переслідуються.

«Поле бою» інформаційної війни постійно розширюється, виходить за рамки традиційних ситуацій збройного конфлікту. Щодо цього вона асоціюється з екстенсивним використанням інформаційних технологій з метою досягнення їх ефективності, рентабельності та оперативності. Така ситуація, своєю чергою, призводить до того, що семантика поняття «інформаційна війна» постійно розширюється і породжує більшою мірою плутанину, ніж чітку дефініцію [1, с.48].

З цієї причини у відповідних дослідженнях задіяно також термін «інформаційні стратегії», що означає використання інформації та інформаційних технологій як інструменту національної могутності, який може бути незалежним або реалізовуватися додатково до збройних операцій. В окремих випадках поняття про інформаційну війну набуває у працях дослідників езотеричного характеру.

Так, інформаційна атака, реалізуючись в універсумі матерії та енергії, представляється як сфера виняткового використання комп'ютерів та комунікації. Атаки неявної інформаційної війни впливають насамперед на рівень спостережень «акціонального циклу спостереження – орієнтація у навколишньої дійсності – прийняття рішення». Явна інформаційна війна руйнує рівень орієнтації зазначеного циклу з метою впливу на аналіз дійсності, який, у свою чергу, результується в актах прийняття рішень та реалізації конкретних дій.

На сьогоднішній день «інформаційна війна» є парасольковим концептом, який, за своїм визначенням, охоплює розрізнені положення з багатьох сфер знання і формує з них складніше утворення, що володіє дієвою пояснювальною силою. Серед найбільш частотних термінів, що використовуються для позначення різноманітних практик в аспекті інформаційної війни, можна відзначити наступні: безпека інформаційних систем, інформаційна перевага, інформаційне домінування, захист критичної інфраструктури, операційна безпека та багато інших [4, с.58].

Їх негативний вплив на найрізноманітніші цінності, як і самосвідомість сторони, що відчуває вплив, може не відчуватися протягом тривалого періоду, а іноді так і залишається не поміченим. Сторона, яка вдалася до інформаційної війни, здатна використати для своїх дій відповідний канал унаслідок взаємопов'язаності та взаємозалежності багатьох інфраструктур у сучасному світі.

І. О. Валюшко розглядає термін «інформаційна війна» у широкому розумінні. Вона визначає його як планомірний інформаційний вплив на всю інфокомунікаційну систему супротивника та нейтральні держави з метою формування сприятливого глобального інформаційного середовища для проведення будь-яких політичних та геополітичних операцій, що забезпечують максимальний контроль над простором [6, с.143].

Також інформаційна війна може трактуватися як нова форма боротьби двох і більше сторін. Тут слід згадати думку М. О. Зінченко, який вважає, що інформаційна війна полягає у цілеспрямованому використанні спеціальних засобів та методів впливу на інформаційні ресурси противника, а також захисту власного інформаційного ресурсу для досягнення призначених цілей [14, с.39].

Аналізуючи наукову літературу, слід розібратися, чи можна ставити знак рівності між поняттями «інформаційна війна» та «інформаційне протиборство». Деякі дослідники відзначають, що інформаційна війна – це протиборство, проте не всі автори погоджуються з цією думкою. Наприклад, М. О. Кондратюк зазначає, що інформаційне протиборство – це форма боротьби сторін, що полягає у впливі на інформаційне середовище протилежної сторони та захисті власної від негативних інформаційних впливів [19, с.14].

Відмінність цих двох понять лише в тому, що інформаційна війна виробляється активніше за допомогою диверсійних і терористичних методів. Саєнко О.Г. вважає, що поняття «інформаційна війна» та «інформаційне протиборство» рівні [33, с.144]. Н. Ф. Семен визначає інформаційно-психологічну війну як війну нового типу, у якій використовується канал безпосереднього впливу на суспільну свідомість, на душі людей [37, с.24]. Завдання у тому, щоб змусити маси діяти у потрібному напрямі навіть проти

своїх інтересів, в країні противника розколоти людей, змусити їх стати один проти одного.

У числі визначень терміну «інформаційне протиборство» та «інформаційна війна» є і таке: інформаційне протиборство – одна з форм державного або внутрішньодержавного протиборства у мирний та воєнний час. Включає сукупність взаємозалежних заходів технічного та інформаційно-психологічного характеру з метою інформаційного впливу на державні, громадські організації, збройні структури, комп'ютерні мережі, системи управління, на суспільну та індивідуальну свідомість у потрібному для протилежної сторони напрямку, їх дезінформації та порушення нормального та достовірного функціонування інформаційних процесів, при одночасному захисті свого інформаційного середовища від впливу протистояння. Організовується і ведеться також в операціях та бойових діях різного масштабу [40, с.11].

Сьогодні мережеві війни перетворилися на реальність нашого життя. Хочеться зазначити, що розмах інформаційних кампаній у мережі часом анітрохи не менший за масштабом інформаційної боротьби у ЗМІ. Часто, тому що в мережі більша оперативність, ніж у ЗМІ. Загальновідомо, що для багатьох Інтернет вже давно став єдиним способом отримання та розповсюдження інформації, у зв'язку з цим організатори будь-якої інформаційної війни обов'язково використовують такий потужний інструмент, як інтернет для досягнення своїх цілей.

Обмін думками в коментарях до блогів та сайтів відіграє дуже важливу роль при формуванні стрічок новин на сайтах. Інтернет відкриває великі можливості для інтерактивності інформації. Для цього використовують все частіше відеоряди.

До базових характеристик стратегічної інформаційної війни відносять [42, с.25]:

- відносно низькі витрати: порівняно з технологіями традиційного озброєння, розвиток інформаційних технологій потребує джерел фінансування або спонсорування з боку держави;

- розмиті традиційні кордони: традиційні розмежування – громадські інтереси vs приватні інтереси, войовничий vs злочинний, як і історично визначені кордони між державами – виявляються несуттєвими через зростання взаємодії лише на рівні інформаційних інфраструктур;
- посилена роль управління актами сприйняття: нові інформаційні технології здатні помітно збільшити міць стратегій обману, маніпулювання образами, таким чином «знешкодити» спроби держави, проти якої спрямована інформаційна війна, заручитися внутрішньою та зовнішньою підтримкою з метою реалізації ініціатив, пов'язаних із власною інформаційною;
- першочерговий виклик розвідувальним службам: недостатнє усвідомлення стратегічної важливості інформаційної війни, потенційної можливості вразливості стати мішенню у цій війні, знижує ефективність діяльності розвідувальних служб, застосування ними методів збирання та аналізу даних;
- актуалізується гостра необхідність розвитку передових методів аналізу емпіричних матеріалів, сфокусованого на поточних потребах стратегічної інформаційної війни;
- проблеми, пов'язані з оцінкою потенційних інформаційних атак з боку ворога: в даний час відсутня будь-яка система тактичного попередження, яка могла б ефективно розмежовувати атаки, пов'язані зі стратегічною інформаційною війною, та інші види діяльності в кіберпросторі;
- труднощі, пов'язані з формуванням і підтримкою коаліцій: учасники коаліційних спільнот наражаються на зовнішні інформаційні атаки, виявляються потенційно вразливими в цьому плані, що дає противнику невідповідну стратегічну перевагу.

1.2. Історичні засади наукових досліджень в галузі інформаційної війни

Перші прояви інформаційної війни, пов'язані з маніпулюванням знаннями, були вже століття тому, але стала вельми поширеною інформаційна війна у другій половині XX століття. Це зумовлено, по-перше, неможливістю

глобальних збройних конфліктів, що можуть знищити планету; по-друге, зміною сутності інформації, яка нині перетворилася на головний продукт постіндустріального суспільства та на нову наступальну зброю.

У зв'язку з цим у другій половині XX століття починають з'являтися результати наукових досліджень із цієї проблематики. Основними суб'єктами інформаційної війни у цей період були наддержави – СРСР та США. Відповідно і основні розробки з цієї тематики ведуться саме в цих країнах. Теоретичні дослідження приносять свої результати. США випробовує методи інформаційної війни під час війни у В'єтнамі, Афганістані [11].

«Холодна війна» закінчується поразкою СРСР, яку неможливо було досягти шляхом військової агресії без загрози тотального знищення людства. Інші країни Західної Європи та Азії, маючи наочний приклад інформаційної війни, розробляють власні концепції інформаційного протиборства. Особливо в цьому досягнув успіху Китай, якому представилася можливість випробувати істинність своїх теоретичних побудов на практиці в ході інформаційного конфлікту з США у фінансовій сфері.

Внесок американської концепції в теорію ведення інформаційної війни полягає в тому, що тут було вироблено і вперше на нормативному рівні закріплено поняття інформаційна війна, яке в багатьох випадках використовується теоретиками в інших країнах, що свідчить про його універсальність. Китайські вчені також ставляться до розуміння інформаційної війни досить прозаїчно і їхні погляди багато в чому ґрунтуються на практиці інформаційних конфліктів останніх десятиліть.

Однак вони прагнуть з найбільшим ефектом використовувати таку властивість, як асиметрію. Це дозволяє Китаю знизити витрати на закупівлю озброєнь за збереження геополітичного статусу. Концепції вітчизняних теоретиків інформаційних війн, з погляду, вищого рівня і дозволяють оцінити інформаційні конфлікти комплексно. Крім того, така позиція дозволяє виробити ефективні заходи щодо дотримання балансу сил у глобальному інформаційному просторі [11].

Виникнення інформаційного суспільства було передбачене ще на початку 50-х рр. XX ст. основоположником кібернетики Н. Вінером, який стверджував, що в майбутньому розвитку обміну інформацією між людиною і машиною, між машиною і людиною, і між машиною і машиною судилося відіграти зростаючу роль. Була висунута ідея про другу промислову революцію.

Значний внесок у дослідження проблеми сутності інформації вніс американський вчений К. Шеннон. Його підхід до інформації як до всього, що може бути передано по каналах зв'язку від джерела до одержувача (при цьому смисловий зміст інформації, її ціннісні характеристики практично не враховувалися), в подальшому вплинув на формування терміну «інформаційне суспільство» і його інтерпретацію [20, с.57].

Основоположником постіндустріалізму є американський соціолог Д. Белл. Виступаючи в 1959 році на міжнародному семінарі, присвяченому проблемам науково-технічної та інформаційної революції, він запустив у вжиток поняття «постіндустріальне суспільство». Суттєвою характеристикою суспільства, що трансформується Д. Белл вважав появу інтелектуальної технології, що використовується в прийнятті управлінських рішень. У своїй книзі «Майбутнє постіндустріальне суспільство. Досвід соціального прогнозування» (1973 р.) він передрікає третю в історії розвитку людства технологічну революцію [20, с.58].

Ключову роль в новому суспільстві, згідно Д. Беллу, грають знання та інформація. Саме вони, на думку вченого, є не тільки «агентом трансформації постіндустріального суспільства», але і «стратегічним ресурсом» такого суспільства, стають головним джерелом інновацій і соціального динамізму, а відповідно і багатства. Саме тому, за думку Д. Белла, головним соціальним інститутом в постіндустріальному суспільстві стануть університети, а точніше – «мультиверситети» – гігантські агломерації академічних університетів і наукових установ.

У новій цивілізації, на думку Д. Белла, професійні фахівці і техніки будуть переважати серед зайнятих працівників. Одним з ключових критеріїв «інформаційного суспільства» Д. Белл вважає економічне і політичне

керівництво, засноване на теоретичному аналізі і плануванні як в масштабах держави, так і в окремих випадках.

На межі 80-х років стало очевидно, що інформаційно-комунікаційні технології на розвиток наших суспільств набагато більш глибокий вплив, ніж можна було собі уявити. Починаючи з цього часу Д. Белл стає прихильником концепції інформаційного суспільства, яку розуміє як своєрідний новий етап в розвитку теорії постіндустріального суспільства [23, с.48].

Французький соціолог А. Турен відмінними рисами нової цивілізації (її він називає «програмованим суспільством») вважає зміни у виробничій сфері та організації відносин влади і управління. Якщо в аграрному суспільстві основним типом діяльності була торгівля, в індустріальну епоху –виробництво, то в постіндустріальну – комунікація. У постіндустріальному суспільстві центри прийняття рішень складають самоорганізовані і самозмінні системи без центрального пункту [23, с.49].

На відміну від індустріального суспільства, де основним конфліктом є класове протистояння робочих і «босів», в «програмному суспільстві» головний соціальний конфлікт пролягає між механізмом виробництва і управління і самим споживачем. Інновації та інвестиції в науку і техніку стають основою виробництва. Зростання автономії і самоврядування як індивідів, так і більших соціальних структур є наслідком зростання здатності використовувати складні системи інформації і комунікацій і збільшення мобільності населення.

Конвергенція практично одночасно зароджених ідеологій – постіндустріалізму та інформаційного суспільства – відбувається в 70-х рр. XX століття. Надалі терміни «постіндустріальне суспільство» і «інформаційне суспільство» стали використовуватися як синоніми. У науковій літературі термін «інформаційне суспільство» з’явилося завдяки роботам японських і американських авторів К. Катоямі, Т. Умесао, Ю. Хаяші, Ф. Махлуп і ін. Загальновизнано вважається, що введення в науковий обіг терміна «інформаційне суспільство» належить Ю. Хаяші, професору Токійського технологічного інституту, а також ряду японських організацій.

Субстратами інформаційного суспільства є значення та інформація [26, с.36]. «Символічним світом» пропонують інтерпретувати субстрат інформаційного суспільства. Субстанцією суспільства стає інформація, а не вартість (як в індустріальній цивілізації, заснованої на капіталістичній економічній системі), а субстратом – символічний світ як непредметні (на противагу предметному субстрату товарного світу речей індустріальної цивілізації). У тому, що в якості основного ресурсу економіки виступає сьогодні наукове знання і інформація і володіння, в першу чергу, ними, а не традиційними товарами і капіталом, визначає суспільну значимість, економічну і політичну міць, солідарні багато сучасних дослідників в сфері інформаційного суспільства.

Суттєвою характеристикою постіндустріального суспільства Д. Белл вважав появу інтелектуальної технології, що використовується в прийнятті управлінських рішень. Інтелектуальна технологія, у викладі Д. Белла, припускає замість інтуїтивних суджень використання алгоритмів як правил вирішення проблем, які можуть бути реалізовані в автоматичній машині, комп'ютерній програмі або наборі інструкцій, заснованих на математичних формулах. Будь-яке сучасне суспільство живе за рахунок інновацій і соціального контролю за змінами. Воно намагається передбачити майбутнє і здійснювати планування. Саме зміна в свідомості природи інновацій робить вирішальним теоретичне знання.

На думку Д. Белла, постіндустріальне суспільство виникає, в першу чергу, завдяки змінам у соціальній структурі, яка включає економіку, систему стратифікації, сферу зайнятості. Розвиток нових технологій поступово призведе до того, що політичні рішення будуть набувати все більш технічний характер, а діяльність нової еліти буде ґрунтуватися на кваліфікації, професіоналізмі, майстерності завдяки утворенням, що знизить значення таких параметрів, як володіння власністю, політичні позиції, ідеологічні орієнтації, що досягаються за підтримки партій і груп [23, с.49].

Інший відомий філософ М. Кастельс, в своєму фундаментальному дослідженні «Інформаційна ера: економіка, суспільство і культура» нове суспільство назвав «мережевим», інформаційна ера розглядається ним як епоха

глобалізації. При цьому мережеві структури стають одночасно і засобом, і результатом глобалізації суспільства, що зароджується «інформаційне суспільство» будується таким чином, що збір, аналіз і передача необхідної інформації стали «фундаментальними джерелами продуктивності і влади». Про інформаційне суспільство сьогодні пишуть економісти, психологи, політологи, інформаційні фахівці [23, с.50].

Незважаючи на те, що комплексно ідея нерозривності забезпечення розвитку інформаційного простору та інформаційної безпеки сучасної України поки ще не знайшла своєї всебічної розробки, окремі аспекти теми дослідження знайшли своє відображення в працях вітчизняних і зарубіжних дослідників. Умовно, наявний по темі дослідницький матеріал можна представити у вигляді трьох груп наукових робіт.

До першої групи відносяться праці, автори яких розглядають проблеми формування і розвитку інформаційного простору, інформаційного суспільства та інформаційної політики держави. Серед них, представляється необхідним виділити таких авторів, як Арістова І., Аркуша Л., Бакуменко В., Гавловський В., Гуцалюк М., Калюжний Р., Цимбалюк В. та ін.

У працях зазначених дослідників розглянуті різні аспекти впливу глобального інформаційного простору на еволюцію всіх сфер життєдіяльності суспільства і держави, дається характеристика структурного змісту глобального і національних інформаційних просторів, аналізуються питання формування та реалізації державної інформаційної політики. Разом з цим, в даних працях слабо проглядається зв’язок проблем розвитку інформаційного простору та забезпечення інформаційної безпеки особи, суспільства і держави.

Другу групу робіт, складають дослідження, присвячені розробці питань, пов’язаних із забезпеченням національної безпеки України. Ці праці мають пряме відношення до розроблюваної теми дослідження, оскільки в них міститься загальна методологія дослідження проблем забезпечення національної безпеки України. Ця методологія цілком інструментальна також для дослідження питань розвитку інформаційного простору та забезпечення інформаційної безпеки України.

Третя група робіт включає дослідження в галузі забезпечення інформаційної безпеки України і роботи, в яких розробляються загальні питання інформаційної боротьби. У числі авторів даних робіт необхідно виділити таких, як Гавловський В., Голубєв В., Желіховський В., Ліпкан В., Максименко Ю., Олійник О., Соснін О., Цимбалюк В. та ін. [11].

Роботи, що становлять розглянуту групу праць, присвячені аналізу загроз інформаційній безпеці України, дослідженню технологій інформаційної війни та інформаційної боротьби, розробці підходів до вирішення завдань забезпечення інформаційної безпеки України. Ці дослідження мають істотне значення для формування уявлень про завдання державної інформаційної політики, спрямованої на розвиток інформаційного простору і забезпечення інформаційної безпеки України. Однак в них явно недостатньо уваги приділяється формуванню світоглядних підстав вирішення цих завдань.

1.3. Становлення проблеми інформаційної війни у XX ст.

На сьогоднішній день можна спостерігати інтенсивний розвиток засобів зв'язку, які мають всеосяжний характер і демонструють абсолютно нові результати, які раніше були недосяжними. Стрімко збільшилися масштаби інформаційних потоків, які звичайні обиватели отримують поза веденням державної влади. Інформація вийшла на якісно новий рівень у тому сенсі, що поєднує в собі як деструктивний, так і творчий вплив, але вже більшою мірою, ніж це було в минулому.

З часом змінюється сенс інформації, інтенсивно зростає її вплив. Змінилися контексти її використання (наприклад, приватне стає загальним «надбанням»). Водночас у вирішенні політичних питань посилилося значення публічної інформації і, як наслідок, підвищилася регульованість та публічність сфери дії політики. Зростання значення інформації є історичним фактом, що базується на ідеях інформаційного суспільства. Дедалі частіше саме інформаційне протистояння є продовженням політики держави.

Так, існує думка, що інформаційні війни прийшли до нас лише у XX ст. разом із настанням технологічної ери. Проте проблеми інформаційних війн та операцій у політичному дискурсі існують уже тривалий час. Один із перших випадків застосування інформаційно-психологічних методів впливу належить ще до V ст. до н. е., коли перський цар Ксеркс I, намагаючись залякати еллінів, поширював чутки про гігантські розміри своєї армії.

Відповідно до «законів Ману», війська супротивника слід заохочувати до заколоту, вносячи розкол до лав тих, хто до цього схильний. Цим принципом користувалися багато стратегів античності, середньовіччя та нового часу [17, с. 182]. У XX ст. інформаційні війни стали частиною воєнної політики держав. У Першу світову війну у Великій Британії було створено так зване Бюро військової пропаганди (1914 р.), яке пізніше було перейменовано в Управління військової інформації.

У Франції при другому відділі генерального штабу міністерства оборони створили відділ Служби військової пропаганди (1915 р.). Обидві установи займалися поширенням пропаганди серед військових та цивільних осіб інших держав. У 1917 р. США була створена психологічна секція при розвідслужбі штабу експедиційних військ. Основними засобами ведення інформаційної війни на той час були листівки, брошури, газети; як технічні засоби російською армією використовувалися гучномовці [28, с. 20].

Відразу після Першої світової війни зріс інтерес до цього явища. Багато держав світу стали публікувати роботи з психологічним методам ведення війни. Англійський дослідник психологічної війни П. Г. Уорбертон писав: «У сучасний час основним завданням у війні є не знищення збройних сил противника, як це було раніше, а підрив морального стану населення ворожої країни загалом до такого рівня, щоб він змусив свій уряд піти на компроміс чи капітуляцію. Збройне зіткнення армій – це лише один із засобів для досягнення цієї мети» [35, с. 281].

Таким чином, теорія інформаційної та психологічної війни почала розроблятися вже під час і після Першої світової війни. До Другої світової війни існувала активна пропаганда режимів: у Німеччині в 1933-1941 рр. – нацистська

пропаганда, у СРСР – комуністична та антикапіталістична, у США та Великобританії – капіталістична та антикомуністична. Під час війни акценти швидко зрушили у бік антинацистської пропаганди [28, с. 22].

Під час Другої світової війни вже функціонували органи державної пропаганди. Це були Бюро військово-політичної пропаганди і 7-е управління Політичного управління РККА. У нацистській Німеччині працювали Міністерство народної освіти та пропаганди та Верховне головнокомандування Вермахту. Свої органи пропаганди існували у США та Великій Британії. У ході війни методи психологічного впливу, що застосовуються, часто мали високу ефективність. Незважаючи на розвиток інформаційних технологій на той час, як і раніше, пропаганда найчастіше здійснювалася у формі листівок та плакатів. Активно застосовувалося радіомовлення мовою противника.

У сучасну епоху політика є невід'ємним компонентом динамічності процесів у суспільстві, які виражаються в мінливій обстановці, в неясності, непередбачуваності та парадоксальності як суспільних процесів, так і їх результату. У свою чергу, глобалізація, широкомасштабна комп'ютеризація, удосконалення сучасних інформаційних технологій послужили джерелом процвітання інформаційного протиборства в політиці.

Визначальним чинником захоплення та збереження влади стає контроль за потоками інформації, результатом чого стала поява терміна «інформаційна війна». Нові інформаційні системи та технології – електронні ЗМІ, Інтернет, мобільний зв'язок, глобальна навігація – ще більше збільшили можливості інформаційного впливу під час війни. Це дозволяє таким індустріальним державам, як США та Японія, значно посилити свою політичну, економічну та військову перевагу за рахунок лідерства у сфері інформатизації, а також встановити глобальний інформаційний контроль над іншими країнами світу, тим самим встановлюючи свої правила у реальному світі.

Цей факт непокоїть менш розвинені країни, адже під загрозою опиняється їхня самобутність, незалежність і суверенність. До таких країн належить і Україна. У вік інформаційних війн, коли основним завданням будь-якого агресора є не фізичне знищення супротивника, а його перепрограмування, саме

ЗМІ виступають як зброя масової поразки. Адже саме створення конкретного матеріалу ЗМІ чимось нагадує проектування засобу масового ураження. Кількість уламків від кожного слова, від кожного сюжету намагаються зробити якнайбільше, а радіус поразки – якнайширше [41, с.65].

Це означає, що дія цих повідомлень має на меті зачепити якомога більшу кількість елементів та зв'язків між ними в інформаційній системі, яка перебуває під впливом ЗМІ. Але на шляху повідомлень, що розсилаються у всіх напрямках, існує значна перешкода: сприйняття повідомлення вимагає спільних понять та категорій, що містяться в ньому, та одержувача цього повідомлення. В іншому випадку повідомлення не дійде до свого адресата, тому завданням персоналу ЗМІ є продукування таких повідомлень, які якнайширше охоплюють рівень своєї цільової аудиторії.

Історія інформаційних війн включає війни, які завершувалися, як правило, або революцією, або переворотом: «холодна війна» між СРСР та США; «оксамитові революції» у країнах Східної Європи наприкінці 80-х років; «революція троянд» у Грузії (2003 р.); Помаранчева революція в Україні (2004 р.); спроба «джинсової» революції у Білорусі (2006 р.); російсько-грузинська війна (2008).

Вплив ЗМІ у суспільстві швидко помітили в Росії. Крім використання різних технологій пропаганди на територіях, охоплених війною, військові кола в Росії стали розробляти стратегії маніпулювання свідомістю через пресу, використовуючи при цьому досить грубі методи: підкуп, шантаж, погрози, використання різних нематеріальних стимулів і т. д. [41]. У 2008 р. під час агресії Росії в Південній Осетії була спроба спотворити ситуацію, звинувативши в масованих бомбардуваннях Грузії .

Спосіб підтримки цієї керованої війни стало створення «образу жертви»: у російських ЗМІ просувалася ідея, що велика Росія спасала Грузію. Основними інформаційними агентствами, що піддавалися критиці та звинуваченням з боку російських політиків, стали CNN і BBC, які висвітлювали ситуацію в Грузії так, як її висвітлювали в самій Грузії, тобто правдиво: Росія виставлялася агресором, а про події в Цхінвалі згадувалися частково.

США активно підключилися до критики Росії, не беручи участь у самому конфлікті. Слід зазначити, що метою неправдивої інформації, що подавалася російськими ЗМІ, була дискредитація політики НАТО у Закавказзі. Кульмінацією інформаційного протистояння стали події, що супроводжували протести на Сході України, кримську кризу та війну на Сході України, в Донбасі 2014 р., що триває й досі.

З початку протистояння західні політики, представники США та ЄС, міжнародні організації (НАТО, ООН, ПАРЄ) та ЗМІ активно засуджували критику Росії, звинувачуючи безпосередньо Володимира Путіна в тому, що він втручається у внутрішні справи України. До перших спроб інформаційного протистояння в Україні слід віднести події «Помаранчевої революції» 2004 року, політичної революції, на думку більшості політологів.

З новою силою інформаційне протистояння розігралося на території України, починаючи з 2013 р.. У цей період звичайною практикою стає агресивне нав'язування «правди» російськими ЗМІ, створення «образу жертви», якою виставляється російськомовне населення. В українських ЗМІ навпаки розповсюджуються факти [43, с. 69].

У свою чергу, у російських ЗМІ підкреслюється «нацистський» та «олігархічний» характер української влади, свавілля ультраправих сил, перекручування історії та актуальних подій в Україні та світі. Характерними знаряддями ведення інформаційної війни у ЗМІ стали «фейки».

Висновки до розділу 1

Наслідки інформаційних війн настільки ж глобальні та довготривалі, що й результати збройних війн. Завдяки Інтернету та сучасним методам політтехнологій за співвідношенням ціна-ефективність на кілька порядків перевершує всі інші. Насамперед це зумовлено тим, що з усіх існуючих засобів масової комунікації Інтернет надає широкі можливості для ведення інформаційних війн.

Інформаційна війна являє собою сферу дієвих інтересів розробників оборонних стратегій і політиків, що стрімко розвивається і все ж таки насилу піддається точному визначенню. Джерелом зростаючих інтересів до цієї сфери можна розглядати так звану інформаційну революцію, яка базується на прискореній еволюції кіберпростору, мікрокомп'ютерів та пов'язаних з ними технологій.

У мілітарних цілях кожна з протиборчих сторін прагне задіяти в інформаційній війні глобальну інформаційну інфраструктуру та відповідні передові технології. Коаліції, залучені у взаємну інформаційну війну, мають значні ресурси, включаючи складні системи управління та інфраструктури, що здійснюють жорсткий контроль над грошовими потоками, повітряними повідомленнями, електроенергією, природними ресурсами (насамперед газом та нафтою) та іншими інформаційно залежними об'єктами. З концептуальної точки зору, у випадку, якщо противник робить спробу зруйнувати ці системи та інфраструктури, використовуючи технології інформаційної війни, то інформаційна війна у відповідь для враженої сторони набуває стратегічного характеру.

Інформаційне суспільство – це нове поняття, нова суспільно-політико-економічна категорія, що характеризує новий щабель у розвитку людської цивілізації. В інформаційному суспільстві змінився спосіб життя людей, стиль роботи, спілкування один з одним, забезпечено підвищення продуктивності праці і тим самим зростання добробуту людей. Структура інформаційного суспільства складніша, ніж структура попередніх товариств, оскільки основна

ланка цього суспільства – комп’ютерні комунікації не є самостійною виробничою одиницею, а є продуктом специфічної індустрії.

РОЗДІЛ 2
СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ ВІЙНИ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

2.1. Причини посилення інформаційних війн на сучасному етапі розвитку суспільства

Незважаючи на певні позитивні зміни військово-політичної обстановки в кінці XX – початку XXI століття, що знизили загрозу виникнення широкомасштабної звичайної та ядерної війни, в основі політики щодо забезпечення національної безпеки та власних інтересів лежить принцип активного задіяння всіх можливостей держави: дипломатичних, інформаційних, військових і економічних. В умовах широкомасштабного впровадження в практику військового будівництва новітніх досягнень в області комунікації та інформатизації військові фахівці звертають особливу увагу на підвищення ролі інформаційного простору (далі – ІП) та необхідності його інтенсивного і масштабного використання при вирішенні міждержавних протиріч і досягнення своїх зовнішньополітичних цілей [8, с.178].

Військові сили завжди будуть відігравати провідну роль в забезпеченні національної безпеки країни. Для забезпечення їх дій в інформаційному просторі провідними фахівцями була розроблена концепція «інформаційних операцій» (далі – ІО). Офіційні документи, присвячені питанням інформаційного протиборства, і в першу чергу повчання, а також виступи і заяви офіційних осіб на цю тему дозволяють зробити висновок про те, що під інформаційними операціями країни розуміють сукупність узгоджених за метою, завданнями, місцем і часом заходів щодо застосування інформаційних можливостей (далі – ІМ) військ (сил), що проводяться одночасно і послідовно, за єдиним задумом і планом в ході військової операції для вирішення завдань з надання впливу або створення перешкод процесу підготовки, прийняття та реалізації військового вирішення ймовірним, потенційним або діючим противником і одночасному

захисті своїх військ (сил) від аналогічних дій. Крім того, в якості об'єкта впливу можуть виступати керівництво і населення інших держав, країн-партнерів і учасників коаліцій [8, с.179].

За характером вирішуваних завдань і виконуваних дій заходи ІМ припускають:

1. Залучення можливостей стратегічної комунікації – комплекс заходів, що проводяться військовими силами, за узгодженим інформуванням іноземних аудиторій про діяльність і погляди держави з різних питань, а також спрямованих на просування та відстоювання національних інтересів у світі, схиляння іншої сторони на свою сторону або спонукання її діяти у вигідному для держави напрямку. Дані заходи організовуються з урахуванням і на підтримку програми публічної дипломатії, яка здійснюється державним департаментом. Особливу увагу питанням стратегічної комунікації останнім часом приділяють при підготовці командирів і начальників усіх рівнів.

2. Участь фахівців у засіданнях міжвідомчої групи – дорадчого органу, який створюється в рамках зонального об'єднаного командування з метою забезпечення всебічної ситуативної обізнаності командувача в зоні відповідальності. До складу цієї групи крім військовослужбовців входять представники державних органів в регіоні, регіональних організацій, уряду. Питання інформаційних операцій не є основними в роботі цієї групи, проте участь фахівців ІО грає важливу роль в синхронізації їх дій і програм з діяльністю перерахованих вище партнерів [13].

3. Заходи щодо забезпечення зв'язку з громадськістю – це узгоджені заходи з підготовки та поширення інформації про діяльність і погляди держави з тих чи інших питань, спрямовані на створення сприятливого сприйняття дій керівництва держави громадянами.

4. Військово-цивільні операції – заходи щодо встановлення, підтримання, дії або використання в своїх інтересах відносин військових з урядовими та неурядовими громадськими організаціями та владою, а також з цивільним населенням на території союзників, партнерів, нейтральних країн і супротивників, з метою співпраці і досягнення оперативних цілей. Такі операції

можуть включати в себе заходи, що організовуються військовими, які в звичайних умовах є обов'язком місцевої влади. Вони можуть мати місце до або під час військових дій, а також після їх закінчення. Військово-цивільні операції можуть бути проведені спеціально створеними підрозділами по роботі з цивільним населенням, бойовими формуваннями, об'єднаними оперативними формуваннями або комбінацією таких сил [12, с.461].

5. Операції в кіберпросторі представляють собою сукупність узгоджених і взаємопов'язаних за цілями, завданнями, місцем, часом, об'єктом і змістом одночасних або послідовних заходів, що проводяться за єдиним задумом і планом, по впливу на об'єкти противника в кіберпросторі [66, с.107].

Кіберпростір – це «глобальна сфера» (домен) всередині інформаційного простору, що представляє собою взаємопов'язану сукупність інфраструктур і інформаційних технологій, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані процесори і контролери. Про важливість кіберпростору і ведення бойових дій в ньому говорить те, що він став рівноправним з традиційними наземним, морським, повітряним і космічним просторами. Крім того, американське військово-політичне керівництво прирівнює загрози, які виходять із кіберпростору, до загроз поширення зброї масового ураження і тероризму [21, с.189].

6. Заходи щодо забезпечення інформаційної стійкості – це дії щодо захисту та недоторканності інформації та інформаційних систем з боку противника шляхом забезпечення їх функціональності, інтегрованості, дотримання встановлених правил авторизованого доступу до них, секретності, а також відновлення їх працездатності.

7. Операції в космічному просторі. В ході ІС активно використовуються можливості сил і засобів ведення операцій в космічному просторі, зокрема космічних систем розвідки, зв'язку, навігації та метеорологічних систем.

8. Операції з інформаційного забезпечення бойових дій, іменовані до середини 2010 року психологічними операціями (далі – ПСО), незважаючи на зміну назви, не поміняли своєї суті: вони являють собою сплановані заходи щодо передачі спеціально підготовленої інформації іноземним аудиторіям з метою

здійснення впливу на їх емоції, мотиви, сприйняття того, що відбувається і в кінцевому підсумку спрямовані на зміну в вигідному для себе напрямку поведінки іноземних урядів, організацій, груп та окремі аспекти їх особистостей.

9. Розвідувальне забезпечення – комплекс заходів, що здійснюються системою розвідки (розвідувальними органами, силами і засобами) в інтересах забезпечення ІС з метою збору, обробки та аналізу розвідданих з подальшим їх розподілом для вирішення певних бойових і інших завдань відповідним формуванням збройних сил на конкретному театрі військових дій.

10. Заходи військової дезінформації – це дії, які мають на меті навмисного введення в оману осіб противника, які приймають рішення про можливості, наміри і дії як своїх, так і дружніх військ, що змушує його робити помилки на всіх етапах ведення бойових дій.

11. Забезпечення безпеки (скритності) дій військ (сил) – комплекс заходів, спрямованих на розпізнавання і захист важливої (критичної) несекретної інформації (з подальшим її аналізом) про діяльність своїх ЗС, характерною для ведення бойових дій, а також іншої діяльності ВС.

12. Спеціальні технічні операції. У відкритих джерелах немає чіткого визначення цього терміну. Наявні дані дають право вважати, що такі дії є комп'ютерні мережеві операції, які частково перекривають область кібероперацій. Комп'ютерні мережеві операції, в свою чергу, поділяються на такі види:

- атака комп'ютерних мереж противника;
- захист комп'ютерних мереж;
- вилучення інформації з комп'ютерних мереж супротивника і використання її в своїх інтересах (експлуатація комп'ютерних мереж) [29, с.42].

13. Операції військ (сил) в електромагнітному спектрі. Такі операції складаються із заходів радіоелектронної війни (РЕВ) (РЕ-атаки; РЕ-захисту; забезпечення РЕВ) і управління ЕМ-спектром в операціях об'єднаних сил, які забезпечують функціонування систем, що залежать від електромагнітного спектра.

14. Залучення до встановлення зв'язку і домовленостей з цільової аудиторією. Даний вид заходів передбачає активне залучення командного складу збройних сил до спілкування з лідерами іноземних аудиторій з метою привертання їх на свою сторону і направлення їх діяльності у вигідному для країни руслі. Такі заходи можуть бути проведені в ході різних операцій, наприклад, протиповстанських, по підтримці стабільності, по евакуації в небойових умовах і гуманітарних операціях.

Очікується подальше становлення інтернет-технології і подальший розвиток до Web 3.0 (високоякісні контент і сервіси Інтернету ще більш високого рівня). Очевидно, що IT на стадії свого остаточного формування буде характеризуватися повсюдною доступністю і широким використанням джерел з надання і розповсюдження файлів мультимедіа (наприклад, Youtube), мікроблогів (Twitter), соціальних мереж (Facebook) в тих районах, де вони ще не так широко представлені. Все це допоможе згуртувати однаково мислячих людей локально і / або регіонально.

Експерти в США відзначають також формування «великих масивів даних» на базі мобільних пристроїв зв'язку і телекомунікації. Більше 70 % населення Землі користуються мобільними засобами зв'язку, що формують так звані великі масиви даних (понад 2,5 трлн. байт інформації в добу). Здатність органів ІВ збирати і обробляти значні обсяги даних стане основою для розуміння потреб і причин дій окремих користувачів і груп осіб [35, с.40].

Що стосується демографічного чинника, то, наприклад, за прогнозами експертів, в майбутньому середній вік європейців або жителів Японії складе близько 45 років; середній вік в Китаї (і більшої частини жителів Південної Азії) – 35 років, на Африканському континенті – 25 років. Оскільки в останні роки в окремих країнах, що розвиваються велика частина молоді стала свідком значних соціальних змін [36, с.40].

В умовах скорочення військового бюджету, вдосконалення технічних засобів, що використовуються для отримання, обробки, зберігання та передачі інформації, а також визнаючи інформацію стратегічним ресурсом, Пентагон

продовжує удосконалювати ІВ як інструмент досягнення цілей військових операцій.

2.2. Вплив інформаційних технологій на трансформацію інформаційної зброї

У світі інформаційні технології займають одне з провідних місць у всіх сферах життя суспільства. Процес інформатизації набуває дедалі ширшого масштабу і охоплює як внутрішню, так і зовнішню політику країн. Особливу роль інформаційні технології грають у сфері інформаційної безпеки. Прагнення створення єдиного інформаційного простору забезпечує можливість розробки та застосування інформаційної зброї. Забезпечення національної безпеки безпосередньо залежить від володіння інформаційною зброєю, ступеня її ефективності, методів використання та засобів захисту.

На сьогоднішній день існує безліч понять інформаційної зброї і не можна говорити про правильність чи неправильність кожного визначення. Здебільшого, всі вони базуються на перерахунку суб'єктів та об'єктів інформаційного впливу. Але перш ніж говорити про інформаційну зброю, необхідно розібратися в понятті зброї як такої.

Зброя це пристрої та засоби, що застосовуються у збройній боротьбі для поразки та знищення противника [39, с.36]. Переходячи до визначення «інформаційне протиборство», ми звернулися до багатьох джерел, оскільки не існує одного певного тлумачення. Так, згідно з словником надзвичайних ситуацій, інформаційна зброя це:

1) спеціальні засоби, технології та інформація, що дозволяють здійснити силовий вплив на інформаційний простір суспільства та призвести до значної шкоди політичним, оборонним, економічним, екологічним та ін. життєво важливим інтересам держави;

2) сукупність способів та засобів інформаційного впливу на техніку та людей з метою вирішення завдань чинної сторони. Відповідно до видів інформаційної боротьби інформаційна зброя поділяється на два основні види:

інформаційно-технічну та інформаційно-психологічну. Головними об'єктами інформаційної зброї першого виду є техніка, другого – люди;

3) комплекс технічних та інших засобів та технологій, призначених для:

- встановлення контролю над інформаційними ресурсами потенційного противника;
- втручання у роботу його систем управління та інформаційних мереж, систем зв'язку з метою порушення їх працездатності, аж до повного виведення з ладу, вилучення, спотворення даних, що містяться в них, або спрямованого введення спеціальної інформації;
- поширення вигідної інформації та дезінформації у системі формування громадської думки та прийняття рішень;
- сукупність спеціальних способів та засобів впливу на свідомість та психіку політичного та військового керівництва, особового складу збройних сил, спецслужб та населення держави, що використовуються для досягнення переваги в інформаційному протиборстві [46, с.183].

Для своєї роботи ми використовуватимемо найбільш відповідне тлумачення. Інформаційна зброя – це засоби знищення, перекручування або розкрадання інформаційних масивів, добування з них необхідної інформації після подолання систем захисту, обмеження чи заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем, всього високотехнологічного забезпечення життя суспільства та функціонування держави.

Інформаційна зброя має низку особливостей та відмінностей від інших видів зброї. До них відносяться:

1. Керованість. Інформаційна зброя здійснює вплив на об'єкт у заданий час та у встановлених масштабах.
2. Прихованість. Досить складно визначити момент початку дії та встановити джерело.
3. Універсальність. Можливість ураження різних об'єктів у досить широкому діапазоні.

4. Низька вартість створення та висока ефективність застосування.

5. Доступність. Легке поширення та високий рівень контролю за процесом виконання.

6. Тривалість. Можливість довгострокового застосування інформаційної зброї без втрати ефективності її застосування.

7. Можливість використання у мирний час та раптовість застосування у разі воєнних дій [49, с.45].

Всі ці особливості роблять інформаційну зброю надзвичайно небезпечною. Її досить легко замаскувати, наприклад під засоби захисту програмного забезпечення. Але основна небезпека використання інформаційної зброї при веденні інформаційного протиборства полягає в тому, що з'являється можливість вести наступальні дії під маскою анонімності і навіть без офіційного оголошення війни.

Виділяють 4 основні види інформаційної зброї:

1. Вплив на людську психіку. До цього типу інформаційної зброї відносяться методи, способи та засоби впливу на психічний стан людини з метою зміни чи підриву цього стану:

- усі види засобів масової інформації;
- друкований матеріал, до якого відносяться листівки, плакати, афіші, матеріал і т.д.;
- засоби зв'язку;
- музика, кінофільми, реклама тощо;
- комп'ютерні ігри.

2. Дезінформування систем прийняття рішень. До цього типу відносяться методи на групові та індивідуальні системи прийняття рішень, з метою вибору рішення, вигідного дезінформатору.

- нав'язування інформації;
- спотворення інформації;
- блокування інформації;
- приховування інформації;
- підміна інформації [3].

До основних засобів ведення протиборства зброєю такого типу відносяться засоби інформації, телекомунікаційні системи, засоби зв'язку.

1. Радіоелектронна боротьба:

- Радіоелектронна розвідка (включає перехоплення та аналіз інформації, що надходить через телекомунікаційні системи, дезінформування);
- радіоелектронна протидія (створення перешкод під час передачі інформації);
- придушення елементів телекомунікаційних систем, радіомовлення, телевізійних сигналів, ліній зв'язку тощо (використання заглушок)

2. Вплив на програмно-технічне оснащення телекомунікаційних систем та автоматизованих інформаційних систем. Цей тип інформаційної зброї включає засоби та методи несанкціонованого доступу до ТКС та АІС.

- розкрадання, викривлення або знищення інформації;
- обмеження або заборона доступу до комп'ютерних систем;
- дезорієнтація роботи комп'ютерних систем;
- блокування або виведення з ладу комп'ютерних систем [9].

Принципова відмінність інформаційного протистояння від звичайної війни полягає в тому, що інформаційне протиборство певною мірою регулюється законодавством. Єдина мета інформаційної зброї – завдання інформаційних систем супротивника найбільшої шкоди. Досягнення цієї мети противники реалізують практично певні завдання. Інформаційна зброя відрізняється від звичайного озброєння керованістю, прихованістю, універсальністю, економічністю та тривалістю.

Крім того, різні види інформаційної зброї впливають на людську психіку, управлінські та радіоелектронні системи, а також на програмно-технічне оснащення, використовуючи при цьому найбільш відповідні методи впливу. Що стосується сфери законодавства з проблеми, то можна зробити висновок, що у зв'язку із встановленням інформаційного простору та розвитком інформаційних технологій, структура українського законодавства включає в себе малу кількість нормативно-правових актів. З розвитком даного сектора база офіційних

документів буде поповнюватися, що допоможе покращити контроль за процесом регулювання проведення інформаційного протиборства.

Цілісність сучасного світу забезпечується в основному за рахунок інтенсивного інформаційного обміну. Інформаційна зброя здатна призупинити глобальні інформаційні потоки, що може призвести до глобальної кризи. Для того, щоб розібратися в питанні застосування інформаційної зброї, необхідно виявити сферу її застосування. Найбільш широкодоступною областю є світові інформаційні мережі.

Світові інформаційні мережі – це сукупність електронно-обчислювальних машин, що пов'язані між собою каналами телекомунікації. Такі інформаційні мережі дозволяють користувачам обмінюватися інформацією, спільно використовувати необхідні інформаційні ресурси [18, с.170]. Глобальна інформаційна мережа поділяється на загальнодоступну та спеціалізовану. Загальнодоступна мережа (Internet, електронна пошта) знаходиться у вільному та рівному доступі для звичайних користувачів. Спеціалізовані мережі є корпоративними або відомчими, тобто призначені для обмеженого кола осіб.

Перша комутована мережа ARPANET розпочала своє існування у США у 1969 р. Тоді до неї було підключено лише 4 комп'ютери. На сьогоднішній день на Заході існує безліч глобальних мереж. Наприклад, BITNET – мережа, що об'єднує понад 800 колективних учасників, переважно серед університетів, коледжів і наукових центрів. Ця мережа охоплює 35 країн Європи, Азії та Америки.

2.3. Перспективи розвитку стратегій ведення інформаційних війн в соціальних мережах

Прийнято вважати, що вперше поняття «соціальна мережа» було введено в 1954 соціологом Джеймсом Барнсом, який представляв соціальну мережу як групу точок, що позначають людей або групи людей і ці точки-лінії, що поєднують, які позначають взаємодію між людьми [24, с.138]. Ця концепція

стала набирати популярності вже після появи в 1969 р. Інтернету, що призвело до виникнення та розвитку сучасних соціальних мереж.

Перша соціальна мережа з використанням комп'ютерної техніки з'явилася 1971 р. і використовувалася військовими для передачі інформації через ARPANET. Через 17 років фінський учений Яркко Ойкарінен винайшов протокол «IRC», який є інтернет-чатом, що ретранслюється і програмне забезпечення для забезпечення його роботи. Після цього стало можливим спілкуватися один з одним у реальному часі, проте справжню популярність соціальні мережі набули пізніше [24, с.139].

У 1995 р. американець Ренді Конрадс створив першу соціальну мережу у сучасному розумінні, яку назвав Classmates.com. Ця соціальна мережа була призначена для тих користувачів, які бажали знайти своїх однокласників чи однокурсників. Нині цією соціальною мережею користуються понад 50 мільйонів.

Найбільш популярними соціальними мережами в Україні на сьогоднішній день є Фейсбук, Твіттер, Інстаграм, Телеграм. Здебільшого зазначені соціальні мережі спочатку були призначені для організації спілкування представників студентської спільноти та випускників вузів, проте надалі стали позиціонуватися як спосіб спілкування людей, що належать до різних соціальних груп та спільнот, дуже часто – як інструмент донесення до суспільства інформації, включаючи рекламу і навіть пропаганди, психологічного впливу на учасників соціальних мереж.

Зворотною стороною стрімкого розвитку соціальних мереж є те, що вони неминуче стають об'єктами та засобами інформаційного управління, а також ареною інформаційного протиборства. Соціальні мережі сьогодні – один із ключових та найефективніших інструментів інформаційного впливу, у тому числі засіб для маніпулювання особистістю, соціальними групами та суспільством загалом. Не дивно, що вони все частіше використовуються як майданчики для ведення інформаційних воєн.

Я. Малик визначає інформаційні війни між двома інформаційними системами як відкриті та приховані цілеспрямовані інформаційні впливи

інформаційних систем одна на одну з метою отримання певного виграшу у матеріальній сфері [25]. Образно, але гранично точно сутність інформаційних війн розкривається за допомогою алегорії, що наводиться ним: «черепаха не знала і вже ніколи не дізнається, що інформаційна війна – це цілеспрямоване навчання ворога тому, як знімати панцир із самого себе».

Інший дослідник Н. Ф. Семен зазначає, що для інформаційних війн характерна спрямованість на зміну поглядів, світогляду населення, підрив суспільної системи противника [37, с. 23]. Під час ведення інформаційних війн об'єктом впливу противників виступає масова та індивідуальна свідомість, а ефективність такого впливу багато в чому залежить від того, наскільки сприйнятливе населення протиборчої сторони до сприйняття інформації, що доноситься.

Безсумнівно, засобами ведення інформаційних війн можуть виступати всі засоби передачі інформації, але найефективнішими інструментами є саме соціальні мережі. Їхньою перевагою перед переважною більшістю засобів масової інформації є інтерактивність. Інтернет-простір перетворює людину на співучасника подій. Соціальні мережі дозволяють висловлювати ставлення людини до того, що відбувається, і надають різні можливості. Лайки і репости не вимагають від мережевої особи великої праці та значних тимчасових витрат, включають її в цю подію та створюють ілюзію причетності.

Потенціал інформаційно-пропагандистського впливу соціальних мереж є надзвичайно високим. Перевірити ще раз інформацію, розміщену в Інтернеті, знайти її первинне джерело і джерела поширення може і бажає лише невеликий відсоток активних Інтернет-користувачів, які бачать у соціальних мережах засіб досягнення конкретних цілей у реальному світі, а не майданчик для вираження власних емоцій.

Більшість учасників соціальних мереж обмежується активністю виключно у віртуальному світі. Для їх позначення в Україні зазвичай використовують поняття «дивані війська» [38]. У деяких публікаціях науковців можна зустріти також термін «слактивісти» (від англ. «slacker» (нероба) і «activism» (активізм), що використовується стосовно даної категорії користувачів Інтернету.

Мережеві слактивісти не можуть відігравати серйозної ролі в організації масових акцій, формуванні громадської думки, здатної впливати на соціально-політичну обстановку та настрої в суспільстві. Ще в 2010 р. соціолог Малкольм Гладуелл стверджував, що справжні соціальні зміни неможливі за допомогою соціальних медіа, так зв'язки в них неміцні та децентралізовані, некеровані, тоді як щоб домогтися реалізації своїх вимог, протестуючим необхідно згуртоване, дисциплінованe добре організоване ядро з центральним управлінням [38].

Проте сучасні реалії свідчать, що це негаразд. Слактивісти стали важливою складовою соціальних хвилювань і протестів, розповсюджуючи інформацію серед широких верств населення про те, що відбуваються насправді або вигадані події. Особливістю слактивістів є те, що зазвичай вони не намагаються перевірити достовірність інформації, яку вони розповсюджують.

Найчастіше вони трансформують дані, що тиражуються, надаючи їм від себе велику достовірність. Так, навесні 2009 р. датський психолог Андерс Колдінг-Йоргенсен, який вивчає поширення ідей в інтернеті, провів науковий експеримент з «Фонтаном лелек», однією з головних визначних пам'яток Копенгагена. Колдінг-Йоргенсен організував у соціальній мережі Facebook групу, яка висловила припущення, що міська влада має намір знищити знаменитий фонтан, що не відповідало дійсності.

Колдінг-Йоргенсен презентував нову групу своїм «друзям» у Facebook і вони протягом кількох годин приєдналися до кампанії. Незабаром приєдналися їхні «друзі» і кампанія проти міської ради стала швидко розширюватися. На піку популярності група щохвилини отримувала у Facebook двох підписників. Коли кількість учасників досягла 27,5 тисяч, Колдінг-Йоргенсен припинив експеримент [38].

У сучасному світі через соціальні мережі регулярно поширюється інформація, що часто не відповідає дійсності і завдає шкоди інтересам особистості, суспільства та держави. Генерує більшість зазначеного контенту нечисленне угруповання активістів, які є ініціаторами поширення інформації (далі – ініціатори). Потім цей контент підхоплюють численні слактивісти. Саме вони критично впливають на інформаційне висвітлення будь-якої події.

Слактивісти значно посилюють інформаційний потік, у той час як без їхньої підтримки подія не отримує належного розвитку та суспільного резонансу.

Іншими словами, пасивна слактивістська периферія настільки ж необхідна для успіху акцій щодо поширення інформації, як і активний центр, що складається з ініціаторів. У процесі ведення інформаційних війн у соціальних мережах дії невеликої групи ініціаторів, підтриманих слактивістами, здатні викликати соціальні хвилювання і завдавати значної матеріальної та репутаційної шкоди державним та приватним організаціям.

З розвитком інформатизації суспільства кількість таких деструктивних інформаційних атак лише зростатиме. Очевидно, що необхідно виробити алгоритм протидії таким атакам. П. Шевчук виділяє такі напрями вищевказаних заходів:

- силові методи: закриття серверів, формування трафіку;
- правова та нормативна практика: кримінальна відповідальність організаторів та учасників віртуальних спільнот;
- Інтернет-цензура;
- моніторинг та аналіз соціальних мереж [47].

При цьому силові та правові методи протидії носять заборонений чи обмежувальний характер, що з урахуванням специфіки інформаційних атак у соціальних мережах не призводить до необхідних результатів. Інтернет-цензура займає важливе місце у протидії інформаційному та психологічному впливу в соціальних мережах, проте як превентивний захід не має потенціалу подальшого розвитку.

Слід погодитися з вищезазначеними дослідниками у тому, що з наведених ними заходів найефективнішими у довгостроковій перспективі є моніторинг та аналіз соціальних мереж. Для їх здійснення необхідне об’єднання фахівців із різних галузей науки і техніки, загальною метою яких буде організація управління та контролю за діяльністю соціальних мереж за допомогою різноманітних методів, а також прогнозування їх розвитку в майбутньому.

Разом з тим, враховуючи швидкість інформатизації суспільства, зростання трафіку переданої та споживаної інформації в мережі Інтернет, потрібна

автоматизація обробки інформаційних потоків, виявлення та аналізу нових спільнот у соціальних мережах з автоматичним розподілом їх учасників на слактивістів та ініціаторів. Як одне з можливих розв'язків завдання забезпечення ефективної інформаційної протидії у соціальних мережах пропонується реалізація такої протидії паралельно за двома напрямками:

- виявлення та встановлення джерела та шляхи розвитку інформаційної атаки, її припинення, у тому числі за допомогою програмно-технічних засобів та інформаційних технологій;
- організація протидії інформаційній атаці та впливу на слактивістів шляхом запуску зворотної інформаційної хвилі (офіційні роз'яснення, спростування, заклики не піддаватися провокаціям та паніці).

Періодично з боку різних державних структур, громадських організацій та політичних діячів вносяться ініціативи, спрямовані на запровадження жорстких обмежувальних заходів у соціальних мережах з метою забезпечення охоронюваних законом інтересів особи, суспільства та держави. Однак спроби встановлення в сучасних умовах адміністративного контролю за розповсюдженням інформації в соціальних мережах шляхом блокування повідомлень, що передаються, відключення від мережі Інтернет і тому подібні методи видаються дуже скрутними.

Крім того, така тактика не може бути довгостроковою і викличе соціальну напругу. З урахуванням викладеного найперспективнішим методом протидії інформаційним атакам, реалізованим з допомогою соціальних мереж, представляється контрпропаганда і навіть застосування превентивних заходів боротьби з потенційними інформаційними загрозами. Проблема використання соціальних мереж в інформаційних війнах потребує постійного серйозного вивчення як частину роботи із забезпечення ефективності реалізації державної політики України у сфері інформаційної безпеки [48, с.326].

Як показує практика, найбільш важливим етапом у веденні інформаційної війни в соціальній мережі є її початок – тобто, забезпечення домінування в інформаційному просторі, або події. Другим ключовим фактором, що забезпечує успіх всього підприємства, є масований характер дій, спрямованих на володіння

пріоритетом у наданні інформації, що має надзвичайно злободенний, глибоко персоніфікований характер, неодмінно з відтінком сенсаційності та ін.

Важливою ланкою тут є надходження інформації з різних, на перший погляд не пов'язаних один з одним джерел. Інформація, підтверджена перехресними відомостями, в очах більшості має незрівнянно більшу вагу. Для цього до соціальних мереж залучаються ЛОМи – лідери громадської думки – рейтингові політики, діячі культури, лікарі чи журналісти, авторитет яких в очах громадськості дуже високий.

З такою категорією користувачів активно працює соціальний сервіс «Твітер» – система, що дозволяє надсилати короткі текстові нотатки (до 140 символів), що містять у собі, як правило, короткий коментар (1-2 пропозиції) опублікованого в інших соціальних мережах або традиційних ЗМІ проблемного матеріалу. Журналісти, блогери та звичайні користувачі починають самостійне розповсюдження підкинутої інформації – «репост» або «ревіт», причому часто в абсолютно вільних та непередбачуваних інтерпретаціях. Після формування у громадськості початкового ставлення до ситуації та запуску механізму інформаційної експансії настає фаза інформаційного протиборства.

Для пікової фази інформаційного протистояння характерне дуже широке охоплення аудиторії, а також наявність у більшості респондентів думки, що сформувалася з питання. У 90% випадків ця думка буде фактично тотожною версії, представленої будь-ким із суб'єктів, які брали участь в інформаційній війні. 10%, що залишилися – специфічна аудиторія, серед якої панує гіпертрофований скепсис по відношенню до будь-якої інформації, що надходить. Ефективність подальшого розміщення інформації стрімко знижується, оскільки початковий інформаційний привід вичерпано [48, с.330].

Отже, механізм інформаційного протистояння можна так:

1. Забезпечення пріоритету представлення інформації в Інтернет-просторі соціальних мереж та запуск механізму інформаційної експансії, коли відбувається вкидання та поширення вигідної суб'єкту інформаційної складової;

2. Досягнення піку інтересу до новини або події та народження передумов «інформаційної гри» – того моменту, коли опонент змушений включитися в

інформаційний процес, якщо моніторинг інформаційного простору не був проведений раніше;

3. Запровадження методів «важкої артилерії» чи контраргументів – етап, характеризується вершиною соціального інтересу і остаточним формуванням аудиторних переваг.

Висновки до розділу 2

Основною мішенню інформаційної зброї є інформаційна структура суспільства. Вона націлена на збройні сили, підприємства оборонного комплексу країни, а також структури, що відповідають за внутрішню та зовнішню безпеку держави. Використовуючи інформаційну зброю під час інформаційної війни, сторони переслідують певну мету – завоювати перевагу над противником і завдати йому поразки у конкретному акті протистояння у зовнішній і внутрішній політиці, економіці, обороноздатності держави загалом.

У ході застосування інформаційної зброї агресор реалізує на практиці такі завдання:

- підрив авторитету держави на міжнародній арені, утруднення співробітництва з іншими країнами;
- маніпуляція свідомістю населення країни, створення атмосфери бездуховності та аморальності, пропаганда негативного ставлення до культурної спадщини;
- провокація політичної напруги всередині країни, національних та релігійних зіткнень, масових заворушень тощо;
- підрив авторитету державних органів у власних очах населення, дискредитація всієї системи управління;
- порушення системи управління країною, армією, технікою, виробництвами;
- завдання шкоди інтересам держави у сфері політики, економіки, соціальної та інших сфер діяльності.

Інформаційна зброя докорінно відрізняється від інших видів зброї насамперед тим, що не несе відкритого військового характеру та не використовує насильницьких дій у ході застосування. Проте, результативність застосування інформаційної зброї можна порівняти із застосуванням зброї масового ураження. Найбільші втрати збройні сили зазнають при використанні противником зброї, спрямованої на вплив на психічний стан людини та системи управління.

Враховуючи стрімкий розвиток сучасних технологій, появу нових форм та методів інформаційної боротьби, це питання навряд чи колись зможе вважатися закритим. Сьогодні ж необхідне створення та розвиток ефективної системи ведення інформаційних війн у соціальних мережах для протистояння потенційним загрозам і політичним супротивникам, а також мінімізації завданих ними збитків.

Он-лайнові соціальні мережі, крім виконання функцій обміну думками та отримання інформації, все частіше стають об’єктами та засобами інформаційного управління, ареною інформаційного протиборства, а також зручною платформою для розгортання та ведення інформаційних війн. В даний час використовується велика кількість дефініцій інформаційної війни, кожна з яких має як свої переваги, так і недоліки.

РОЗДІЛ 3
ПРАКТИЧНЕ СТВОРЕННЯ ТЕЛЕГРАМ КАНАЛУ «INFO BREAKER» ЯК МЕТОДУ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ

3.1. Особливості розробки та створення телеграм-каналу

Інтернет-месенджер «Телеграм» планувався як максимально захищений від злому інструмент міжособистісного спілкування. Проте сьогодні він перетворився також на затребуваний канал масової комунікації, медійне середовище. Громадсько-політичні канали телеграм грають все більш важливу роль у формуванні новин, а їх публікації викликають громадський резонанс. Вартість рекламної публікації в стрічці топових телеграм-проектів сягає 500–2,5 тис. доларів.

Зростання популярності телеграм можна пояснити низкою причин. В першу чергу це імідж «недоступної для прослуховування» програми, попит на яку різко зріс після викриттів Е. Сноудена. Архітектура телеграм та алгоритми шифрування гарантують конфіденційність листування та анонімність авторів. Іншим значущим фактором є дрейф телеграм у бік медійного майданчика. У 2015 році було створено інфраструктуру, необхідну для її розвитку: у месенджері з’явилися канали (аналог мікроблогів) та «супергрупи», що дозволяють охопити до 20 тис. учасників. Нові можливості для виробників та дистрибуторів контенту відкрили роботи – інтерактивні програми, що надають інформацію за запитами користувачів [7].

Телеграм досить багатогранна соціальна мережа і крім стандартного набору функцій як обмін повідомленнями у групах та діалогах, месенджер дає можливість зберігати необмежену кількість файлів та документів, створювати та вести свої канали (мікроблоги), розробляти та використовувати ботів. Канали в телеграм як правило використовують як: новинні стрічки, просування свого каналу (блогу), групи, продажу огляду чи різних послуг та/або товарів, оповіщення про знижки та акції, а також ботів.

До використання роботів починають вдаватися багато користувачів, блогери, а також великі компанії. Це допомагає якісно та швидко збирати статистику, взаємодіяти з підписниками та загалом вести канал. Боти полегшують деякі рутинні завдання та допомагають практично повністю автоматизувати ведення свого каналу, запланувавши, наприклад, автопостинг, створити опитування на будь-яку тему або ж надсилати повідомлення підписникам. Боти також допомагають завантажувати різні аудіо, відео файли і навіть конвертувати відео з Ютуб в аудіо повідомлення в телеграм.

У каналу в телеграм як самостійного маркетингового інструменту багато переваг:

- формат каналу свіжіший, ніж класичний блог або стрічка новин і ще не набрид користувачам.
- У телеграм можна створити власне бюджетне бренд-медіа.
- Є система сповіщення про нові пости. І навпаки: повідомлення про вихід постів легко вимкнути.
- Висока залученість та охоплення. До 90% бачать та реагують на пости.
- Немає дратівливої реклами, як на Ютуб, в Інстаграм та інших соцмережах.
- Можливе дотримання анонімності автора.
- Цільова аудиторія телеграм більш просунута, освічена і молода, ніж в інших соціальних мережах і месенджерах.

Створити канал у телеграм можна як із мобільного додатка, так і через веб-версію месенджера. Телеграм – це безкоштовний захищений месенджер, що вигідно виділяється на тлі інших додатків та соціальних мереж. Працює швидше сайтів та сервісів розсилок, простий та зрозумілий у використанні. На момент січня 2021 року аудиторія перевищила 500 мільйонів активних користувачів.

3.2. Наповнення телеграм каналу антипропагандними матеріалами

Термін «пропаганда» (від лат. Propaganda – поширення) має багато наукових визначень, з яких в якості основних можна виділити наступні:

1) система діяльності, спрямована на поширення знань, цінностей і іншої інформації з метою формування певних поглядів, уявлень, емоційних станів, надання впливу на соціальну поведінку людей;

2) поширення в масах ідеології та політики певних класів, партій, держав;

3) засоби маніпуляції масовою свідомістю [8, с.83].

На наш погляд, під пропагандою доцільно розуміти мотивований інформаційно-психологічний вплив на емоційно-вольову сферу масової свідомості, за допомогою якого впроваджуються ідеї, погляди, установки і формується суспільна поведінка. Основною психологічною метою пропаганди є вплив на систему ідейних, громадських і політичних установок людей, яку можна змінити шляхом формування нових установок або через посилення (ослаблення) вже існуючих.

Соціальні установки висловлюють ставлення особи до суспільних норм і стандартів і проявляються в соціальній поведінці даної людини. Існують і інші установки (світоглядні, патріотичні), які також формуються під впливом політичної пропаганди і випливають з вищеназваних груп. Психологічному впливу пропаганди піддаються в першу чергу емоції. Залежно від того, які емоції пробуджує пропаганда, розрізняють позитивну і негативну пропаганду [15, с.54].

Позитивна пропаганда, виконуючи виховну, інформаційну, роз’яснювальну функції, сприяє соціальній гармонії, вихованню людей у відповідності із загальноприйнятими цінностями і нормами. Вона здійснюється в інтересах тих, кому адресована, а не необмеженого кола зацікавлених осіб. Позитивна пропаганда не переслідує жорстких маніпулятивних цілей. Негативна пропаганда спрямована на створення ілюзорної, паралельної реальності, вигідної пропагандисту, з перевернутою системою цінностей, переконань, поглядів з метою маніпулювання суспільною свідомістю в інтересах вузької групи осіб. Вона сприяє розпалюванню соціальної ворожнечі, соціальних конфліктів,

загострення протиріч в суспільстві. Це дозволяє роз'єднувати людей і нав'язувати вигідні пропагандистам переконання і стереотипи.

Дослідники технологій маніпулювання суспільною свідомістю вважають політичну пропаганду найпотужнішим засобом психологічного впливу (навіть тиску) на суспільну свідомість і думку з метою формування певного політичного мислення. З безлічі досліджуваних ними методів (прийомів) пропаганди виділимо такі, при реалізації яких, на наш погляд, в значній мірі підвищується ефективність формування і впровадження іміджу (образу) політичних акторів в свідомість громадян.

Можна виділити наступні істотні властивості пропагандистського дискурсу, які слід враховувати при проведенні лінгвістичної експертизи в зв'язку з пропагандою екстремізму і тероризму:

1. Наявність суб'єкта пропаганди (часто інституційно оформленого).
2. Наявність адресата пропаганди (часто узагальненого, тобто сукупності осіб, уявлення про дійсність яких повинні бути змінені в результаті пропагандистської діяльності).
3. Наявність сукупності відносно простих несуперечливих тез (опис бажаної ситуації – стану справ) і аргументів.
4. Наявність протиставлених оцінок бажаної ситуації та її негативних альтернатив.
5. Періодична реалізація в дискурсі зазначеної сукупності тез або її фрагментів з ідентичною або дещо модифікованою аргументацією.
6. Наявність безлічі текстів за певний період часу (період пропагандистської кампанії) [22, с.105].

Сучасні трансформаційні перетворення української господарської системи супроводжуються ускладненням структури інформаційного простору як сегмента економічного простору, фактором формування якого виступає інформація. Обмін інформацією та інші види інформаційної активності є основою реалізації економічних процесів. Більш досконале середовище інформаційної активності, знижуючи невизначеність господарської діяльності

суб'єктів, дозволяє їм досягати більш високого рівня ефективності використання ресурсів.

Розвиток глобальних інформаційних мереж сприяє залученню в господарський обмін все більших інформаційних ресурсів, забезпечуючи кількісну і якісну зміну структури витрат та пред'являє нові вимоги до технологічної складової економічного прогресу. Необхідність скорочення трансформаційних і трансакційних витрат, пов'язаних з використанням інформації, обумовлює формування інформаційного простору.

Поняття інформаційного простору органічно вписується в систему вже досить звичних, визнаних концептів теорії інформатики, пов'язаних з локалізацією інформаційних параметрів, властивостей і відносин, таких як, наприклад, інформаційний ресурс та інформаційне середовище. Однак ці категорії ще слабо розроблені в теоретичному і методологічному аспектах. Перераховані поняття вживаються без урахування їх можливої тотожності, слабо представлений їх взаємозв'язок з економічною діяльністю, властивостями і відносинами ресурсів і середовища. Тому важливо визначити сутність цих категорій в соціально-економічному аспекті, виявити можливі категоріальні взаємозв'язки, враховуючи при цьому рівні структуризації суб'єктів інформаційних та господарських відносин.

Інформаційний простір доцільно визначати як вид економічного простору, виділений на основі визнання ендогенних інформаційних факторів виробництва, що включає відносини господарюючих суб'єктів з приводу цього фактора, а також відповідні умови, ресурси і продукти їх діяльності. Застосування структурної рекурсії до господарських систем дозволяє отримати для кожної з них на різних рівнях внутрішньо інформаційний простір, що відбиває аспекти їх внутрішнього середовища [30, с.100].

Таким чином, виникає ієрархія «вкладених» інформаційних просторів різних рівнів, яка відображає гетерархію аспектованих підсистем всередині господарської системи кожного рівня, що обумовлює і забезпечує їх функціонування. Інформаційний простір регіонального ринку праці – аспектно специфікована форма декомпозиції простору господарської системи мезорівня.

Глобальний інформаційний простір являє собою багаторівневу ієрархічну систему, на самому нижчому рівні декомпозиції якої знаходяться взаємопов'язані сукупності різних предметно орієнтованих інформаційних систем.

По суті, вони є однорідними і витягають, і обробляють дані безпосередньо з відповідної предметної області. Транзакційні витрати є параметрами, що визначають специфіку відносин між суб'єктами регіонального економічного простору, для функціонування яких характер інформаційного обміну як невід'ємний атрибут їх взаємодій має вирішальне значення. Інформаційний фактор як завершальний ендогенний поряд з організаційним і інституціональним забезпечує транзакції, пов'язуючи виробників і споживачів в просторі відтворювальних процесів. Це буде виражатися в характері і структурі обмінів, і взаємодій між окремими інформаційними системами агентів в інформаційному просторі регіональної економіки [31, с.180].

В процесі перетворення інформації суб'єкти інформаційного простору сприймають навколишнє середовище шляхом фільтрації і обробки інформації за допомогою ментальних моделей, що забезпечують розуміння навколишнього середовища і вирішення виникаючих проблем.

Інформаційний простір має такі основні властивості. Це, перш за все, цілісність, що розуміється як єдність усіх об'єктів і суб'єктів в економічному просторі. Інститути та підтримуюча їх діяльність переводять безліч суб'єктів, що функціонують в рамках економічного простору, в певну впорядковану інституційну структуру. Отже, основний фактор цілісності, системності суб'єкта – прояв його економічної діяльності.

Інформаційний простір розкривається у вигляді різноманітних соціально-економічних, суспільних і інформаційних зв'язків суб'єктів економічного простору, є мірою їх залучення в суспільні відносини. Наступна властивість інформаційного простору – комунікативність, що виявляється через взаємопов'язані процеси інтеграції та диференціації як всередині суб'єкта, так і з зовнішнім середовищем. Оскільки відзначається постійне збільшення числа взаємодій суб'єктів, що відбуваються в економічному просторі в одиницю часу,

а інформація про ці події відтворюється і тиражується в усе більшому обсязі, в інформаційному просторі, логічно виділити таку властивість інформаційного простору, як динамічність [51, с.14].

Іншими важливими властивостями інформаційного простору є розширення меж, що відбувається за рахунок дедалі більшої складності економічних суб'єктів і їх інформаційного відображення і підвищення щільності, що посилюється завдяки зростанню взаємозв'язків між суб'єктами діяльності, її інтернаціоналізації, кооперації, підвищення числа елементарних інформаційних обмінів в одиницю часу.

3.3. Специфіка роботи з платформою Телеграм

Телеграм, на перший погляд, схожий на інші месенджери – Ватсап, Вайбер, Фейсбук. Листування, обмін фото та відео – все як у всіх. Але, на відміну від конкурентів, телеграм пропонує низку переваг:

- передача файлів будь-якого формату – RAR-архів, таблиці в Excel, інструкція у PDF, MP3 та відео. За розміром файлів – обмеження до 1,5 Гб.
- Хмарне зберігання даних.
- Синхронізація із пристроями. Месенджер працює на iPhone, Android, WindowsPhone. Є он-лайн та декстоп-версії. Крім того, можна заходити відразу з кількох пристроїв: кількість одночасних сесій необмежена.
- Моментальна доставка повідомлень та файлів. Без глюків та зависань.
- Створення великих чатів – до 5000 учасників.
- Безпека. Павло і Микола Дурови пообіцяли винагороду в 200.000 $ тому, хто зможе зламати код і прочитати їхнє листування. Поки що нікому не вдалося це зробити. І ще до питання безпеки. В додатку можна встановити налаштувати видалення повідомлень та облікового запису. А ще – без побоювання вести конфіденційні бесіди: кожне повідомлення самознищується після прочитання співрозмовником.

Деякі опції в месенджері «Телеграм» знаходяться на поверхні, інші ж не видно відразу, про треті можна і зовсім не здогадуватися. Розробники постійно працюють над оновленнями функціоналу, завдяки чому програма обходить конкурентів із завидною швидкістю.

Головною особливістю месенджера, що разюче відрізняє його від конкуруючих додатків, є безпека передачі інформації. Телеграм і був задуманий Дуровим для максимального захисту персональних даних, що було успішно здійснено командою розробників. Ні прочитати особисті повідомлення, ні прослухати дзвінки не можуть навіть спеціальні структури.

Додаткову безпеку забезпечують секретні чати із функцією самознищення повідомлень. Листування миттєво видаляється на пристроях обох учасників, якщо це зробить хоча б один з них, а про збереження даних шляхом скріншота співрозмовнику прийде повідомлення. У месенджері можуть бути використані двоетапна аутентифікація та блокування чатів за допомогою пін-коду або сканера відбитків пальців. Налаштування також дозволяють захистити свій обліковий запис, видаляючи сесії на інших пристроях, на випадок, якщо людина користувалася чужим девайсом і не вийшла з профілю.

Особливості спільнот:

1. Тематичні чати закритого типу створюються з метою спілкування невеликої групи людей та можуть включати до 200 осіб. Додавати нових співрозмовників може кожний учасник.

2. Супергрупи об’єднують велику кількість людей за інтересами (до 5000). Доступ до всієї історії листування мають усі учасники. Кожен може редагувати або видаляти повідомлення. Очищати чат, закріплювати записи, контролювати кількість учасників можуть лише адміністратори.

3. Канали – це тематичні спільноти, які можна лише читати, без права коментування, на них може підписуватись будь-який бажаючий користувач, причому кількість підписників не обмежена. Надсилання повідомлень може здійснюватися як між двома співрозмовниками, так і в групових чатах. Користувачі можуть переписуватися на тлі музики, що програється, ділитися

файлами (причому неймовірних для інших месенджерів об’ємів), виправляти або видаляти відправлені записи.

Можна виділяти тексти жирним, писати курсивом чи шрифтом розробників. Можливості форматування повідомлень у телеграм не такі різноманітні, як хотілося б, але все ж таки присутні. Для їх розширення можна скористатися сторонніми ресурсами, будь-якими текстовими редакторами або платформою Telegra.ph, спеціально розробленою для створення публікацій. Тут є можливість додавання фото, відео до постів. Додаткову реєстрацію платформа не вимагає.

Раніше опція здійснення аудіодзвінків у месенджері була відсутня, але зараз користувачам надана і ця можливість. Розмови через програму шифруються за тією ж технологією, що й секретні чати, тому переживати про безпеку розмов не варто. Дзвінки в телеграм контролюються нейронною мережею, яка аналізує технічні дані про кожен голосовий виклик. Із зібраної інформації вдосконалюється якість кожного наступного дзвінка. Налаштування приватності забезпечують максимальний комфорт спілкування, дозволяючи визначати, від кого є бажання приймати дзвінки, а від кого – ні. Можна також вимкнути функцію звукових дзвінків. До речі, на відміну від інших програм, де сигнали виклику звучать однаково, в телеграм за звуком гудка можна зрозуміти, в мережі абонент або ні.

3.4. Аналітика телеграм каналів щодо протидії інформаційній війні на прикладі українських продуктів

Події 24 лютого не лише сколихнули світ, а і прямо змінили тактику донесення інформації. Крім того, мережа «Телеграм» стала плацдармом не лише для ведення пропаганди, а й антипропаганди. Через велику популярність мережі «Телеграм» через безпечну передачу даних, з моменту початку війни створили сотні телеграм каналів, основна мета яких є сповіщення про ситуацію в країні. Та кількість фейків та пропаганди, яка звалилась на українців, затьмарює кількість раніше існуючих підпільних спільнот.

Через те, що аудиторія телеграм каналів, як правило – молодь, ведення пропаганди дається більш легко, адже більш старші люди спочатку критично підходять по публікацій, різнобічно її оцінюють і лише потім репостять. Натомість молодь дуже рідко вдається до заходів перевірки джерела інформації, стаючи учасником розповсюдження інформації.

Варто визнати, що телеграм зараз дає можливість оперативного повідомлення ситуації через спільноти. Це дозволяє не лише швидко дізнатись інформацію, але і підтвердити її чи спростувати. Далі розглянемо кілька телеграм каналів та специфіку подачі інформації.

Лідером із ведення антипропагандистських матеріалів по праву можна вважати офіційний канал Президента України Володимира Зеленського. Його візуальне зображення представлено на рис 3.1.

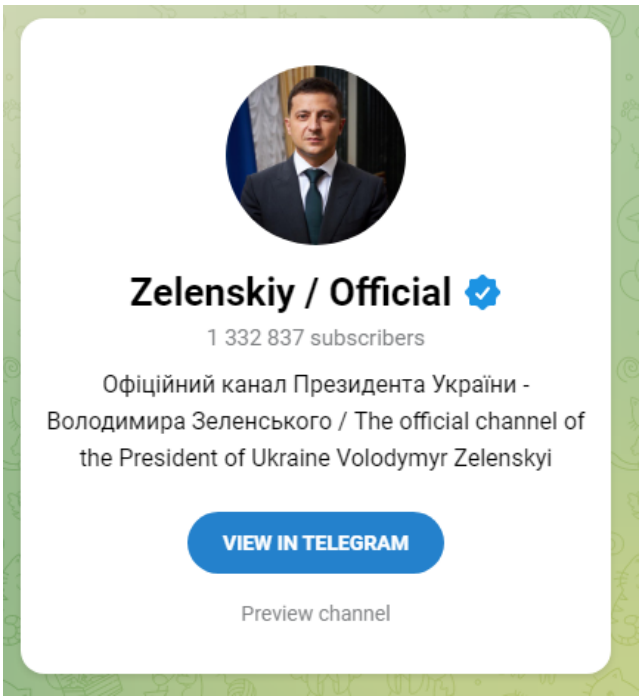

Рис. 3.1. Офіційний канал в телеграм Володимира Зеленського

На теперішній момент чисельність підписників складає 1332837. Звісно ця цифра не є сталою і постійно змінюється. На каналі подається оперативна інформація щодо дій противника, виступів Президента для іноземних урядів, участі В. Зеленського в світових нарадах тощо. Крім того, активно подається спростування неправдивої інформації та дається попередження про можливі загрози для життя.

При визначенні стильової приналежності тексту враховуються як екстралінгвістичні показники, так і власне мовні. Важливими виявляються сфера спілкування (ділова, спеціальна, політико-ідеологічна, естетична), функція мови і тексту в цілому (повідомлення, вплив), призначення тексту (інформування, припис, інструктування, навчання). Серед показників мовно-стилістичного плану враховуються загальні стильові і стилістичні домінанти, з них найбільш узагальненими і типовими виявляються:

- абстрактність – конкретність;
- логічність – емоційність;
- стандартність – стилістична маркованість;

об’єктивність – суб’єктивність

В. Зеленський викликає посилену довіру у своїх громадян, а відтак цей канал можна розглядати як один із кращих варіантів ведення активної інформаційної війни з любителями «руського мира».

Наступним популярним телеграм-каналом є канал голови Миколаївської ОДА В. Кіма. Цей посадовець набув популярності через гумор, посмішку та відкритий «стьоб» з рашистів. На рис.3.2. представлено його візуал.

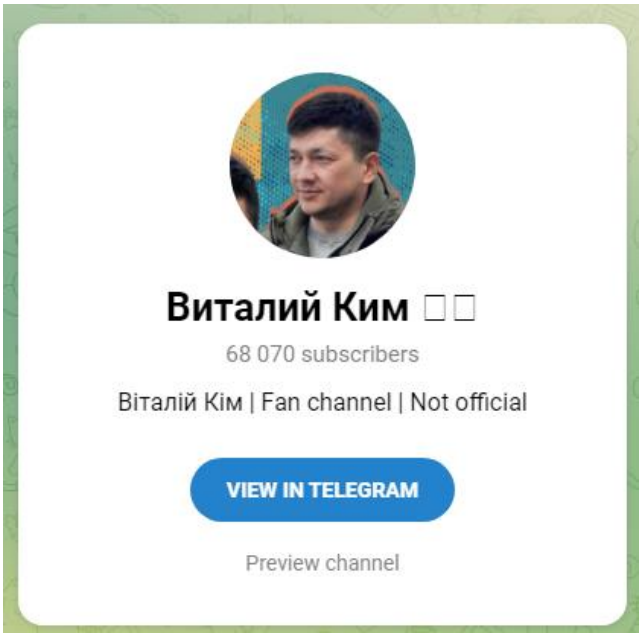

Рис. 3.2. Офіційний канал в телеграм Віталія Кіма

На момент проведення аналізу кількість підписників сягає 68000 осіб. На початку війни В. Кім публікував не лише необхідну аналітичну інформацію та звіти про роботу, а і інформував населення Миколаївщини про роботу влади в період війни. В. Кім «ріже» фейки і відкрито насміхається з провокаційних пропагандистських матеріалів «руського міра». Також на сторінці здійснюється репост публікацій з телеграм каналу Президента України.

3.5. Опис розробленого телеграм-каналу «Info Breaker»

Месенджер «Телеграм» дає можливість своїм користувачам створювати публічні канали для поширення актуальної інформації, таким чином перетворюючи Інтернет-майданчик на інноваційний вид цифрового засобу масової інформації. Цю заслугу платформа отримала завдяки можливості збереження анонімності авторів, що, у свою чергу, дозволяє говорити про належний рівень захисту інформатора від різних зовнішніх факторів, у тому числі державної цензури, з якою стикаються класичні ЗМІ.

Продовжуючи розмову про особливості телеграм як інноваційної форми ЗМІ, слід згадати відсутність можливості коментування постів, що виділяє даний месенджер серед інших соціальних медіа. З одного боку, це дозволяє говорити про відсутність оціночного тиску на авторів публікацій, однак, в той же момент, даний фактор не дозволяє тим же авторам публічних каналів справедливо дати оцінку ступеня «цифрового шуму» навколо новин, що публікуються і позицій у рамках політичної комунікації.

Описуючи явні недоліки даної платформи, слід насамперед зазначити, що телеграм-канали характеризуються певною часткою маніпулятивності, формуванням особливого інформаційного фону навколо подій, в деяких випадках, що відрізняються від дійсності та зниженої грамотністю, яка в свою чергу, є характерною рисою сучасних соціальних мереж.

Останнім часом телеграм став використовуватися для дезорієнтації в суспільстві завдяки тому, що багато авторитетних політичних каналів стали публікувати так звані уявні новини. В результаті цього можна говорити про трансформацію незалежного майданчику в повноцінне поле для ведення інформаційної війни між прихильниками та противниками «спеціальної військової спецоперації РФ».

Канал «Info Breaker» був розроблений в рамках дипломного проєкту. Знайти його можна в пошуку телеграм за ніком @news020201. Канал орієнтовано на українську молодь, яка цікавиться сучасною геополітичною ситуацією у світі та військовим вторгненням РФ в Україну.

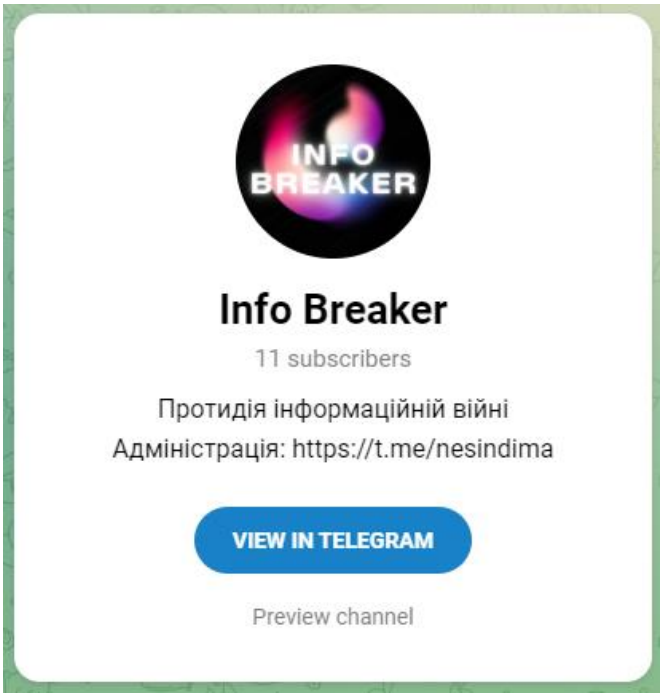

Рис. 3.3. Телеграм-канал «Info Breaker»

Змістовне наповнення каналу викладене українською мовою. Основний меседж каналу «Стоп пропаганді РФ». Основною метою створення інформаційного майданчику було розміщувати правдиві, офіційні та перевірені дані для розвінчування міфів російської пропаганди. За ознакою новизни інформації телеграм-канал можна назвати агрегатором повідомлень відкритих джерел та постачальників ексклюзивів.

На каналі «Info Breaker» публікуєтеся власна колонка текстів, яка допомагає читачеві розібратися в речах, які відбуваються в інформаційному полі. Майже кожен день автори «Info Breaker» вивчають новини, щоб виявити в них слова, які вже перетворилися на журналістський штамп. Задача «Info Breaker» – з'ясувати, що вони насправді означають. Адже без цього ми не можемо розуміти новини.

На прикладі текстів про «Традиційні цінності» чи «Патріотизм», якими часто оперує російська пропаганда можна зробити висновок, що автори каналу дуже добре розуміються на темах, які ворог використовує в якості важелів впливу.

Перевагою, яка виділяє «Info Breaker» на фоні інших каналів є те, що автори пишуть свої тексти на зрозумілій читачу мові, без використання складної термінології. Дуже важливо що канал є орієнтовним саме на молодіжну аудиторію.

Загалом можна говорити про високу залежність порядку денного інформаційного телеграм-каналу від ЗМІ. Ця залежність простежується як у дотриманні сформованим масмедіа трендів, а також у використанні матеріалів ЗМІ при формуванні своєю особливої інформаційної картини.

Висновки до розділу 3

Соціальні мережі представляють он-лайн-платформи, де люди можуть спілкуватися та будувати соціальні взаємини один з одним. У соціальних мережах можна зблизитися з людиною завдяки схожим інтересам, а також можна підтримувати спілкування зі знайомими та друзями з оф-лайн життя. Месенджер (або система миттєвого обміну повідомленнями) – це програма, яка використовується для спілкування за допомогою повідомлень.

Якщо розглядати месенджер «Телеграм» як платформу для розповсюдження інформації, вона дає редакторам ще більше переваг, ніж соціальні мережі. Як і будь-який інший майданчик для розміщення матеріалів, соціальні мережі та мессенджери диктують власні правила розміщення контенту. Наприклад, у соціальних мережах рідко можна побачити довгі статті та лонгріди – їх намагаються публікувати у вигляді посилань на сайт, де можна почитати повний текст статті, якщо заголовок та підводка зацікавлять читача.

Телеграм як майданчик для публікації новин та взаємодії з аудиторією добре показує себе на прикладі роботи багатьох ЗМІ. Особливості присутності політиків, державних посадовців у телеграм передбачають трансформацію всіх матеріалів, що публікуються. Тому на постінг кожної вже опублікованої статті у редактора йде певна кількість часу, тому що потрібно міняти стиль подачі тексту і часто його повністю переписувати.

На наш погляд телеграм є прекрасним варіантом для пропаганди, а відтак виникає потреба у формуванні анти пропагандистських матеріалів. В роботі досліджені 2 телеграм канали: президента України В.Зеленського та голови Миколаївської ОДА В. Кіма. Канали телеграм – новітня площадка для реалізації інформаційної політики України та боротьби з фейками, які активно використовуються в інформаційній війні проти України.

На основі всіх порад був створений телеграм-канал «Info Breaker», який активно розвінчує фейки російської пропаганди та допомагає читачам молодого віку розумітися в речах, які оточують їх в інформаційному просторі.

ВИСНОВКИ

Провівши дослідження теоретичних аспектів виникнення та ведення інформаційної війни, можемо зробити наступні висновки.

Сьогодні нові засоби масової комунікації пов’язали невидимими нитками практично весь світ і, на жаль, цей світ не обходиться без інформаційних війн. Термін «інформаційна війна» є актуальним і важливим на сучасному етапі розвитку. Без чіткого розуміння поняття «інформаційна війна» неможливо зрозуміти процеси, що відбуваються у політичному житті країни та світу.

Традиційними засобами розгортання інформаційної війни постають дані, інформація та знання, які, у свою чергу, можуть бути визначені у лінійній послідовності. Дані описують характеристики об’єктів реальної дійсності, інформація є зібраними даними, які представлені у певному контексті, знання – це інформація, що інтерпретується у світлі певного життєвого досвіду.

Інформаційна війна, по суті, інтерпретується як феномен, синонімічний революції в інформаційних технологіях з її потенціалом реалізовувати стрімкі трансформації військових стратегій. Процвітання держави – якщо не сам факт її виживання, залежить від її здатності ефективно розвивати та застосовувати інформаційні технології. Без надійного захисту життєво важливої інформації, інформаційних процесів та систем загальнодержавна стратегія приречена на провал.

Інтернет пропонує деякі унікальні здібності для організаторів інформаційної боротьби, наприклад, анонімність. Завдяки Інтернету можна вигадати несправжні персонажі, наділяючи їх необхідним характером та історією. Тим часом аудиторія таких псевдоперсонажів сприйматиме цілком за реальних. Творець такого героя може викликати величезну довіру у оточуючих до свого персонажа. Одну думку, ідею можна одразу транслювати на кілька майданчиків.

Люди одночасно на різних сайтах бачать ту саму інформацію, отже, більше починають їй довіряти. Вважається, що найефективнішою є та пропаганда, яка транслюється відразу за всіма напрямками. У зв’язку з бурхливим розвитком

соціальних мереж виникає велика кількість псевдоінформації. На основі цієї інформації аудиторія робить помилкові висновки.

Перспективи поширення пропаганди засобами комунікації залежать від об'єктивних потреб соціальної еволюції суспільства у напрямі розвитку таких моделей формування суспільної думки, які передбачають когнітивну основу суб'єктно-об'єктних зв'язків. На відміну від спонукальних функцій реклами, котра апелює переважно до емоційної складової реципієнта, засоби пропаганди за своєю інформаційною сутністю підвищують культуру населення, збагачують тезаурус електорального соціуму. Саме тому на порядок денний висуваються визначальні складові, що забезпечують реалізацію пропагандистської функції, а саме: формування наукової школи здійснення пропаганди; поширення комунікативної мережі; організаційне наближення інститутів громадянського суспільства до інформаційних ресурсів; професіоналізація пропагандистської діяльності на постійній основі каналами комунікації.

Соціальні мережі – це комунікаційне явище, що використовує в якості основного джерела і передавача інформації, суспільство в цілому, тим самим просунувши міжособистісну комунікацію на наступний рівень. Відмінною рисою соціальних мереж від традиційних медіа як майданчика для комунікації є інтерактивність і як результат двонаправленість.

Так само, соціальні мережі дозволили комунікації стати більш персоналізованою. Велика аудиторія соціальних мереж, використовуючи соціальні стрічки для отримання нової інформації, спілкування з друзями, нових знайомств і пошуку груп за інтересами. У зв'язку з цим, для багатьох користувачів соціальні мережі стають синонімом Інтернету.

В рамках дипломного проєкту було створено телеграм-канал «Info Breaker», який активно публікує власні тексти про речі, які оточують кожного в інформаційному полі під час війни. Також канал розвінчує фейки використовувані пропагандою російської федерації.

В нашому дослідженні розглядалась соціальна мережа «Телеграм» як платформа для ведення антипропаганди та розвіювання фейків. Крім того телеграм по праву слід визнати чудовим засобом ведення інформаційної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти. МВС України, Ун-т внут. справ, За заг. ред. О.М. Бандурки Харків, 2016. 366 с.
2. Бернейс Э. Пропаганда / пер. с англ. И. Ющенко. Москва: Hippo Publishing, 2010. 176 с.
3. Бобало О. Ю. Комунікативні стратегії. Львів: Вид-во Львів. політехніки, 2015. 344 с.
4. Богуш В.М. Інформаційна безпека держави. Київ: МК-Прес, 2005. 432 с.
5. Бондарсук О.В. Відображення у дискурсі ЗМІ пропагандистських кампаній. *Political science*. № 12 (104). 2013. С.49-53.
6. Валюшко І. О. Основні виклики і загрози в епоху інформаційних війн. *Науковий вісник Дипломатичної академії України. Зовнішня політика і дипломатія: традиції, тренди, досвід. Частина II. Серія «Політичні науки*» / За заг. ред. В.Г. Ціватого, Н.О. Татаренко. 2016. С. 142-147.
7. Васильчук Г.М., Маклюк О.М., Бессонова М.М.Феномен пропаганди та антипропаганди у сучасному світі: історико-політологічний дискурс. Запоріжжя: Інтер-М, 2018. 386 с.
8. Гавловський В. І. Організаційно-правові питання формування державної інформаційної політики в Україні. *Наук. вісн. зб. наук. пр. Акад. держ. податков. служби України*. 2012. № 3. С. 177-182.
9. Гавловський В., Калюжний Р., Цимбалюк В. ін. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права. *Прав., нормат. та метрол. забезпечення системи захисту інформації в Україні*. 2017. № 8.
10. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. Вип. № 1. С. 136–141.

11. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу: Навчальний посібник. Київ: КНТ, 2007. 260 с.

12. Демків Т. Ф. Взаємодія органів державної виконавчої влади з засобами масової інформації (на прикладі досвіду Державної податкової служби України). *Сучасна регіональна політика: формування, реалізація та розвиток публічної служби: матеріали підсумк. наук.-практ. конф. за міжнар. участю.* Одеса: ОРІДУ НАДУ, 2010. С. 461–463.

13. Додонов А.Г., Горбачик Е.С., Кузнецова М.Г. Современные технологии и проблемы информационной безопасности. *Інформаційні технології та безпека: Зб. наук. праць. Київ: Інститут проблем реєстрації інформації НАН України*, 2006. В. 9. С. 51-59.

14. Зінченко М.О., Плугова О.Б, Драглюк О.В. Інформаційна війна, засоби реалізації та протидії. Інформаційний вимір гібридної війни: досвід України: *матеріали міжнародної науково-практичної конференції.* Київ: НУОУ, 2017. С. 38–40.

15. Іваницька Б. Основні методи пропаганди в російському інтернет-ЗМІ pravda.ru. *Вісник Національного університету «Львівська політехніка».* Серія: Журналістські науки. 2018. № 896. С. 54–58.

16. Іжутова І. Мартін Лібікі: «Що таке інформаційна війна?» *Військо України*. 2014. URL : http://viysko.com.ua/texnologiji-voyen/martin-libiki-shho-take-informacijna-vijna

17. Карпенко В. Інформаційний простір як чинник національної безпеки України. *Українознавство: науковий громадсько-політичний культурно-мистецький релігійно-філософський педагогічний журнал*. 2005. № 3. С. 182-192.

18. Кіца М. Особливості реклами в українських інтернет-змі в умовах інформаційної війни. *Теле- та радіожурналістика.* 2015. Вип. 14. С. 170–174.

19. Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах. *Вісник Харківської державної академії культур*. 2013. Вип. № 41. С. 1–6.

20. Костюк І.А. Інформаційні війни в контексті революційних подій в Україні. *Актуальні проблеми соціальних комунікацій*: матеріали студентської наукової конференції, 22 травня 2014 р. Київ, 2014. С. 57-60.

21. Крупський І. Безпекові імперативи інформаційного простору України. *Телевізійна й радіожурналістика: зб. наук.-метод. пр. Львів. нац. ун-т ім. І. Франка*; редкол.: В.В. Лизанчук (відп. ред.) та ін. Львів, 2007. Вип. 7. С. 189-198.

22. Леонтьєва Л.Є. Пропаганда як інформаційно-психологічний складник політичних процесів. *Львівський нац. ун-т ім. Івана Франка*. Київ, 2004. 298 с.

23. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії: Моногр. Київ, 2017. 222 с.

24. Магда Є. Виклики гібридної війни: інформаційний вимір.*Наукові записки Інституту законодавства Верховної Ради України* . 2014. № 5. С. 138-142.

25. Малик Я. Інформаційна війна і Україна. *Науковий вісник*. 2015. Вип. 15. URL : http:// www.lvivacademy.com/vidavnitstvo_1/visnyk15/ fail/Malyk.pdf.

26. Пєвцов Г.В. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: Монографія. Харків: Цифрова друкарня № 1, 2013. 272 с.

27. Почепцов Г. Пропаганда 2.0. Харків, Фоліо, 2018. 800 с.

28. Прибутько П.С. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ: Вид. А. В. Паливода, 2007. 252 с.

29. Присяжнюк М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. *Вісник Київського національного університету імені Тараса Шевченка*. 2007. № 14-15. С. 42–44.

30. Притула А. М. Пропаганда – компонент гібридної війни: шляхи протидії засобами кримінального права. Юридична наука. 2015. № 3. С. 99–104.

31. Пропаганда vs контрпропаганда у медіа просторі: минуле, сучасне, майбутнє: матеріали міжнародної науково-практичної конференції (Запоріжжя, 12 лютого 2018 р.) Запоріжжя: Інтер-М, 2018. 406 с.

32. Радковець Ю.І. Ознаки технологій «гібридної війни» в агресивних діях Росії проти України. *Наука і оборона*. 2014. № 3. С. 36-42.

33. Рибак М. І., Атрохов А. В. До питання про інформаційні війни. *Наука і оборона*. № 2. 2018. С. 65–68.

34. Саєнко О.Г. Інформаційна війна як прояв інформаційного протиборства. *Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка*. 2008. Вип. 12. С. 142–147.

35. Салата О.О. Інформаційна війна Німеччини та СРСР за вплив на окупованих територіях. *Наукові праці історичного факультету Запорізького національного університету, 2009, вип. XXVII*.С.281.

36. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. *Вісник Книжкової палати*. 2013. № 1. С. 40-43.

37. Семен Н. Ф. Поняття «інформаційна війна» в контексті соціальних комунікацій. *Держава та регіони: Серія: Соціальні комунікації.* 2016. № 1 (25). С. 22–25.

38. Семен Н.Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог»): автореф. дис. к. н. соц. комун; спеціальність 27.00.01. Дніпро : Дніпровський національний університет імені Олеся Гончара, 2018. 23 с.

39. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. 2015. С. 36-42.

40. Странніков А.М. Інформаційно-психологічне протиборство у воєнних конфліктах другої половини XX ст.: автореф. дис. на здобуття наук. Ступеня канд. істор. наук: спец. 20.02.22 Військова історія. Львів, 2010. 23 с.

41. Толубко В.Б. Підготовка і ведення інформаційної боротьби в Збройних Силах України: Навчальний посібник. Київ: НАОУ, 2004. 280 с.

42. Феклістов А.О. Сучасні погляди на місце інформаційних операцій в системах інформаційної боротьби // Системи озброєння та військова техніка. 2010. № 2(22). С. 25–27.

43. Фролова О.М. Нормативно-правові аспекти протидії інформаційним впливам РФ. *Матеріали Міжнародної науково-практичної конференції «Деокупація і реінтеграція інформаційного простору Криму: міжнародно-правові та медіа комунікативні інструменти*». Київ : Інституту міжнародних відносин. 2019. С. 69–74.

44. Цуканова О.В. Інформаційні війни: вплив на суспільство. URL: http://www.sworld.com.ua/konfer34/800.pdf.

45. Чирва Р. Інформаційна війна – зброя, страшніша за ядерну. *Профспілкові вісті*. 2014. № 13. С. 8-9.

46. Чистоклетов Л. Г. Інформаційно-психологічні впливи як невід'ємна складова парадигми інформаційної безпеки. *Науковий вісник Львівського державного університету внутрішніх справ*. 2012. С. 183–192.

47. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. Демократичне врядування. 2014. Вип. 13. URL: http://lvivacademy.com/visnik13/zmist. html.

48. Шпига П.С. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. Вип. 8. С. 326-339.

49. Шуляк Н. Інформаційні війни в інтеграційних процесах. *Міжнародні інтеграційні процеси: історичний досвід, сучасні виклики та перспективи*. С. 44–46.

50. Юськів Б. М. Опорний конспект лекцій з дисципліни «Інформаційні війни». Рівне: РІС КСУ, 2003. 55 с.

51. Яковлєва Н. І. Пропаганда як складова політичної комунікації: автореф. дис. канд. політ. наук: 23.00.02; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2010. 18 с.