МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ І ПРИКЛАДНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ

БОЙКО ЮЛІЯ ВАЛЕРІЇВНА

Допускається до захисту:
в.о. завідувача кафедри
інформаційних систем управління,
д-р екон. наук, професор
_____ Ольга АНІСІМОВА
« _____ » _____ 2021 р.

ІНФОРМАЦІЙНА ВІЙНА ЯК ЗАСІБ ВПЛИВУ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ УКРАЇНИ

Спеціальність 029 Інформаційна, бібліотечна та архівна справа

Кваліфікаційна (магістерська) робота

Науковий керівник:
Ковальська Л.А., д-р істор. наук,
доцент, професор кафедри
інформаційних систем управління

Оцінка: __/___/_____
(бали за шкалою ЄКТS/за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця – 2021

АНОТАЦІЯ

Бойко Ю.В. Інформаційна війна як засіб впливу на тимчасово окупованих територіях України. Спеціальність 029 «Інформаційна, бібліотечна та архівна справа». Донецький національний університет імені Василя Стуса, Вінниця, 2021. 76 с.

У кваліфікаційній роботі досліджено принципи, форми та методи інформаційної війни. Розглянуто інструментарій, що використовується під час ведення інформаційної війни та методику її ведення . Особлива увага приділена питанням національної інформаційної безпеки та її забезпечення на законодавчому рівні. У кваліфікаційній роботі запропоновано ряд заходів для формування ефективної протидії інформаційним атакам на державному рівні.

Ключові слова: інформаційна війна, інформаційна безпека, інформаційна атака, інформаційна зброя, комунікація, інформація, інформаційне протиборство.

Табл. 1. Рис. 9. Бібліограф.: 63 найм.

SUMMARY

Boyko Yu.V. Information Warfare as a Means of Influencing the Temporarily Occupied Territories of Ukraine. Specialty 029 «Information, library and archive», Vasyl’ Stus Donetsk National University, Vinnytsia, 2021. 76 p.

The principles, forms and methods of information warfare are studied in the qualification (master's) work. The tools used during information warfare and methods of its conduct are considered. Particular attention is paid to issues of national information security and its provision at the legislative level. The qualification work proposes several measures to form an effective response to information attacks at the state level.

Keywords: information war, information security, information attack, information weapon, communication, information, information confrontation.

Tabl. 1. Fig. 9. Bibliography: 63 items.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Електронно-цифровий характер сучасних комунікацій створив новітню модель взаємодії суспільства та призвів до появи нових проблем. До таких проблем відносять загрозу національній інформаційній безпеці країни та її населення. На даному етапі не існує ефективної системи, яка могла б забезпечити захист інформаційного поля держави. Жодна країна не має цілком захищеного інформаційного середовища і в будь-яким момент може стати об'єктом інформаційної атаки з боку інших держав. На сьогоднішній день більшість країн розглядають інформаційну війну як інструмент для реалізації зовнішньої політики.

Традиційні концепції ведення такого роду війн набувають нових масштабів. Переходять на задній план винищувальні та виснажливі стратегії боротьби. З'являються гібридні війни, непрямі атаки та принципово нові форми ведення війни: моральна, ментальна та фізична. В таких умовах інформаційна боротьба стає протиборством сторін, у якому застосовуються спеціальні засоби впливу на інформаційне середовище та психологічний стан супротивника і засоби захисту власного інформаційного поля. Інформаційна боротьба є головною складовою військових конфліктів не лише при їх підготовці, а у під час їх ведення.

Інформаційно-психологічна війна може негативно впливати не лише на взаємини між державами, а і на стан всередині цих держав. Іноді цілком достатньо використання засобів масової інформації для встановлення впливу на значні маси людей. Тому у цьому дослідженні розглядається проблематика інформаційної війни та її протидії на державному рівні.

Об'єктом дослідження є інформаційна війна як засіб впливу в сучасному інформаційному просторі у вигляді різноманітних інформаційно-комунікаційних форм протистояння на території України.

Предметом дослідження є зміст та особливості ведення інформаційного протиборства в сучасному інформаційному суспільстві України.

Мета дослідження – виявлення сутності інформаційної війни та комунікаційних механізмів реалізації інформаційного впливу як засобу маніпулювання в національному інформаційному просторі і визначення методів інформаційного протиборства у безпековому просторі України.

Реалізація мети передбачає послідовне вирішення сформульованих **завдань**:

- проаналізувати зміст і особливості реалізації інформаційної війни;
- розкрити особливості ведення інформаційної війни;
- простежити специфіку виникнення та розвиток інформаційних воєн в історичній ретроспективі;
- виявити особливості реалізації тактики інформаційної війни проти України;
- охарактеризувати сучасне законодавство України щодо питання врегулювання інформаційного протиборства;
- виокремити проблеми інформаційного протиборства України;
- запропонувати рекомендації щодо врегулювання питань інформаційного протиборства.

Методи дослідження. У процесі дослідження сформульованої мети та вирішення завдань запропонованих у роботі, використано комплекс методів. На різних етапах дослідження під час вирішення поставлених завдань використано аналітичний метод роботи з джерелами інформації та проведення всебічного аналізу проблеми. Методи пошуку і систематизації наукової інформації використано у процесі визначення стану розробленості наукової проблеми, а документальний метод дозволив осмислити залучені документи як підтвердження подій і явищ. Порівняльний метод дозволив простежити феномен інформаційна війна в історичній ретроспективі та сучасних її проявах, виявляючи тенденції та особливості розвитку явища. Системний метод застосовано у вивченні специфіки функціонування та протидії інформаційній війні, що дозволило сформулювати цілісне бачення проблеми та системність бачення проблеми і шляхів її вирішення. Запропонований методологічний

комплекс дозволив розглянути поняття «інформаційної війни» більш детально, дослідити її інструментарій та базис використовуваних прийомів в атаках, ознайомитись із ситуацією в інформаційному середовищі України та запропонувати подальший розвиток законодавства в інформаційній сфері.

Наукова новизна дослідження. У магістерській кваліфікаційній роботі розкрито специфіку і запропоновано теоретичне обґрунтування питання інформаційної війни з підходу інформаційної діяльності та документаційного забезпечення управління. Всебічний аналіз проблеми дозволив показати міждисциплінарний характер у вивченні питання, який поєднує в собі філософський, управлінський, історичний, політичний, психологічний та інші аспекти. Аналіз інформаційно-комунікаційної складової інформаційної війни дозволив виявити специфіку інформаційного впливу та розвитку протиборства із залученням новітніх технічних засобів та технологій впливу. Це дозволило розкрити сутність інформаційної війни як засобу впливу, оцінити ступінь розвитку інформаційно-комунікаційних технологій поширення інформації та протиборства, виявити механізми протидії інформаційному впливу та запропонувати шляхи і засоби убезпечення від цілеспрямованого інформаційного маніпулювання з метою посилення позицій ворога на території іншої держави.

У результаті вивчення процесу розвитку інформаційної війни як сучасної технології впливу, запропоновано шляхи удосконалення безпеки держави і боротьби в інформаційному середовищі шляхом законодавчого врегулювання інформаційної національної безпеки.

Апробація одержаних результатів. Основні наукові положення і аспекти теми, результати і висновки магістерської кваліфікаційної роботи представлено у науковій статті Віснику студентського наукового товариства Донецького національного університету імені Василя Стуса (м. Вінниця, 2021); обговорені на конференціях VI Міжнародної науково-практичної конференції «Документно-інформаційні комунікації в умовах глобалізації: стан, проблеми і перспективи» (м. Полтава, 2021); Всеукраїнської науково-практичної

конференції «Прикладні аспекти сучасних міждисциплінарних досліджень» (м. Вінниця, 2021).

Структура даного дослідження підпорядкована досягненню мети і зумовлена завданнями дослідження. Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних посилань із 63 найменувань. Загальний обсяг роботи – 77 сторінок, основна частина якої 70 сторінок. Робота містить 9 рисунків, 1 таблицю.

РОЗДІЛ І
ПОНЯТТЯ «ІНФОРМАЦІЙНА ВІЙНА» ТА ЇЇ ВПЛИВ НА ІНФОРМАЦІЙНИЙ ПРОСТІР ДЕРЖАВИ

1.1 Зміст і особливості реалізації інформаційної війни

Поняття «інформаційна війна» досить широке та непросте для дослідження. Дослідники тривалий час вивчали даний феномен, генерували нові визначення, уточнювали об'єктно-предметну складову чи видозмінювали встановлені раніше трактування.

Інформаційна війна, як зазначав С. Расторгуєв, являє собою боротьбу держав із використанням інформаційних технологій, відкриті або приховані впливи інформаційних систем з метою досягнення матеріальної переваги [1]. Інформаційні впливи у даному визначенні можна тлумачити як впливи із використанням засобів, що допомагатимуть у досягненні поставлених цілей.

Науковці Р. Рудник та П. Шпига зазначають, що на сьогодні існує чотири підходи до встановлення визначення інформаційної війни:

- перший підхід визначає її як сукупність соціально-економічних, політико-правових та психологічних дій, що захоплюють інформаційний простір ворога, витискуючи його, шляхом знищення його комунікацій та засобів зв'язку;

- у другому підході поняття інформаційної війни розглядається як гостра форма протидії в рамках інформаційного простору, у якій важливого значення набуває безкомпромісність, часові межі та інтенсивність конфлікту між суперниками;

- третій підхід інтерпретує інформаційну війну як форму ведення військових дій із використанням новітніх інформаційних технологій;

- у четвертому підході інформаційна війна прирівнюється до кібернетичної війни, тобто протистояння за допомогою технічних систем [27].

У своїх роботах О. Юдін та Д. Богуш зазначають, що визначити, чи являє собою дане явище інформаційну війну, можливо лише у випадку, коли існує

певний комплексний вплив на інформаційне поле супротивника, чи передбачені певні умови для ведення дій, що виступають як самостійні чинники та можуть впливати таким чином, що конфронтуюча країна відмовиться від поставлених цілей в політичній, економічній чи іншій сфері діяльності. У такому випадку особливостями ведення інформаційної війни залишатимуться ризики та невизначеність кінцевого результату [27].

Одним з головних завдань інформаційної війни, як визначає Р. Чирва, є маніпулювання великою кількістю людей та їх дезорієнтація [1].

Також до головних завдань інформаційної війни дослідники відносять:

- здійснення руйнівного впливу на політичну силу країни шляхом послаблення її потенційних та реальних можливостей щодо забезпечення безпеки, формування труднощів для розвитку та підтримки зовнішніх зв'язків та ослаблення ролі владних органів;

- формування бездуховної атмосфери та негативного відношення до культури й історичної спадщини у населення ворога;

- маніпуляційні дії із громадською думкою та політичною системою держави противника з метою створення напруги у політичній сфері;

- дестабілізація відносин між політичними партіями та об'єднаннями з метою підбурювання конфліктних ситуацій та стимулювання недовіри населення до владних органів;

- провокація політичних, економічних, соціальних чи релігійних конфліктів;

- зниження рівня інформаційної безпеки;

- ініціювання бойкотів та страйків, масових заворушень та інших акцій протесту;

- підрив авторитету влади та країни на міжнародному рівні;

- применшення значимості відкриттів та світових досягнень в науці та перебільшення масштабів помилок;

- створення передумов політичної, економічної чи військової поразки;

- захист від інформаційно-психологічної атаки з боку противника [23].

У загальному, інформаційна війна являє собою всеохоплюючу та цілісну стратегію, що обумовлюється зростанням значення інформації в аспекті політики, управління та командування.

Інформаційну війну також можливо трактувати як таку форму конфлікту, при якій ведуться прямі напади і атаки на інформаційну систему противника.

Будь-яка інформаційна війна містить такі характерні складові:

- психологічні операції, у яких інформація існує як головний чинник порушення психологічного стану супротивника;

- електронна війна, у якій інформація спотворюється ще до того моменту як її отримає ворог;

- дезінформація має на меті надання неправдивої інформації про наявні сили та дії;

- фізичні руйнації, метою яких є вплив на складові інформаційних систем та виведення їх із працездатністю;

- заходи для безпеки, метою яких є протидія досягнення противником реальних та правдивих даних;

- прямі інформаційні атаки, у яких інформація викривлюється.

У своїй роботі «Що таке інформаційна війна» М. Лібікі визначив такі форми інформаційної війни:

1. командно-управлінська (її метою є знищення каналів зв’язку між командною частиною та виконавцем завдань).

2. психологічна (пропагандистська обробка населення за допомогою інформаційних атак та його деморалізація).

3. розвідувальна (збирання та зберігання інформаційного ресурсу).

4. економічна (блокування інформаційних каналів).

5. хакерська (диверсії та атаки проти супротивника за допомогою спеціальних програм).

6. електронна (атаки на станції радіозв’язку, радари та комп’ютерні мережі)

7. кібервійна [5].

Ключовим елементом, також, вважається теоретична модель інформаційної війни, яка визначається, як система інформаційних впливів між соціальними групами, які спрямовані на отримання переваг в економічних, політичних та військових протистояннях.

Інформаційна війна має в своїй основі три складових: хай-тек, хай-сенсоро та хай-х'юм. Кожна із цих складових характеризується власним технологічним наповненням.

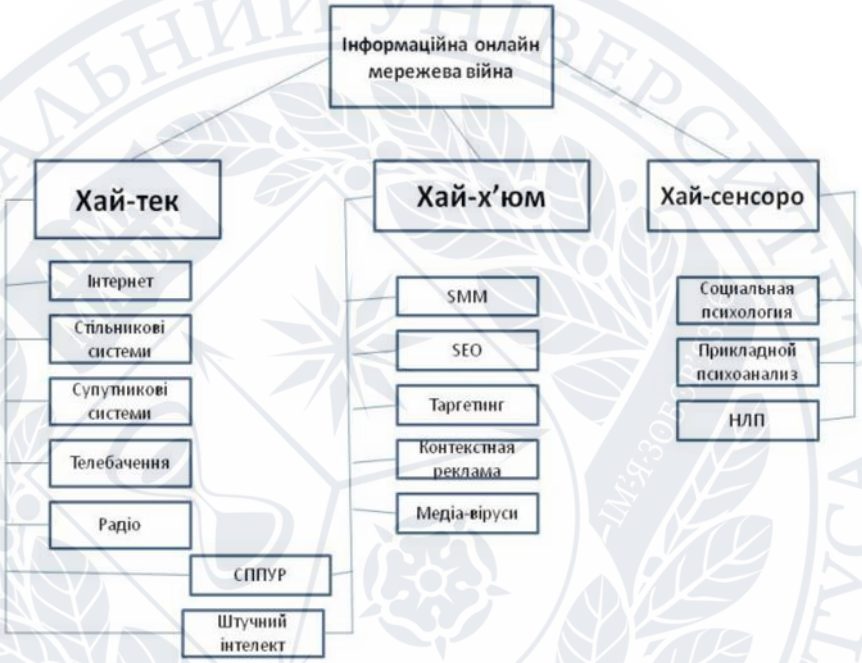

Рисунок 1.1 – Модель інформаційної війни

Хай-тек характеризується як сучасна цифрова комунікаційна технологія, яка охоплює телебачення, Інтернет, радіо та сучасні засоби зв'язку до яких відносять смартфони, планшети, стаціонарні комп'ютери тощо.

Класичне телебачення, як ефірне так й цифрове, в контексті інформаційної війни визначається, як технологія трансляції звуку та зображення за допомогою кодування сигналів із застосуванням каналів за стандартами MPEG.

Радіо, в аспекті сучасних ЗМІ, можливо розглядати в аналоговому та цифровому форматі, що визначається, як технологія передачі та дешифрування сигналів у цифровому форматі із використанням електромагнітних хвиль у радіодіапазоні.

Інтернет являє собою систему комп'ютерних мереж, що об'єднані між собою та виконують функцію трансляції та зберігання інформації. На основі Інтернету формуються поштові системи, сервери для зберігання даних та нові формати радіо й телебачення.

Інтернет-телебачення відрізняється від традиційного телебачення та містить в собі міжмережевий протокол – систему, сформовану на базі двосторонньої цифрової передачі сигналів за допомогою Інтернету та широкополосного підключення.

Інтернет-радіо являє собою групу технологій передачі та трансляції сигналів аудіо за допомогою інтернет-з'єднання для здійснення трансляції.

Месенджери – системи миттєвого з'єднання. До них відносять Viber, Telegram, WhatsApp, Skype, Facebook та інші.

Хай-х'юм, в контексті інформаційної війни, означає сучасні соціально-гуманітарні технології для створення, зберігання та розповсюдження інформації. Прикладами можуть бути SEO, SMM, таргетингова та контекстна реклама тощо.

У даному аспекті, SEO являє собою комплекс заходів із оптимізації та підвищення позицій сайту в пошукових системах.

SMM являє собою комплекс заходів, які спрямовані на просування окремого контенту чи сторінки в соціальних мережах.

Таргетингова реклама являє собою певний рекламний механізм, який дозволяє виокремлювати зі всієї аудиторії соціальної мережі лише ту частину, яка відповідає необхідним вимогам.

Контекстна реклама являє собою методи та засоби розміщення інформації, яка направлена на зміст інтернет-ресурсу та представлена у вигляді банеру або текстового повідомлення.

Хай-сенсоро, в контексті інформаційної війни, означає сучасні психологічні технології, які дають можливість керувати та врегульовувати соціально-комунікаційні процеси в групах чи на рівні окремих індивідів. Прикладний психоаналіз, нейро-лінгвістичне програмування та соціальна психологія вважаються типовими прикладами хай-сенсоро.

Прикладний психоаналіз є частиною психології, у якій розкривається практика використання концепцій за допомогою яких буде можливим досягнення повного розуміння людської природи та суспільства.

Нейро-лінгвістичне програмування (НЛП) – технологія моделювання поведінки індивіда, у вербальному та невербальному контексті, із використанням форм мовлення, рухів тіла та пам'яті.

Соціальна психологія є частиною психології, яка орієнтована на вивчення принципів діяльності людей та їх взаємодії у групах.

Головною складовою інформаційної війни є інформаційний процес, який характеризується як діяльність із формування, накопичення, зберігання та поширення інформації тематичного характеру [6].

Будь-яка інформаційна війна складається із інформації та комунікації. Інформація, у даному контексті, розуміється як певні відомості про навколишнє середовище людини, а комунікація як процес передачі інформації [63].

У різні часи інформаційний процес містив у собі ті технології, які були у дану епоху. Це відображалось на ході та особливостях інформаційних протистоянь.

Кожна з таких технологій в історичному аспекті мала назву інформаційного вибуху чи інформаційної революції.

Під інформаційною революцією розуміється докорінна зміна методів та засобів створення, зберігання та поширення інформації. Під інформаційним вибухом розуміється значне прискорення процесів створення, зберігання та поширення цієї інформації. Типовим прикладом такого прискорення є винайдення друкарства та Інтернету [6].

Усі інформаційні процеси завжди відбуваються у площині, яка узагальнено називається інформаційним полем. Останнє трактується як певний соціальний або географічний простір, у рамках якого відбувається комунікація, де учасники обмінюються інформацією.

Суб'єкти інформаційних процесів є складовими інформаційного поля та характеризуються як індивідууми, соціальні групи та учасники комунікації.

Об’єкти інформаційних процесів являють собою сукупність інформації, яка отримується в ході комунікації. Об’єкти та суб’єкти інформаційного процесу взаємодіють між собою за допомогою діалогових та лінійних моделей процесу комунікації.

Лінійна модель, в даному контексті, означає однобічний та цілеспрямований процес обміну інформацією між автором даних та отримувачем. Ця модель складається із декількох етапів, де на першому у свідомості автора формується думка, яку він формує та перетворює на інформацію шляхом кодування, що є другим етапом. На третьому етапі сформована таким чином інформація транслюється автором чи посередником. На четвертому етапі ця інформація досягає отримувача, що її декодує, для кращого розуміння отриманих даних. На п’ятому, кінцевому, етапі ці дані обробляються отримувачем, після чого він формує власну думку з приводу наданої інформації.

У випадку, коли отримувач планує відреагувати на інформацію, він транслює власну думку використовуючи описаний вище механізм. Такий процес обміну інформацією називається циклічною моделлю комунікації та передбачає взаємообмін даними в ході якого автор та отримувач поступово змінюються.

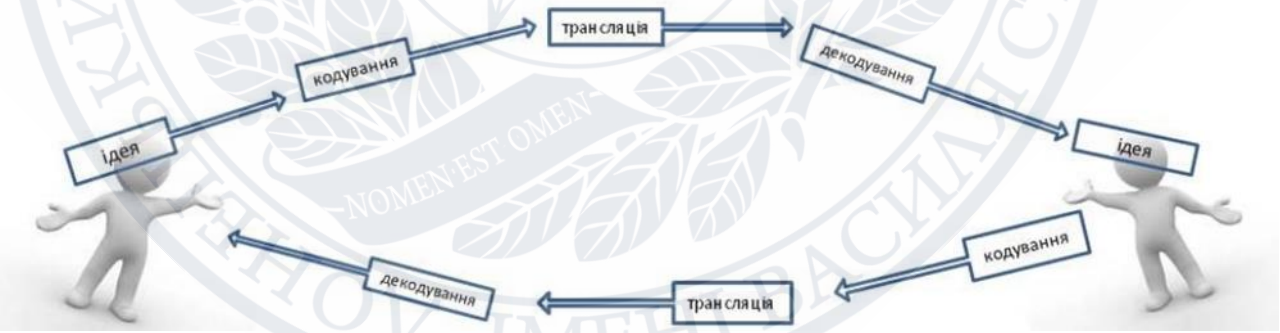

Рисунок 1.2 – Базовий комунікаційний процес

Головними сферами використання інформаційної війни є політична, економічна та військова сфери. Боротьба у них має циклічний або лінійний обмін інформацією, що може нанести шкоду отримувачу та надати певні переваги автору. Саме це є сутністю сучасної інформаційної війни.

Маніпуляції є основою інформаційної боротьби та засобом психологічного впливу, що використовується для прихованого впливу на психіку жертви для досягнення поставлених цілей.

Головним елементом інформаційної боротьби є інформаційна зброя. Її необхідно трактувати як сукупність організаційних та технічних впливів на інформаційну систему та системи автоматичного керування, які передбачають використання таких систем та засобів:

- викривлення, розкриття, знищення, формування неправдивої інформації;
- подолання засобів захисту;
- обмеження чи розширення доступності інформації;
- протидія технічним засобам та дезорганізація комп'ютерних систем;
- керування інформаційними системами [7].

Інформаційна зброя має вигляд програмних та апаратно-програмних систем, які легко замаскувати під системи захисту, діяльність яких може бути анонімною без оголошення війни. Такі системи можуть бути наділені такими властивостями як варіативність побудови та використання, універсальність у застосуванні та радикальність дії в контексті заподіяння максимальної шкоди.

Мішенню для інформаційної зброї є національна інформаційна структура та засоби глобальної інформаційної структури. Також мішенями можуть бути засоби масової інформації, засоби зв'язку, транспорт та енергетика, виробництво, освіта та наука тощо.

На сьогодні використовуються такі види інформаційної зброї:

- апаратні закладки (чіпи, ВІС тощо);
- програмні закладки (програмні платформи, логічні та часові бомби, троянські коні, програмне забезпечення);
- віруси (орієнтовані на локальні та глобальні мережі).

Одним з прикладів вдалого використання інформаційної зброї можна назвати операцію «Буря в пустелі», яка проводилася США на території Близького Сходу. Метою проведення операції було використання прийому психологічного впливу американськими військовими із вилученням

повідомлень, у яких протилежна сторона виправдовувала свої дії. Дана операція вважається першою в історії війною в прямій трансляції за допомогою телезв'язку [8].

Головною метою будь-якої інформаційної атаки є одержання переваг у реальній військовій чи економічній боротьбі [9].

Традиційним інструментом у інформаційній війні є медіа, які здійснюють роль посередника при трансляції думок у вигляді повідомлень, між автором та одержувачем. Під медіа розуміються канали зв'язку, засоби зберігання, поширення та трансляції інформації. До них можна віднести будь-який інформаційний носій, який виконує вищезазначені функції. Поряд із медіа існує поняття мас-медіа, які часто ототожнюють. Однак мас-медіа означає більш конкретну технологію трансляції джерелом широкому загалу, що обмежується інформаційним полем, у якому мас-медіа використовуються [10].

Усі мас-медіа за специфікою їх функціонування можна умовно розподілити на такі групи:

- друкована преса;
- аудіовізуальні;
- засоби маскультури;
- рекламно-інформаційні;
- інформаційні служби.

За географічним розповсюдженням їх розділяють на:

- місцеві;
- регіональні;
- національні;
- транснаціональні [3].

У XX ст. на світ з'явився а набув розвитку в XXI ст. новий формат інформаційної війни, який називається кібервійна. Під кібервійною розуміють певну боротьбу сторін на полі програмного забезпечення, де витягується закрита інформація та виводяться з ладу програмно-апаратне обладнання противника для

отримання значних переваг у реальних військових та економічних протистояннях.

Головними особами у такій війні є хакери та кракери. Перші займаються видобутком необхідної інформації, другі – псуванням програмно-апаратних засобів.

Кібервійну розподіляють на такі види:

- вандалізм, за якого відбувається псування сторінок в Інтернеті та зміна змісту початкового повідомлення;

- пропаганда, що являє собою поширення повідомлень для привернення уваги й підбуренні до певних дій суспільство;

- збір інформації, що необхідних для взлому сторінок окремих осіб чи організацій для отримання інформації;

- втручання в апаратно-програмне забезпечення, для здійснення атак на комп'ютерну техніку противника;

- атаки на інфраструктуру, на комп'ютери, які врегульовують діяльність державних, військових та громадських організацій [3].

Із появою технологій web 2.0 була сформована мережева війна. Остання містить в собі інформаційно-комунікаційну боротьбу в офлайн та онлайн форматах мережевих структур.

До офлайн мережевих структур відносять організації чи тимчасові об'єднання на основі спільних думок та інтересів.

До онлайн мережевих структур входять інтернет-ресурси та соціальні мережі [59].

Важливу роль у веденні інформаційної війни відіграє поняття гібридної війни. Останню трактують, як засіб протидії, що поєднує в собі набір інструментів військового, політичного та економічного характеру. По-іншому гібридну війну називають асиметричною війною, що підкреслює специфіку характеру боротьби, яка відбувається із використанням нетрадиційних стратегій та тактик ведення війни. Головною метою цієї боротьби є компенсація недостатньої кількості ресурсів чи отримання значних переваг у ході конфлікту.

Полем для використання інструментів у гібридній війні є міжнародне суспільство та населення територій противника.

Під час ведення такої війни часто використовують:

- громадські заворушення, акції протесту, демонстрації та вуличні зіткнення;

- повстання, відкриті виступи проти державної влади;

- партизанський рух;

- тероризм, масові вбивства, підрив транспорту, будівель;

- громадянську війну, військове протистояння між прихильниками відмінних між собою ідеологічних та національних груп та території однієї держави [3].

Якщо розглядати новітні інформаційні технології в аспекті зброї, то можливо дійти до висновку, що вони можуть перетворитися на катастрофу для людства, оскільки в якості інструментарію політики інформаційні війни являють собою переважання одного суспільства над іншим, шляхом обману та дезорієнтації.

1.2 Особливості ведення інформаційної війни

Інформаційний вплив на широкий загал суспільства прослідковується протягом усього ходу історії, однак окремим видом протистояння він став з XX ст., саме у той час зміцнювались засоби комунікацій. На сьогодні будь-який військовий конфлікт містить в собі інформаційно-психологічні операції. Однак такі операції мають місце не лише у воєнних діях, а й в бізнес-процесах, політичних дебатах та конкуренції між державами. Враховуючи те, що інформаційна боротьба являє собою невід’ємну складову сучасних відносин на різних рівнях, проблема її дослідження є важливим чинником у розумінні процесів розвитку суспільства.

Інтенсивність застосування тих чи інших засобів впливу зумовлена стрімким розвитком технологій. Методи інформаційного впливу, на перший

погляд, не змінювались протягом століть, однак технології впливу та засоби трансляції інформації зазнали значних змін. Весь історичний розвиток інформаційної боротьби можливо поділити на декілька етапів [17].

Античність, Середньовіччя та Новий час можливо об'єднати в один період, впродовж якого методи та форми інформаційного протиборства в основі своїй залишались незмінними [17].

Усі яскраво виражені модифікації можливо помітити у другому історичному періоді розвитку інформаційної боротьби. У рамках цього періоду відбулись національні революції, які внесли серйозні зміни в трактуваннях інформаційної війни та зростання важливості її методів та засобів. Вказаний період розвитку інформаційної боротьби визначається зростанням ролі цього протиборства як допоміжного засобу при врегулюванні військових, політичних чи економічних питань [17].

Третій етап характеризується піднесенням значення інформаційного впливу на населення. З ролі допоміжного засобу управління, інформаційна боротьба переходить до незалежного та основного інструменту для досягнення поставленої задачі. Відповідно до цього відбуваються зміну й у рівні наукового розвитку та матеріально-технічному забезпеченні інформаційного протиборства [17].

Сучасні інформаційні технології базуються на досягненнях серед засобів зв'язку та комп'ютерної техніки. Стрімкий розвиток останньої став поштовхом до формування «інформаційного суспільства».

Серед вітчизняних вчених, які досліджують феномен інформаційного протиборства варто виділити Г. Почепцова, І. Шаравова, В. Петрова, Я. Жаркова, О. Литвиненка та інших [17].

Значною кількістю досліджень проблематики інформаційної війни займались зарубіжні науковці.

Розглядаючи роль та зміст інформації у суспільстві, М. Мак-Люен висловлював свою думку про те, що тотальна війна – це війна, у якій використовується інформація. Саме він першим серед науковців говорив про те,

що економічні зв'язки та комунікації на сьогодні набувають форми взаємообміну даними. Боротьба за капітал та ринки збуту відходять на другий план, поступаючись місцем доступності інформаційних ресурсів, спонукаючи тим самим до збільшення кількості військових дій в інформаційному просторі за допомогою інформаційної зброї [17].

Ще у біблійній легенді про Гедеона згадувалось про використання залякування в якості зброї. У цій легенді воєначальник настільки залякав свого ворога, що той у паніці напав на свої ж війська. Серед видатних постатей в історії, які успішно використовували методи впливу був і Юлій Цезар. Перед кожною військовою битвою він поширював спеціальні звернення та проводив театралізовані вистави, отримуючи тим самим всенародну підтримку. У часи феодалізму відбувалась постійна боротьба з «єрессю», що є яскравим прикладом інформаційного тиску. У наполеонівській пропаганді також наявні риси психологічної війни. Так, наприклад, він часто фальсифікував хід історичних подій, постійно стверджував про необхідність єдності всередині держави, замовчував неприємні новини та висвітлював вигідні для країни, викривлював повідомлення представників ЗМІ ворога, намагався висміювати противника та звинувачував його у своїх власних злочинах. Наполеон стверджував про те, що декілька газет можуть завдати ворогові більшої шкоди, аніж величезна армія [4].

Особливої ролі інформаційне протистояння набуло вже у XX ст., у часи, коли газети, радіо та телебачення ставали головними засобами поширення інформації у масових масштабах. У 20-х роках XX ст. США поширювали інформаційні повідомлення на території своїх традиційних інтересів, такі як Латинська Америка та Великобританія. Німеччина, яка вимагала повторного розгляду умов Версальського миру – на жителів Померанії, Чехії та Польщі. У 30-х роках XX ст. інформаційні протистояння перестають грати роль додатку до збройної боротьби та виокремлюються у самостійне явище, як це сталось у часи німецько-австрійської радіовійни 1933-1934 рр. Ще тоді набуло широкого поширення визначення «інформаційного агресора» [4].

Незважаючи на це, саме поняття «інформаційної війни» та споріднені з ним визначення почали осмислюватись пізніше.

Частина вчених вважає, що дане поняття було введене в Китаї в 1985 році. В основу його було покладено теоретичні засади давньокитайського діяча Сунь Цзи. Він першим визначив важливість інформаційного впливу на ворога. У своїй роботі «Трактат про військове мистецтво» він писав про те, що підкорити ворога здобувши перемогу у боях – не вершина мистецтва, а перемогти без жодної битви є його вінцем.

Одним з найпотужніших засобів впливу, що був винайдений у Стародавньому Китаї є стратагеми, якими користуються досі. Під ними розуміють формування стратегічного плану, що передбачатиме використання пасток.

У вищезазначеному трактаті Сунь Цзи писав, що будь-яка війна – це дорога брехні, а тому:

- необхідно переконати ворога у тому, що ти щось не можеш, навіть якщо ти це можеш;
- навіть якщо ти знаходишся близько – варто показати що ти далеко;
- необхідно заманювати ворога вигодою;
- потрібно руйнувати душевну рівновагу противника;
- якщо ворог сильніший за тебе – ухиляйся;
- якщо ворог ще готовий боротись – стоми його;
- необхідно сіяти розбрат у лавах ворога;
- нападати на ворога варто тоді, коли він цього не чекає.

Поряд із цим, існує думка, що «психологічна війна» вперше була визначена британським істориком Дж. Фуллером у 1920 році. Після нього «естафету» підхопили американці, які дали власне визначення у 1940 році. Визначення «психологічної операції» вперше застосував Е. Захаріас у своїх роботах. А з 1957 року у своїх офіційних документах їх почали використовувати американські дипломати. Саме психологічні операції дали змогу застосовувати необхідний інструментарій у випадках, коли відсутня широкомасштабна військова боротьба.

Даний інструментарій можливо використовувати не лише по відношенню до ворогів, а й по відношенню до союзників та нейтральних країн [4].

Термін «інформаційних операцій», що використовує НАТО, передбачає їх використання навіть при відсутності будь-яких військових дій. Прикладом можуть слугувати миротворчі операції. Однак, якщо у випадку з воєнними діями зміна навколишнього середовища має сталий характер, то у випадку із мирними операціями стан оточуючого середовища має динамічний розвиток.

Інформаційні операції у різні часи привертали увагу владних та військових діячів. Навчання у цій сфері в США розпочалось у 1967 році з відповідного курсу в Школі спецоперацій повітряних збройних сил. Однак у наступному 1968 році проєкт було закрито через відсутність повного фінансування. В 1974 році курс було відновлено, а навчання стратегії, тактиці та методиці психологічних операцій продовжили військові офіцери [18].

Якій би країні не приписували першість у встановленні понять «психологічна війна» та «психологічна операція» історія їх розвитку має набагато довше коріння. Основою для формування та корегування інформаційних впливів стала пропаганда, а її трактування з’явилось набагато пізніше самого визначення. Уперше «пропаганду» застосували у 1622 році в назві інституції, часи заснування папою Урбаном VIII конгрегації пропаганди у формі комісій кардиналів.

Так, французький психолог Жак Еллюля запропонував розподіл пропаганди на вертикальну та горизонтальну. Де вертикальна пропаганда означала класичний варіант звичної нам пропаганди, де інформаційний потік рухається згори до низу [18].

Горизонтальна пропаганда являла собою винахід та реалізовувалась у певній соціальній групі. У ній всі учасники мали однакові можливості та не виокремлювався лідер. За такої пропаганди інформація сприймалась із більшою довірою, на відміну від вертикальної.

У свою чергу горизонтальна пропаганда розподілялась на китайську та американську. У китайській пропаганді від учасників груп не вимагали

озвучення своїх думок. У американському варіанті ж навпаки, від членів групи вимагалась максимальна активність.

Якщо у випадку із вертикальною пропагандою необхідний апарат масових комунікацій, то при горизонтальній – самоорганізація людей. У своїх роботах Ж. Еллюля описував пропаганду як спеціальну форму існування думок та вважав її ірраціональною. Також він розрізняв соціологічну та політичну пропаганду. Де політична пропаганда складалась із технік впливу на суспільство зі сторони держави, а соціологічна – стиль життя та тип поведінки, які є нормою для країни. Останню він вважав важчою для розуміння, оскільки вона є непомітною, на відміну від політичної, яка має цілеспрямований та планомірний характер. Розподіл пропаганди на вертикальну та горизонтальну, соціологічну та політичну здається, на перший погляд, умовним, однак між ними є значні відмінності. Вертикальна та горизонтальна пропаганда описують напрямок комунікації, відображаючи ієрархічну структуру суспільства, політична та соціальна – канали розповсюдження інформації [18].

Серед фахівців існує думка, що пропаганда приречена на провал, коли вона зовні має вигляд пропаганди.

Якщо використовувати принцип скритності в якості ознаки ефективності, то «переможцем» серед пропаганд буде горизонтальна, оскільки вона не взаємодіє із зовнішнім, по відношенню до групи, середовищем. У другому розподілі «переможцем» можна вважати соціологічну пропаганду, оскільки окрім Ж. Еллюля про неї ніхто не говорив [19].

Більшість дослідників пропаганди досить часто висвітлювали її у негативному руслі, спотворюючи її особливості. В контексті обмеження джерел інформації та авторитарному режимі пропаганда дійсно має деструктивні риси. Однак варто зазначити, що вона не завжди розповсюджує упереджені позиції. Існують і позитивні моменти, за яких відбувається поширення демократичних принципів та цінностей єдності суспільства.

Варто зазначити, що діалоги не завжди мають місце в процесі комунікації. Так, наприклад, завданням влади, у політичному контексті, може бути

розповсюдження інформації без стимулювання зворотного зв'язку зі сторони громадян. Такий перебіг подій можливий, коли при наявності певного конфлікту відсутня інформація, що дозволятиме зберегти стабільність та запобігти панічних настоїв серед населення. Однак, досить часто, на фоні права населення на поінформованість, ЗМІ можуть дестабілізувати ситуацію та підбурювати політичні пристрасті. У політичному житті досить часто бувають випадки недоцільності врахування інформаційних потреб населення. У схожих випадках використання пропаганди є доцільним.

Чутки є специфічною технологією інформаційного протиборства. Більшість фахівців зазначають, що світ сформувався на чутках, на них тримається та ними живе. Дослідники пояснюють це твердження тим, що люди при зустрічі із новим та невідомим, шукають пояснення цьому для зняття психологічної напруги. Однак, трактування нових фактів досить часто здійснюється неправильно, що й породжує чутки [4].

У зв'язку із цим виникає питання, що саме провокує поширення чуток? Основною причиною появи чуток є відсутність інформації чи вона не в достатній та повній кількості. В таких умовах недостатньої кількості інформації у офіційних джерелах формуються чутки. Науковець Г. Почепцов зазначав, що недостача інформації компенсується чутками. Він називав це явище «ситуацією чуток» та говорив про можливість існування закону, що звучить як: якщо інформації немає в офіційних джерелах, вона з'явиться у неофіційних [20].

Появі чуток сприяє поширення в маси недостовірної та суперечливої інформації щодо подій, які проходять в умовах недовірливості до джерел даних.

На думку психологів, головною причиною появи чуток є емоційна складова, а компенсація такої складової перекривається чутками. Нестабільна економічна та політична ситуація в країні можуть створити сприятливі умови для появи та розвитку чуток.

Некомпетентність населення з різних питань також підбурює появу чуток, оскільки люди можуть не розуміти в повній мірі проблеми, вони починають

вигадувати свої варіанти перебігу подій, доповнюючи реальні чи повністю їх викривлюючи.

Свідоме створення чуток з метою поширення певних думок серед громадськості називають інформаційною зброєю. Перші випадки використання чуток в особистих інтересах були ще у давні часи. А вже у XX ст. їх досить активно застосовували у політичній та економічній боротьбі серед держав.

Дослідники виділяють декілька типів чуток відповідно до їх інформаційної характеристики.

Рисунок 1.3 – Типи чуток

Одним з головних прийомів ведення інформаційного протиборства є провокація. Вона являє собою специфічну інформаційну операцію, що спонукає ворога застосовувати невигідну для себе стратегію та тактику. Для використання провокації необхідно прораховувати наперед величезну кількість програшних варіантів ведення дій суперника.

Ще однією формою інформаційного впливу, основою якої є обман противника для досягнення поставленої мети є дезінформація. Історична практика вказує на те, що існує безліч методів ведення заходів із використанням дезінформації, як в позитивному, так й в негативному контексті. Вибір того чи іншого методу залежить від обстановки та перебігу подій. У світовій практиці найчастіше використовують такі методи:

- висвітлення фактів у залежності від тенденцій, що полягають у висвітленні необхідних фактів за допомогою правдивих даних, які актуальні у певний проміжок часу.

- «мінування» термінами, що полягає у спотворенні суті базових термінів, які мають світоглядний та оперативний характер.

У загальному вигляді дезінформацію можливо використовувати шляхом застосування ЗМІ, власних інформаційних агентств та формування враження успішної розвідки іноземних партнерів.

Психологічний тиск являє собою вплив на психіку населення методом залякування для спонукання їх до певних дій. До методів психологічного тиску відносять:

- донесення до населення даних щодо реальних чи вигаданих небезпек;
- прогнозування убивств, репресій тощо;
- шантажування;
- здійснення масових отруєнь, підпалів та проведення інших терористичних дій.

Диверсифікація свідомості є ще однією технікою інформаційного впливу. Вона являє собою розпорошення уваги владної верхівки держави на штучно створені проблеми та відволікає їх від першочергових завдань економічного та політичного розвитку. До методів диверсифікації відносять:

- дестабілізація середовища в країні чи її окремому регіоні;
- активізація акцій проти політичного плану владної верхівки держави;
- ініціювання скандальних кампаній та використання міжнародних санкцій.

В інформаційній боротьбі зазвичай використовуються способи та форми тиску. До них відносять: провокації, маніпуляції, блеф, шахрайство, політичні ігри, дезінформацію, чутки та містифікацію даних. Даний список використовуваних способів не є повним [21].

Інформаційна війна є невід’ємною частиною політичних відносин та виступає одним з головних інструментів примусу, пронизуючи форми політичної та економічної боротьби, зазначав О. Горбенко [22]. Інформаційна боротьба вже не обмежується впливом на суспільство, а фокусується на суспільну свідомість держав та системи прийняття рішень у різних сферах

держави. Політичні лідери постійно обмінюються інформаційними впливами у стані жорстокого конфлікту [22].

Застосування інформації в якості зброї у боротьбі з супротивником має довготривалу історію, а в сучасному інформаційному суспільстві набуває першочергового значення як інструменту, що здатний впливати на величезну аудиторію. Більшість форм та методів інформаційного впливу досить давні та широковідомі, однак поряд із цим вони залишаються досить дієвими. Сучасні інформаційні технології надають можливість використання необхідної державі інформації, розповсюджуючи її серед цільових груп як в середині держави, так і в міжнародному соціумі [4].

Будь-яку інформаційну атаку можливо розділити на декілька етапів:

- формування контенту;
- поширення інформації на певному майданчику в Інтернеті;
- моніторинг перебігу подій та аналіз результатів.

До найбільш ефективних прийомів інформаційних атак відносять:

- дезінформація;
- залякування;
- схематизм;
- глузування;
- фальшування;
- вклинювання.

Дезінформація використовується у випадку, коли необхідно виграти час та отримати перемогу надаючи хибну інформацію. Прикладом можуть слугувати події після Євромайдану. У той час поширювалась фейкова інформація про те, що із заробітної платні жителів Донецької та Луганської областей вираховуватиметься відсоток на відновлення території Майдану. Дана інформація поширювалась через неформальні канали комунікації, що пришвидшувало поширення інформації.

Залякування використовують у випадках, коли необхідно відвернути увагу від реальних намірів ворога. При залякування інформація, що транслюється, має

на меті дезорієнтацію та формування у населення тривожних настроїв. Прикладом можуть слугувати події на Сході України та в Криму, коли активно поширювалась інформація про те, що українські націоналістичні організації готують терористичні атаки на російськомовне населення. Такі дані сформували у свідомості населення уявлення, що необхідно відокремлюватись від України, оскільки їх дискредитують. Окрім поширення вищезазначеної інформації у ЗМІ також поширювали відео-ролики, що містили постановочні кадри за участю вдаваних українських націоналістів, які штурмували будинки та підпалювали авто, тероризуючи місцеве російськомовне населення. Особлива роль надавалась фейковим свідкам злочинів Національної гвардії чи «Правого сектору», що здійснювали жорстокі правопорушення.

Для підвищення рівня якості та швидкості сприйняття інформації суспільством використовують схематизацію, за якої дані подаються у графічно-кількісному вигляді та доступні цільовим групам на які вони націлені. Інформація, що подається у такому вигляді, містить в собі образно-символьний принцип, що є найбільш ефективним у розрізі промоцій чи ідеологічних концепцій.

Під час формування плану ведення традиційної офлайнової війни глузування виступає нейтралізатором уявлень що до реальних можливостей ворога. У цьому випадку противника висвітлюють у комічному світлі, що нейтралізує побоювання та страх у населення.

Для посилення ефекту від інформаційної атаки використовують вклинювання, що передбачає додавання даних та корекцію повідомлень противника у необхідному руслі.

Прикладом можуть слугувати фейкове відео, де висвітлюють зникнення хасида, який перебував на той момент в Умані на святкуванні Нового року. У цьому відео показано як, начебто, військові катують викраденого хасида [22].

У контексті соціальних мереж вклинювання використовують для подачі прихованих меседжів на фоні повідомлень у ЗМІ. При цьому у якості основи повідомлення використовується візуальний матеріал, який доповнюється

текстовою частиною, у якій концентрується основний зміст. Для цільових груп, у яких основна частина людей не має критичного мислення, такий підхід є досить дієвим. Так, наприклад, на основі повідомлень у білоруських ЗМІ про епідемію у ДНР та ЛНР українськими бійцями було створено меседж, що мав поширювати панічні настрої серед населення, яке підтримувало Росію. Такий прийом використовувався й з протилежного боку, де в основі повідомлення був відеоролик з виступом Р. Лижичко, який висвітлював події на окупованих територіях Донбасу. Головною метою цього повідомлення було застосування авторитетної думки відомого лідера для посилення ефекту впливу та приховання реальних задумів.

Метод фальшування використовується протягом усього часу інформаційної війни, яку веде РФ. У ньому інформація викривлюється та за основу беруться інші події. Так, наприклад, блогер із «ДНР» на своїй сторінці опубліковував фото з подій в Ізраїлі, видаючи його за фото з подій в Донецьку. Подібні практики досить часто використовуються представниками ЗМІ фейкових республік, де інформація спотворюється, а матеріали з інших джерел підкріплюються власними дописами.

Інтегроване маніпулювання використовувалось у меседжах відомого інформаційного телеканалу «1+1» та їх заголовках до новин, що гіперболізували зміст повідомлення.

Прикладом маніпулювання можуть бути повідомлення в газеті «Комсомольська правда», де подавалась фейкова інформація про відвідини Москви послом США. У цьому меседжі посол, начебто, виступав із акцією протесту у ролі духовного лідера. Для висвітлення інформації за основу було взяте змонтоване фото цього посла на фоні акції, але в іншому місці [3].

Інформаційний процес при стратегічному плануванні містить декілька рівнів.

Стратегія – перший рівень. На ньому зазначаються базові напрями діяльності та умови комунікаційних процесів. На початковому етапі визначається мета, що може мати вигляд:

- консолідації. Дане поняття являє собою необхідність сприяння поєднанню окремих груп та організація для досягнення певних цілей. Такі цілі можуть мати місце у ситуаціях, коли необхідно об'єднати населення в умовах військової агресії чи при протидії внутрішнім силам для вирішення економічних або соціальних проблем. Прикладом у цьому випадку може слугувати ситуація у 2014-2015 рр., де мала місце російська агресія. У цьому випадку використовувалась консолідація, яка переважно мала стихійний характер. У ході агресії громадськість одразу окреслила свої пріоритети у соціальних мережах, сформувавши волонтерський рух. Об'єднавшись навколо українських цінностей та національної символіки. Ініціаторами даного руху стали окремі користувачі у соціальних мережах, які досить швидко згуртували суспільство для обміну інформацією та веденні волонтерських справ.

- заспокоєння. Воно характеризується як потреба у зменшенні суспільної агресії та незадоволення населення й цільових груп. Прикладом можемо слугувати економічна криза 2014-2015 рр. за якої значно зріс настрій протесту населення України. За тих обставин зовнішній противник скористався ситуацією та використав гібридну війну штучно створивши кризову ситуацію, яка призвела до росту агресії в суспільстві. Головною тезою була громадянська війна в Україні. Натомість українське суспільство знаходилось на інстинктивному рівні, де блогери поширювали певні матеріали у яких вказувались перспективи розвитку, які б сприяли формуванню патріотизму у населення.

- залякування. Дане поняття характеризується викликами невпевненості у суспільстві по відношенню до загроз. До залякування вдаються у випадку необхідності призупинення розвитку процесів політичного чи економічного розвитку. Це є ознакою прихованої психологічної агресії.

- невдоволення. Воно необхідне для виведення з рівноваги населення та груп людей та намаганні викликати дискомфорт щодо існуючих обставин.

- протести. Являють собою публічні дії активних представників населення націлених на протидію окремим особам чи ситуаціям. За використання протестів

відбуваються організовані дії, які можуть призвести до знищення соціальних інститутів, усуненні осіб від керівництва тощо [3].

До стратегічного рівня можливо також віднести формування завдання, яке б конкретизувало та корегувало шляхи досягнення поставленої мети. Стандартними завданнями, в контексті SMM-комунікації, вважаються такі:

- формування контенту, що створюється у вигляді інформаційного повідомлення за певною тематикою. Таке повідомлення може містити текстовий матеріал, фото, відео, аудіо та поширюватись за допомогою соціальних мереж в Інтернеті.

- розповсюдження контенту, що спрямоване на поширення інформації серед конкретних цільових груп чи окремих персон.

- збір контенту для аналізу та систематизації інформації з метою отримання уявлення про перебір подій чи реакцій населення на певні дані.

Після постановки завдання необхідно визначати цільові групи для встановлення комунікації. Виділяють такі цільові групи:

- за статтю;

- віком;

- соціальним положенням;

- ситуативний розподіл;

- персоналізація.

Варто також враховувати зміст та характеристику меседжів, які спрямовані на цільові групи. Меседжі розподіляють за характером:

- на ті, що спрямовані закликати, спонукати до певних дій;

- на ті, що фіксують перебір подій, стан речей та констатують факти.

Тактика – другий рівень. На ньому визначається інструментарій, шляхи досягнення поставленої мети та канали комунікації.

У роботі з соціальними мережами каналами комунікації можуть бути: Instagram, Facebook, VKontakte тощо.

Наступним кроком визначаються основні засоби робити, до яких відносять:

- роботу на інших майданчиках, на яких розміщують свій власний контент чи збирають інформацію. Такий підхід використовується у випадку, коли джерело поширення контенту необхідно приховати, а при його розповсюдженні застосовується «партизанський» маркетинг.

- роботу на персональних майданчиках, де розміщується контент, що спрямований на залучення цільової групи до взаємодії. У цьому випадку у соціальних мережах формуються тематичні сторінки та акаунти відповідно до інтересів цільових груп чи окремих персон.

- поєднання персональних та чужих майданчиків, що дають змогу проводити складні комунікаційні операції в межах цільових груп [3].

Отже, інформаційний вплив на свідомість суспільства в історичному аспекті постійно існував, однак виділитись в окремий вид боротьби він зміг лише у XX ст., саме у той час зміцнювались засоби комунікацій. Будь-який військовий конфлікт на сьогоднішній день не обходиться без інформаційно-психологічних операцій. Хоча такі операції присутні не лише у воєнних діях, а й в бізнес-процесах, політичних дебатах та конкуренції між державами. Беручи до уваги те, що інформаційне протиборство являє собою невід'ємну складову будь-яких відносин на різних рівнях, проблема її вивчення є важливим чинником у розумінні процесів розвитку суспільства.

РОЗДІЛ ІІ
ГЕНЕЗИС ІНФОРМАЦІЙНИХ ВІЙН В ІСТОРИЧНІЙ РЕТРОСПЕКТИВІ

2.1 Інформаційні війни первісного суспільства та Античності

Ще за часів першої людини – Homo erectus, близько 3,5 млн років до н.е., існували інформаційно-комунікаційні технології, що допомагали первісному населенню організовувати свою взаємодію один з одним під час полювань, риболовлі та захисту своїх близьких. Такі комунікації мали форму вигуків, міміки, жестів й тактильної взаємодії. У подальшому історичному розвитку вигуки трансформувались, перетворившись на мову в мовленнєвому контексті. За своїм значенням мовлення є системою звукових знаків, які мають певне соціальне призначення [11].

Для першої людини мовлення відігравало важливу роль, оскільки допомагало:

- у передачі знань та вмінь;
- у координації колективних дій в ході полювань, війни;
- у пізнанні навколишнього середовища та при міжособистісних контактах.

Протягом X-V тис. до н.е. мови первісних людей починали формуватися у мовні родини, яких на сьогоднішній день налічують близько 25 по всьому світу.

Другим, але не менш важливим, винаходом в аспекті розвитку інформаційно-комунікаційних технологій за часів первісного суспільства вважається мистецтво, що є графічним засобом передачі інформації та веденні комунікації. Нажаль, розвиток доісторичного мистецтва можливо відслідкувати лише за допомогою знахідок кам’яної доби, що збереглися до цих часів. Уявлення про музичну культуру первісної людини можливо сформувати завдяки музичним інструментам, а про образотворче мистецтво – завдяки наскальному живопису [11].

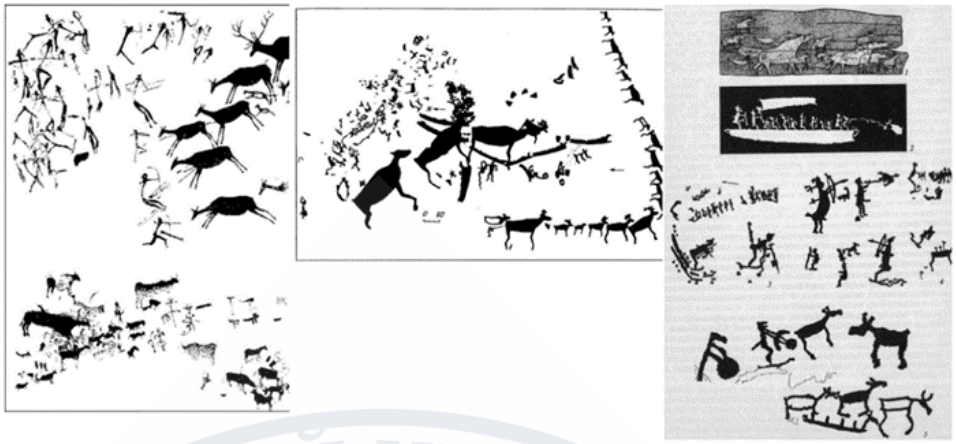

Рисунок 2.1 – Приклад перших графічних зображень

Подальший розвиток образотворчого мистецтва бере свій початок з розписів у печерах, які трансформуються у певні символи, що несуть в собі інформацію та передають її в просторі та часі.

Образні малюнки з часом перетворюються у символи, при цьому окремий символ несе в собі ту ж інформацію що й малюнок, означаючи певний об’єкт, явище чи подію [11].

Не менш важливою у контексті тематики, що розкривається, є система протописемності, яка бере свій початок у трипільській культурі. Деякий час дана писемність не була розкрита повністю, мала частина символів була розшифрована радянським археологом Б. Рибаковим [11].

Рисунок 2.2 – Трипільська символіка на кераміці

В епоху неоліту, що була наприкінці кам’яної доби, почали з’являтися перші протоміста, тваринництво та землеробство. Населення починало об’єднуватися у соціальні групи, для функціонування яких необхідне створення символьно-

образної системи, що дозволило накопичувати, зберігати та поширювати інформацію.

До основних прикладів первісної інформаційної війни можливо віднести сакральну боротьбу за допомогою магії із силами природи та на внутрішньоплемінному та міжплемінному рівнях. Така боротьба супроводжувалася магічними обрядами, залякуванням жертви, дезінформацією та приховуванням, що є прототипами інформаційних атак сучасності [12].

Інформаційний процес на базовому рівні у первісні часи містив у собі дослідження навколишнього середовища, фіксацію за допомогою мистецтва та передачу за допомогою мовлення інформацію. Головними інформаційними носіями у цьому випадку виступали твори мистецтва, побутові речі, шкіра та кістки, печери та дерева.

Виникнення протоміст призвело до необхідності створення певних правил та регламентуючих систем, які б врегульовували питання розподілу праці, прав та обов'язків жителів. За такими правилами створювалися перші міста, що були на території долини річки Інд, межиріччі Тигру та Єфрату та Нілу.

Важливим елементом державного устрою вищезгаданих міст були універсальні системи управління, які в основі своїй мали інформаційно-комунікаційні технології. Це стало поштовхом до трансформації образно-знакової системи первісних часів до ієрогліфічної системи писемності. Дана подія є типовою інформаційною революцією.

У різних містах формувалися свої власні системи писемності, однак принцип, за яким вони формувалися залишався базовим та однаковим для всіх. Рисунок трансформувався у абстрактний символ, а після перетворювався у символ із чітким змістом [12].

Подальший розвиток письмових систем призвів до появи абеткової писемності, яку винайшли фінікійці, як значно надійніший засіб для фіксації інформації для полегшення обрахунків у торговельній справі та мореплавстві. На відміну від писемності на основі ієрогліфів, яка могла складатись із декількох сотень, а то й тисяч, знаків, абеткова система складалась із 22 знаків. Вона була

більш універсальною, завдяки чому лягла в основу письмових систем епохи Античності [12].

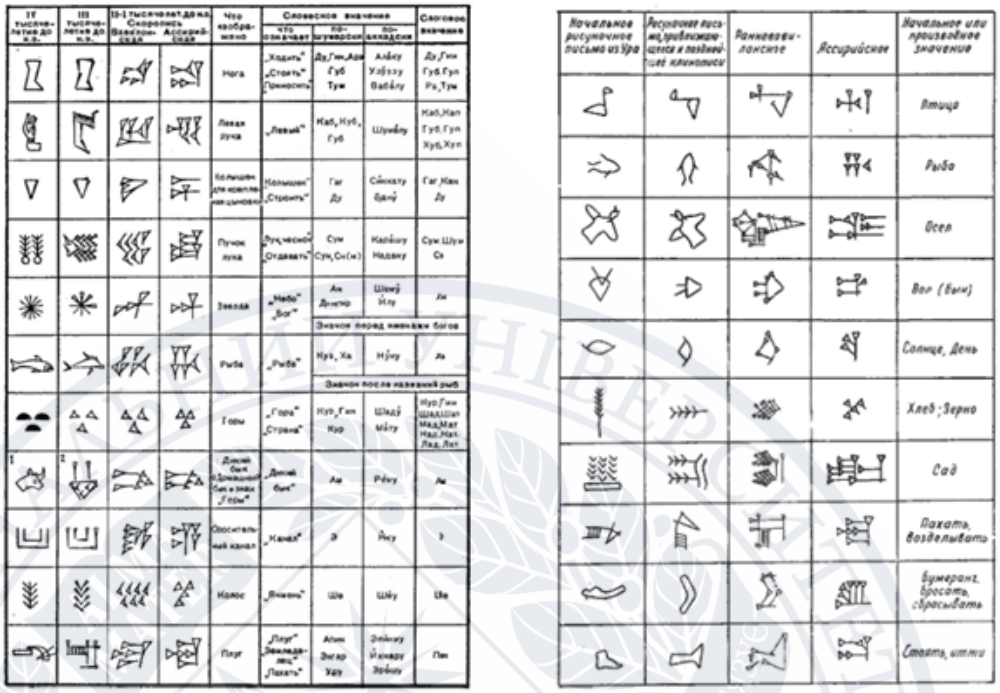

Рисунок 2.3 – Трансформація малюнка в писемність

За допомогою писемності інформаційний процес набував чіткості та конкретності. Поступово починала з’являтись можливість надійного фіксування та ефективного передавання інформації серед суспільства.

Інформаційна боротьба держав Сходу містила різноманітний характер. Вона мала місце у військових діях, політичних, релігійних та економічних процесах. Саме у ті часи людство починало системно використовувати інформаційно-комунікаційні технології. Під час своїх атак командування застосовувало методи залякування, психологічний тиск, дезінформацію, що були спрямовані проти супротивників. У політичному контексті командування держави досить часто використовувало засоби маніпуляції свідомістю населення для досягнення впевненості останніми і божественності походження їх царя. У економічному контексті використання інформаційної боротьби помітно не було. Однак існують факти, які підтверджують використання інформаційно-комунікаційних технологій під час сутичок за ресурси сировину та ринки збуту продукції.

Економіко-політичне та суспільне життя античних міст Греції та Риму вимагало поліпшення наявних інформаційно-комунікаційних технологій, які не були революційними, однак відігравали важливу роль в історії.

Одними з таких інформаційних вибухів в період античності можна вважати появу реклами. Первинна її форма функціонувала як система аудіо та письмових оголошень за допомогою глашатаїв та настінних віршів. Така комунікація мала мирний характер та виступала у вигляду оголошень, зборів чи повідомлень. Однак такі повідомлення мали характер інформаційної зброї. Так, наприклад, у Помпеї були помічені записи, які можна було трактувати як явну дискредитацію та компромат, позитивні чи негативні відгуки про якусь персону, що обиралась в міські магістрати. Також за допомогою глашатаїв у ті часи закликали до певних дій, чи висували обвинувачення певним особам [13].

Інформаційний супровід військових конфліктів та дипломатичних стосунків супроводжувався демаршів та дезінформацією, за допомогою шантажування ворожих сил. Хоча напрацювань, які б розкривали мистецтво ведення інформаційної війни у ті часи немає, але цю проблему в своїх роботах частково розкрив давньогрецький філософ Аристотель [13].

У 500 роках до н.е. військовий стратег Китаю Сунь Цзи написав роботу під назвою «Мистецтво війни», у якій згадувалося про необхідність використання елементів інформаційної війни для досягнення переваг у реальних воєнних діях. Автор описав прийоми гібридної війни:

1. Висміювання та дискредитування цінного та позитивного, що є у держави-ворога.

2. Втягування відомих діячів ворога у злочини.

3. Підрив іміджу лідерів супротивника.

4. Залучання до співпраці злочинних та негативних діячів.

5. Розпалювання суперечок та провокування конфліктних ситуацій серед жителів країни-ворога.

6. Підбурювання молоді протидіяти старому населенню.

7. Підрив міцності військ.

8. Знецінення традицій та національних цінностей держави-ворога.

9. Розбещення населення.

10. Підкупи та стимулювання корупції.

11. Протидія діяльності влади.

Інформаційні-комунікаційні технології тих часів досить активно використовувались античними політиками. Наприклад, в Давній Греції їх застосовував оратор Демосфен у ході війни з македонським царем Філіпом, що він активні атаки на грецькі міста. Такі відомі афінські політики як Солон, Фемістокл, Перикл, також активно застосовували публічні виступи, дискусійні діалоги для досягнення поставлених цілей.

В Давній Греції відбулась трансформація традиційних глашатаїв у софістів – спеціалістів в області публічних виступів та переконанні. Такі політики як Юлій Цезар, Марк Цицерон та Марк Аврелій використовували інформаційно-комунікаційні технології в ході боротьби з політичними чи зовнішніми ворогами. Сципіон Африканський був активним прибічником воєн із Карфагеном, закінчуючи кожен свій монолог перед Сенатом цитатою: «Однак Карфаген повинен бути знищеним». Даний прийом має в основі багатократне повторення однієї конкретної тези й сьогодні використовується сучасними політиками [13].

В основі сатиричних творів використовувалась інформаційна зброя, дія якої була спрямована проти конкретних діячів для маніпуляції свідомістю колективу.

Прототип першої газети з’явився у Давньому Римі. Вони мали вигляд сувоїв з актуальними новинами для населення Риму, записів подій та розміщувалися у людних місцях для покращення рівня поінформованості населення [13].

Підсумовуючи усі вищеперераховані здобутки та відкриття ранніх держав у сфері інформаційно-комунікаційних технологій варто окреслити їх ознаки. Зокрема, у первісному суспільстві базовий інформаційний процес починався з формування, фіксації та передачі інформації.

Інформаційним носієм первісної людини була шкіра та кістки тварин, посуд із глини, дерев’яні вироби та папірус. Головними прикладами інформаційних

воєн у ті часи були класичні інформаційно-психологічні операції епохи держав Сходу та Античності. Такі операції досить часто супроводжували військові дії, політичні чи релігійні конфлікти.

У часи ранніх країн Античності виготовлення контенту виділялось в окремий вид діяльності, що охоплював релігію, мистецтво, військові дії та державне управління. Створенням, формуванням та поширенням інформації займались окремі люди чи групи осіб. Досить часто це були жерці та вчені, які виступали виробниками нової інформації.

Релігійні храми та світські навчальні заклади виконували роль виробників контенту, зміст якого залежав від специфіки чи тематики діяльності цих закладів. Більша частина цього контенту зберігалась у прототипах бібліотек у Шумері, Вавилоні, Єгипті тощо. Центрами створення інформації могли бути й адміністративні структури у вигляді канцелярій, муніципалітетів, торгових об’єднань.

2.2 Тренди інформаційних війн Середньовіччя, Відродження та Нового часу

Епоха Середньовіччя та Відродження характеризувалась сильним та всеосяжним контролем церкви та її участю у перебігу подій. Саме церква у ті часи була головним центром формування нової інформації та активно використовувала інформаційні війни для досягнення мети [13].

До традиційних інструментів медіа технологій (мови, мистецтва, писемності та реклами) починають додаватись нові, такі як: пропаганда й психологічна війна. Їх активно застосовувало керівництво Ватикану, зокрема папа Урбан II [13].

За часів протистояння Реформації з католицькою церквою у 1622 році було сформовано «Конгрегацію пропаганди віри». Ця організація першою в історії проводила інформаційно-психологічні спецоперації.

У цій боротьбі велось протистояння за свідомості населення, їх духовні цінності й настрої у політиці. Провідними діячами були Мартін Лютер, Жан Кальвін, Томас Мюнстер, а головною зброєю – слова. Їх публічні виступи, друковані тексти та дискусії є прикладом інформаційних атак. Головним їх завданням було повідомити населення про корупцію у церковних лавах. Каналами комунікації були відкриті й таємні організації. Церква намагалась боротись традиційними методами використовуючи свої храми, монастирі, авторитетність папського престолу, кардиналів та єпископів. Також до боротьби залучались божественні дива та підміна історичних фактів [13].

Вагомий внесок у розвиток інформаційних війн вклала Візантійська імперія. На це вказує безліч історичних фактів, у яких візантійські імператори отримували перемогу використовуючи психологічний тиск, дезінформацію та підкупи. Такі війни досить часто велись проти Київської Русі, ісламських держав та кочових племен. Після таких атак більшість прийомів були запозичені князями Київської Русі та набули широкого використання під час військових конфліктів та у внутрішньополітичних процесах. Не останню роль у цій боротьбі відігравала й православна церква. Найвідомішими київськими князями, що широко використовували технології маніпулювання були Володимир Мономах, Ярослав Мудрий, Володимир Великий, Ольга та Святослав [13].

У часи Середньовіччя основними виробниками контенту були релігійні організації, монастирі та духовні ордени. Протягом тривалого проміжку часу вони друкували книги, розробляли ідеологічні постулати напрацьовували методики інформаційно-комунікаційних процесів та виконували роль наукових та мистецьких центрів. З часом, ці ролі перехопили на себе школи, університеті та адміністративні центри.

Друкарство виникло в епоху Відродження та стало першою в історії глобальною мас-медіа технологією. Першою надрукованою книгою була «Біблія», яку Іоган Гутенберг у 1452 році зміг надрукувати на своєму друкарському верстаті. Хоча він був не першим, хто використовував друкарські винаходи, однак раніше такі технології на набули широкого вжитку [12].

Вагомий внесок у формування інформаційно-комунікаційних технологій в епоху Відродження зробили гуманісти. Вони широко використовували словесність у формі філології та риторики. Лоренцо Валла, наприклад, звертав увагу на те, що необхідно сформувати комунікацію між населенням та керівною верхівкою держави. Вітторіно да Фельтре, П'єтро Паоло та безліч інших гуманістів акцентували на тому, що існує необхідність постійного розвитку соціальних комунікацій з метою розширення знань та їх передачі суспільству.

Найближче до проблематики ведення інформаційної війни був Ніколо Макіавеллі. У його праці «Государ» було сформульовано поради для військових та політичних керівників для ведення ефективної інформаційної політики в ході військових дій та при управлінні державою. Також Макіавеллі надавав поради щодо формування комунікації між населенням та державними діячами й побудові останніми міжнародних стосунків [13].

Отже, основний інформаційний процес в епоху Середньовіччя складався зі створення, фіксації та передачі інформації, що нічим не відрізнявся від епохи Античності.

Однак, на відміну епохи ранніх держав Європи та Сходу, у часи Середньовіччя та Відродження інформаційними носіями були книги, твори мистецтва та офіційні документи, які фіксувалися на тканині, глині, папері та папірусі. З плином часу храми відходили на другий план, а на першому з'являлись університети та школи, які ставали виробниками контенту. Значна кількість інформації зберігалась саме в них.

Інформаційні війни у часи формування ринкових капіталістичних відносин відігравали роль допоміжних технологій та супроводжували збройні конфлікти. Європейці впроваджували нові технології та поширювали свій вплив на інші континенти далеко за межами Європи. Прикладом може слугувати Північна Америка, яка на початкових етапах була колоніальною, а у подальшому отримала свою незалежність.

Історичний розвиток США розпочинався зі збройних протистоянь за незалежність проти Англії. Саме у часи цієї боротьби були сформовані базові

технології та набули системний характер інформаційно-комунікаційні технології [13]. Колоністи широко застосовували такі товариства як «Сини свободи» та «Кореспондентські комітети», образні символи та стереотипи. Також вони активно використовували чутки, маніпуляції та дієві тогочасні акції. Так, наприклад, маніпуляції мали місце у «Бостонському чаюванні» у 1773 році, де пара перевдягнених колоністів у індійців мала на меті знищення вантажу чаю, що прибув з Англії. Окрім цього, колоністи активно проводили пропаганду щодо опису перебігу подій у Новому світі жителям Старого світу. Таким чином вони змогли перевести на свій бік Францію та Російську імперію.

Після боротьби за незалежність у Новому світі відбулись інші події, які стали не менш важливими в історії становлення інформаційних війн – наполеонівські війни та Французька революція. Ці події були непересічними та залишили по собі значний внесок у суспільно-політичну історію. Французька революція та весь її подальший розвиток був підготовлений такими вченими як Ж.-Ж. Русо, Вольтер, Д. Дідро, Ш. Монтеск'є та Ж. Д'Аламбер. Досліджуючи питання розвитку суспільства вони сформували технології, які з'явились у часи революції. Важливим інструментом вважались ідеї свободи та рівності, які розповсюджувалися у середині держав із монархічним типом правління. Французи використовували методи впливу на думку жителів ворожих країн для підриву їх єдності та наштовхували на формування ними опозиційних організацій.

Усі історично важливі суперечки XIX ст. містили в собі інформаційні протистояння у яких використовувалась преса, яка є другою в історії глобальною мас-медіа технологією. Це визначення бере своє коріння із назви першої газети «La Presse», яка була видана у 1831 році. У подальшому особливості проведення інформаційної війни набули особливого характеру. Преса почала відігравати роль інструменту, що може масово впливати на свідомість населення, а разом з цим і засобом для маніпулювання, залякування та дезінформації суспільства [13].

Разом із газетами, наприкінці XIX ст., почала з’являтись ще одна інформаційно-комунікаційна технологія – радіо. Вона стала третьою в історії глобальною мас-медіа технологією.

Вивченням особливостей інформаційних війн у ті часи займались чимало науковців та теоретиків. Серед них можливо виділити Карла Фон Клаузевіца, яких написав книгу в 1832 році під назвою «Про війну». У цій роботі він описував відчуття перемоги, дух та мораль як одні з головних складових успіху. На його думку вони були основною мішенню в інформаційно-комунікаційних атаках [9].

Отже, у часи Французької революції та наполеонівських війн інформаційними носіями виступали книги, листи та твори мистецтва, а виробниками контенту були заклади освіти та наукові центри.

На початку XX ст. було розпочато порушення сталого світового порядку. Стався ряд революції у Росії, Німеччині, Америці та Америці. Також відбулися дві світові війни, в ході яких світ розділився на два поля: СРСР та США. Виведення Росії з числа учасників Першої світової війни та розпад Російської імперії стали першим успішним прикладом використання інформаційної війни у XX ст.

Рисунок 2.4 – Агітаційні плакати Першої світової війни

Беручи до уваги усю міць Антанти (до цього об’єднання входили 34 країни, зокрема такі як: Англія, Франція, Росія та США) та неможливість перемоги

Німеччини у цьому протистоянні, урядом Кайзера Вільгельма було прийнято рішення стимулювання населення Росії до революційних рухів та зміни очільників держави. У результаті цих маніпуляцій Росія покинула лави Антанти та почала протистояння зі своїми союзниками [9]. Однак, такі маніпуляції для досягнення перемоги Німеччині нічого не дали. Після закінчення війни Антанта отримала перемогу, а Німеччина розділилась на декілька республік у ході революцій.

Одним з перших, хто досліджував питання розвитку інформаційно-комунікаційних технологій був Г.Д. Лассуел. У своїх роботах він розкривав методи психіатрії, психоаналізу, а також методи соціальної політики в аспекті пропаганди та політичної поведінки. Саме він одним з перших проаналізував інформаційну війну під час Першої світової війни. Свої дослідження Лассуел поєднав у книзі «Техніка пропаганди у світовій війні», що була видана у 1927 році. У цій праці пропаганда трактувалась як особливий вид зброї, який може впливати на моральний та психологічний стан противника [9].

Радянська Росія постала після Першої світової війни та з часом перетворилась на СРСР, що активно використовує інформаційно-комунікаційні технології для ведення війн та боротьби. Інформаційна війна, що велась всередині СРСР була направлена проти політичних опозицій та національних об’єднань. У боротьбі з ними велись агітаційні кампанії, дискредитаційні атаки, маніпуляції та залякування. У ході таких війн жертвами ставали невинні громадян, а в наслідок – було створено державний концтабір [9].

Зовнішня інформаційна війна велась проти політичних та економічних конкурентів СРСР, якими на той момент були США, Німеччина та союзи СОТ, ЄС, НАТО. Інформаційні атаки мали відкритий та прихований характер за участю СРСР. Серед таких конфліктів були війни з Польщею, Німеччиною, Фінляндією, В’єтнамом, Африкою та Латинською Америкою.

Майже весь час після свого формування та до розпаду СРСР знаходилась у стані інформаційної війни, що дало змогу КДБ, ЗМІ та партійним радянським

організаціям отримати значний досвід та напрацювати величезний інструментарій для ведення інформаційних та гібридних війн.

Рисунок 2.5 – Агітаційні плакати перших десятиліть СРСР

У дослідженнях розвитку інформаційних війн важливе значення відіграли напрацювання канадського науковця Г.М. Мак-Люена. Він займався дослідженнями ролі та значення мас-медіа у сучасному світі та у подальшому історичному розвитку. У своїх працях він виділяв три періоди: дописемний, писемний та сучасний. Основними ознаками останнього були «глобальне село» та «електронне суспільство». Під цими значеннями він розумів світ, у якому цифрові технології знаходились у одному інформаційному полі. Також саме Мак-Люен запровадив класифікацію медіа технологій за їх функціями та можливостями поділивши їх на «гарячі» та «холодні» [14].

Одним з найпотужніших противників СРСР були США, СОТ, ЄС та НАТО.

Після Першої та Другої світових війн саме СРСР та США розподілили світ на зони впливу, а їх протистояння одержало назву «холодної війни» 1946-1991 рр. Ця боротьба полягала у тому, що велись інформаційні протистояння на

постійній основі, відбувались гонки озброєнь та конфлікти за джерела сировини та ринок збуту [58].

У ході захисту своїх політичних та економічних інтересів США брала активну участь у значних та масштабних регіональних конфліктах на території Латинської Америки, Європи, Близького Сходу та Азії. Але у більшості випадків головним її конкурентом залишався СРСР. Протистояння цих двох держав неодноразово могли б закінчитись справжньою гарячою війною. Серед таких протистоянь були й Карибська криза 1962 року, 1 Берлінська криза 1961 року.

До головний центрів розробки та планування інформаційної війни у США відносились ЦРУ, які розробляли плани спецоперацій, Державний департамент, що займався дипломатичним прикриттям цих операцій та Пентагон, що займався військово-політичними операціями [15].

Серед найбільш успішних кампаній, що закінчились для США перемогою відноситься фінальна боротьба у «Холодній війні», яка прискорила процес розпаду СРСР на безліч окремих держав. Головним у цій боротьбі був Рональд Рейган, що був на той момент 40-м американським президентом. Ще у 1979 році він розпочав інформаційно-психологічну війну проти СРСР, назвавши останню «Імперією зла».

Головними складовими у цій боротьбі були економічні показники – економічні санкції та різке зниження цін на нафту, яка була основним джерелом прибутку СРСР. Разом з цим велись гонки озброєнь, які спустошували економічні запаси СРСР [15]

Активно застосовувалась ідеологічна складова. Так, у 1983 році Рейган оголосив про початок програми «Стратегічна оборонна ініціатива», зміст її полягав у використання лазерних пристроїв на американських супутниках для знищення ядерних ракет, які були б націлені на США. У цьому проєкті мали місце дезінформація та маніпуляційні дії. До таких дій були долучені навіть відомі особи Голівуду, які створили фільм «Зоряні війни». Також існувало багато галасу навколо кліматичної зброї. Саме американський уряд змусив Михайла

Горбачова, радянського лідера, підписати декілька мирних угод зі стороною Заходу та самовільно капітулювати.

З 1991 року США фактично залишається без конкурента та перебудовує систему економічних відносин під свої потреби. Під час війни на Балканах, Перській затоці, в Іраку перед США не виникає особливих складнощів.

Після вищеперерахованих конфліктів в Америці формується остаточна базова доктрина інформаційно-психологічної війни, її інструментарій, стратегія та методи. Створюється новий військовий підрозділ PSYOPS, як центр інформаційного забезпечення. А термін «інформаційної війни» набуває широкого вжитку [16]. Основними документами, що врегульовували б перебіг інформаційної війни стають Польовий Статут армії США та Доктрина спільних інформаційних дій.

Починаючи з XX ст. в ході інформаційної війни починають використовуватись не лише традиційні медіа, які застосовувались раніше, а й кіноіндустрія, телебачення та мережа Інтернет. Цей інструментарій значно підвищив рівень ефективності інформаційно-комунікаційних технологій в аспекті військової справи. А телебачення та мережа Інтернет стали четвертою та п’ятою глобальною мас-медіа технологією, відповідно [57].

Напрацювання Мак-Люена значно вплинули на встановлення розуміння значень та ролей мас-медіа в ході інформаційної війни. Відомий соціолог та політолог З. Бжезінський також займався теоретичними та методологічними аспектами інформаційної війни, видавши у 1997 році книгу для політологів «Велика шахівниця» [15]. У своїй роботі, спираючись на тенденції та особливості сучасного світу, він сформував роль США на світ та роль і перспективи Росії. Щодо України він зазначав про те, що дана країна є важливим центром у євразійській шахівниці й, що завдяки її незалежності, у Росії відбуваються певні трансформації.

Наприкінці XX ст. людство розпочало перехід до цифрової епохи. Разом із цим збільшилась кількість інформаційних конфліктів, що поступово перейшли

на Інтернет майданчик. Нового значення набуває визначення кібервійни, що стає невід'ємною частиною «гарячої» війни».

Поява та впровадження нових інформаційно-комунікаційних технологій ніяк не вплинула на сутність цілі інформаційної війни. У XX ст., як і попередніх століттях, використання інформаційної війни суттєво підвищувало можливість перемоги у військових, економічних та політичних конфліктах [57]. Прикладом можуть слугувати конфлікти Російської Федерації з іншими країнами світу. Після епохи правління Єльцина, до влади в Росії приходить Володимир Путін, а разом із ним починають звучати реваншистські заяви та розпочинається мілітаризація суспільства зі значним зростанням рівня виробництва зброї. З минулих епох до Путіна у спадок переходять конфлікти із Абхазією, Чечнею та Придністров'ям. До цього переліку додаються війни з Грузією та анексії Південної Осетії та Криму, а на Донбасі формуються терористичні угрупування, які називають себе Донецької та Луганською народними республіками. Окрім цих конфліктів Російська федерація втручається у внутрішній конфлікт Сирії, у якому урядові війська протистоять військовим угрупуванням ІДІЛу.

У вищеперерахованих конфліктах Російська Федерація демонструє набутий раніше досвід ведення інформаційно-психологічної війни, надаючи Путіну певних переваг та короткострокову перемогу. Однак, як показує досвід минулих років, це може завести Росію до геополітичної пастки, як за часів Рейгана.Варто зазначити, що інформаційна складова у зовнішній та внутрішній політиці Російської Федерації підіграє основну роль.

Важливим напрацюванням в аспекті інформаційно-комунікаційних технологій стало створення офлайн та онлайн структур. Останні відігравали важливе значення будучи у мережевому форматі WEB 2.0.

Разом із появою Інтернету, соціальні мережі набули кардинально іншого значення та відкривали перед людством нові можливості. Ще у 1995 році Ренді Конрадс створив перший в історії віртуальний соціальний ресурс під назвою Classmates.com, що охоплював, переважно, території США та Канади. Головною метою цього ресурсу було формування та підтримка спілкування друзів та

родичів, які мали бути зареєстровані на сервісі. Далі починають з'являтись нові соціальні мережі , так як: Friendster, Linked in, Tribe та Hi5 [15]. У 2004 році завдяки гарвадському студенту Марку Цукербергу на світ з'являється Facebook. Слідом за ним, свої соціальні мережі відкривають науковці на території СНД: Vkontakte.ru та Odnoklassniki.ru.

На сьогодні цифрові пристрої відіграють роль головних інформаційних носіїв, а інформаційні війни переходять у цифрову площину, супроводжуючи реальні військові конфлікти. Головною функцією суспільства стає виробництво контенту для забезпечення та підтримки наукової діяльності, економічних процесів та державного управління.

Досліджуючи історію військових дій між державами та народами можливо дійти до висновку, що інформаційна війна, як явище, завжди мала вплив на перебіг подій військового конфлікту. Ще у часи Київської Русі літописцями був зафіксований вплив та використання інформаційної зброї на територіях сучасної України. Прикладом може слугувати випадок із незафіксованим у джерелах візитом княгині Ольги до Константинополя. Мета та причини такої далекої поїздки не були висвітлені ані руськими літописцями, ані візантійськими, що наводить на думку про те, що тут мали місце інформаційні маніпуляції. Князь Святослав завжди повідомляв своїх ворогів про можливість нападу з його боку, однак залишав поза увагою напрямок дій та сили, які будуть задіяні. Таким чином, він наводив паніку серед лав ворогів та миттєво перемагав [1].

У сучасному житті суспільства відбувається посилення важливості інформації як у житті всього соціуму, так і в житті кожної окремо взятої людини. Інформація набуває матеріальної, економічної, енергетичної та вартісної форми. Разом із зростанням вагомості інформації в житті суспільства, перед державою постають нові завдання врегулювання суперечностей між існуючими та зростаючими потребами людини в інформаційному ресурсі, у якісному надані послуг та забезпеченні інформаційної безпеки.

РОЗДІЛ ІІІ
ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ТАКТИКИ ІНФОРМАЦІЙНОЇ ВІЙНИ ПРОТИ УКРАЇНИ

3.1 Інформаційно-психологічні засоби маніпуляції в операційній діяльності російських військових

Інформаційна війна є складовою боротьби за ідеали, що не призводить до безпосереднього кровопролиття чи руйнувань, породжуючи упереджене та легковажне ставлення до неї. Однак, руйнування, яких завдають інформаційно-психологічні атаки, за своїми масштабами та значенням можна прирівняти до руйнацій традиційних воєнних дій. Прикладів такого інформаційного впливу на стан противника в історії чимало. Але особливого значення вони набули лише у ХХ ст., із появою радіо та телебачення, що стали засобами масового розповсюдження інформації [23].

Вже наприкінці ХХ ст. з'являються нові засоби та форми протистояння збройним конфліктам. Поняття «війна» розширює поле своєї діяльності, охоплюючи політичні, психологічні та інформаційні аспекти. Хоча визначення війни залишається класичним, однак його діяльність стає неможливою без інформаційної складової, яка відіграє вирішальну роль в отриманні переваг у боротьбі із супротивником. Події на сході України досить часто класифікують як «гібридну війну», що включає в себе і збройний, і інформаційний конфлікти [56].

Ще з ХХ ст. у Російської федерації (РФ) існують конфлікти у Чечні, Абхазії та Грузії. До них додались війна з Південною Осетією та з Україною. У цих конфліктах використовувалися сучасні інформаційно-психологічні технології і продовжують вдосконалюватися їх різновиди. Після розвалу СРСР політичні лідери РФ сформували стратегію відновлення свого впливу на території пострадянських держав. Ця стратегія була спрямована зокрема і проти України, вихід якої з СРСР призвів до його розпаду. Отже, відносини між Україною та РФ необхідно розглядати через призму глобальних та геополітичних інтересів [23].

Інформаційну агресію проти України можна характеризувати як боротьбу нацистського режиму проти демократичного. Вона ведеться усіма можливими способами та засобами, а жертвами у даному конфлікті виступають не лише українці [29].

Інформаційна війна проти України направлена на розхитування стабільної ситуації всередині країни та на формування негативного іміджу України на міжнародному рівні, зазначає Є. Магда. Розпочався цей процес ще у 2005 році з початком першої «газової» війни. Тоді Україна була представлена у негативному світлі в ролі сумнівного транзитера газу. Разом з цими звинуваченнями було показово наголошено на необхідності альтернативних шляхів газопроводу. Однак звинувачення щодо крадіжок газу не підкріплювалися доказами [29].

За останні роки Україна досить часто була об'єктом інформаційних атак не лише з боку РФ, а й з боку Європи. До найбільш яскраво виражених прикладів інформаційних атак можна віднести нав'язування ідеї федералізації та надання державного статусу російській мові. У різні часи провідні теми змінювались, від проблеми Чорноморського флоту до проблеми паливно-енергетичного комплексу, від проблеми Криму та його жителів до діяльності екстремістських політичних об'єднань [30].

Вперше перемогу у війні такого роду над Україною була отримана вдяки поширенню та викривленню інформації щодо неспроможності країни обслуговувати ядерну зброю, внаслідок чого держава добровільно відмовилась від ядерного статусу та втратила вплив у міжнародних масштабах. «Касетний скандал», «газові» війни та звинувачення у продажах збройного устаткування у російсько-грузинській війні продовжили інформаційні атаки. За роки незалежності Україна не використовувала випереджаючу тактику та активну позицію, використовуючи лише методику оборони від інформаційних нападів.

Протягом останніх років усе, що висвітлювали російські медіа на окупованих територіях України залишалося поза увагою та не розглядалось у якості загрози національній безпеці країни, понаднормова зацікавленість російськими ЗМІ українського населення не викликала побоювань, що з часом

призвело до дестабілізації свідомості громадян. Так, наприклад, канал «Россия 24» висвітлював інформацію, що понад 140 000 біженців покинули територію України та шукали притулку в РФ, використовуючи у своїх повідомленням фото українсько-польського кордону. Закордонне телебачення часто також показує своїм глядачам вигадане беззаконня в Україні, за певним сценарієм, із використанням спецефектів, музики та акторської гри.

О. Саприкін вважає, що «інформаційна експансія» є більш містким поняттям, ніж «інформаційна війна» та «інформаційна атака». Ці визначення є складовими такої експансії. А сама інформаційна експансія визначається як система, яка містить методи пропаганди для досягнення поставлених цілей [32].

Як стверджує український вчений В. Карпенко, по відношенню до України проводиться інформаційна експансія. За його словами на теренах російського та українського телебачення одні й ті ж події досить часто висвітлюються під різним кутом. Тут іноземний інформатор використовує інформаційний простір в інтересах своєї країни [28].

Технологія створення іміджів є однією з форм застосування інформації. Варто зазначити, що в іміджі України переважають негативні риси, такі як: бюрократія, корупційні схеми та скандали, відсталий сервіс тощо. Однак, поряд із цим, існують і позитивні риси: орієнтованість на демократичні зміни та поведінкові характеристики населення.

Головними напрямами маніпулювання щодо України П. Шевчук визначає:

- поступове зменшення ролі України на міжнародній арені з метою її послаблення;

- рівномірне дозування та викривлення інформації з метою виведення з ладу державних систем влади, запроваджуючи керований хаос;

- створення стереотипу вторинної ролі України, із руйнуванням націоналістичних почуттів;

- підвищення важливості російської мови, культури та витіснення української [33].

У своїх роботах Ю. Радковець, кандидат військових наук, зазначає, що існують усі підстави для того, щоб стверджувати, що Україна зіткнулась з гібридною формою війни. Це підкріплюється особливостями ходу конфлікту, де відмінною ознакою є відсутність прямих воєнних дій. У ній використовуються нові методи ведення війни: шантаж, підкуп, викрадення людей, залякування, захоплення державних будівель та терористичні акти. Все це супроводжується активними пропагандистськими виступами та акціями насильства і мародерства. Безпекова та соціально-політична ситуація в Україні штучно «підриваються» різними виконавцями для формування повного безладдя [33].

Вітчизняні ЗМІ значно програють закордонним ЗМІ. При висвітленні подій на сході України зазначаються дані про кількість українських військових підрозділів, типи та види їх озброєння, номерні знаки військової техніки, кількість убитих. Наявність подібної інформації дає можливість підрахунку та зіставлення отриманої інформації аналітиками терористів [34].

Початок інформаційної війни у 2014 році ознаменував посилення впливу Росії на Україну. Для першої цей вплив розпочався із гібридної війни, яка межувала із державним тероризмом. Тобто, інформаційна війна, яка була активізована російською збройною агресією була направлена на інформаційну підтримку сепаратистського руху на сході України та послаблення контролю цих територій владою. По-іншому дане явище можливо назвати «рефлексивним контролем» [34]. Американський вчений Стів Тетем зазначав, що такий контроль застосовувався у псевдореферендумах в Криму [34].

Російською владою ця техніка також застосовувалась у ході переконання США та європейських союзників у невинуватості та непричетності до подій в Україні. Дана модель принесла значні зміни у міжнародному контексті, зокрема країни Заходу зберегли нейтралітет по відношенню до конфліктної ситуації між Україною та РФ. Однак Заходу необхідно виробити способи протистояння з рефлексивним методом війни.

Головними складовими рефлексивного методу інформаційної війни проти України є:

- заперечення будь-яких військових дій чи приховання наявності російських сил та території Донбасу;

- приховання головної та реальної мети РФ в конфлікті з Україною;

- пояснення законності діяльності РФ у ООН та інших міжнародних організаціях;

- проведення масштабної пропаганди серед свого населення та населення інших країн [2].

Хоча результати зусиль РФ не є однозначними, вона домоглась з боку західних держав їх невтручання у конфлікт, тим самим отримавши час для проведення військових дій. Також РФ змогла сформувати розбрат між країнами-членами НАТО та ЄС та створити напругу у питаннях щодо антиросійських санкцій.

Дезінформація також являє собою один із основних засобів ведення інформаційної війни РФ проти України. Вона має на меті збиття з пантелику, що дає змогу РФ заперечувати присутність її військ на території України та проведення військових операцій. Активна дезінформація дозволяє розширювати кількість можливих політичних рішень та надає змогу прикриття військових сил [2].

Ведення інформаційної війни проти України є масштабним втручанням в суверенітет держави, основною формою ведення такого роду війни є психологічна агресія, яка здійснюється шляхом інформаційно-психологічного впливу на свідомість суспільства, його почуття. Головним завданням такого інформаційного впливу є деморалізація населення України та спонукання військових сил і громадян до державної зради, формування у них викривленого сприйняття подій та підтримка прихильників об’єднання РФ та України. Існують декілька методів та прийомів, що застосовуються в інформаційній війні проти України [24].

Дезінформація та маніпуляції становлять собою методи, які передбачають введення об’єкта в оману щодо реальних намірів для направлення його на запрограмований план дій [1].

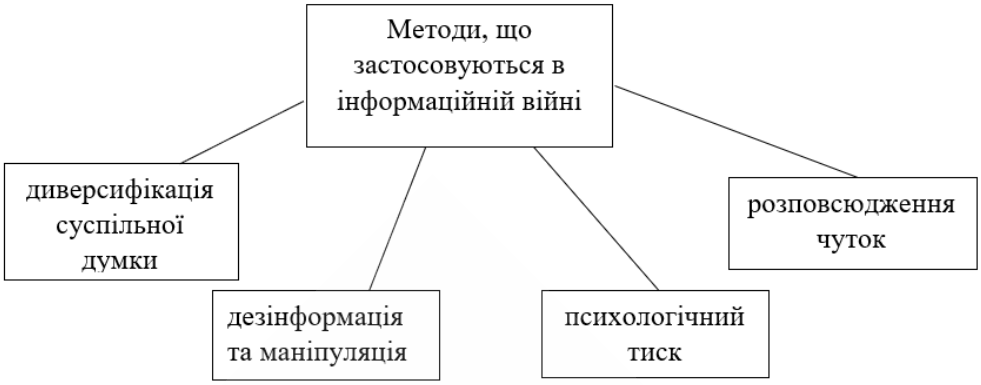

Рис 3.1 – Методи та прийоми, що застосовуються в інформаційній війні

Аналізуючи публікації російських ЗМІ з січня 2016 року по березень 2018 можливо зробити висновок, що усі ці повідомлення мали негативний характер по відношенню до України. На сьогоднішній день їх настрій та тематика не зазнали змін. Уся інформація у російських ЗМІ найчастіше описує питання діяльності ЗСУ, особливості співпраці України з Європою та НАТО, хід реформ в українському законодавстві та розвиток подій на окупованих й анексованих територіях України. Повідомляється, що Україна є центром легалізації тероризму та про наявність на її території тренувальних таборів. Однак, джерела та правдивість даної інформації не підтверджують жодні факти [26].

Будь-яка інформаційно-психологічна російська кампанія має на меті вплив на свідомість населення. Такий вплив є одним з психологічних прийомів інформаційної війни, які описував у своїх роботах Д. Зеркалов. Неправдиву інформацію можливо легко перевірити. Однак, якщо така інформація наводить на індивіда страх та паніку, то він може не замислюватись про її перевірку. Так, наприклад, інформаційне повідомлення на сторінці «Україна – ру» під заголовком «Порошенко – прибічник Люцифера» не мала нічого спільного із реальністю й після привернення уваги інших ЗМІ, її видалили. Подібні випадки в інтернет-просторі зустрічаються досить часто: «Керівництво України вимагає від Монголії матеріальної компенсації за нашестя Батия», «Загони поліції в Україні отримають інструменти від США для взлому будинків та житлових приміщень», «В Україні можливе примусове відключення електроенергії» [26].

Іншою характерною рисою інформаційної війни РФ проти України є демонізація останньої. У інформаційних повідомленнях досить часто по

відношенню до українських силових структур використовуються такі епітети, як «нацисти» та «каратели».

Також у повідомленнях закордонних ЗМІ торкаються питань релігії. Таке підвищення уваги до останньої зумовлене історичним розвитком двох держав та сильним впливом релігії на населення. У деяких матеріалах писали про те, що «тисяча паломників підтримали православних, які були вигнані радикалами». Варто зазначити, що українські священники у цих повідомленнях описувались як «церковні рейдери», а Київський патріархат записаний у лапках, для применшення його значимості у порівнянні з Московським. У повідомленні «Пастирі смерті: хто годує духовно українських карателів» зазначалось, що «стало відомо ім'я церковного служителя, якого було затримано у Донецькій області із зарядженою зброєю та ручними гранатами; ним став активний учасник Майдану та священик Іван Гопко; симпатія до зброї масового вбивства притаманна як уніатським, так й духовним наставникам карателів». Українську греко-католицьку церкву описано як «розкольницьку», а головного капелана як «духовного наставника карателів» [26]. Українська політична еліта також потрапила під дискредитаційний вплив РФ, про що свідчать повідомлення: «Документаційна драма: чому українські депутати запасаються паспортами інших держав», «Найбільш дивного знущання годі й придумати: Порошенка розкритикували за привітання Донецька із Днем міста».

Інформаційну атаку, яка ведеться проти України, не можливо розглядати як інформаційне протиборство, оскільки останнє являє собою форму боротьби, що об'єднує в собі спеціальні військові, економічні та дипломатичні методи, усі можливі способи та засоби впливу на інформаційне поле об'єкта впливу [26]. Складовою інформаційного протиборства є інформаційна війна, яка ведеться із використанням ЗМІ як інструментарію. Враховуючи всі особливості інформаційної війни можна стверджувати, що інформаційні атаки проти України мають такі ознаки:

- постійні дискредитуючі Україну публікації;

- перекривлення інформації;

- нав’язування думок читачам;
- поширення фейкової інформації;
- дискредитація українських лідерів;
- порушення доктрин журналістської діяльності [26].

Також можна констатувати, що РФ використовує весь арсенал інформаційно-психологічної зброї проти України, а замість єдиного дружнього радянського народу українці починають відігравати роль бандерівців для росіян. Відповідно змінюється відношення українців до російського народу, оскільки настільки масштабної інформаційної атаки не було раніше. Про це повідомляється в спільному дослідженні російської організації Левада та Київського інституту соціології, що базувались на результатах опитувань. Так, у 2014 році, з лютого по травень, відсоток позитивно налаштованих до РФ українців впав з 78 % до 52 %. У РФ відсоток позитивно налаштованих до України зменшився з 66 % до 35 %, а негативних зріс з 26 % до 49% [35].

Варто зазначити, що державні органи України, її громадяни та засоби масової інформації не були готові до масштабної інформаційної та військової агресії, що має назву «гібридної війни». Тому, першочерговим завданням громадськості, влади та науковців є розробка та впровадження ефективних заходів щодо нейтралізації інформаційного впливу зі сторони РФ та протидія подальшим атакам. Крім того, проблеми, які на сьогодні постали перед Україною, вимагають негайних заходів щодо модернізації інформаційної безпеки держави.

3.2 Протидія зовнішньому інформаційному впливу та контроль безпекового простору України

На сучасному етапі розвитку інформаційної безпеки, стратегічне інформаційне протиборство являє собою важливу проблему. Воно визначається як застосування глобального інформаційного середовища державами для

проведення стратегічних операцій та операцій зі зменшення впливу на особисті інформаційні ресурси.

Інформаційна безпека будь-якої держави являє собою стан захищеності національних інтересів у інформаційному полі. Деякі вчені трактують поняття «інформаційної безпеки» значно ширше. Так, наприклад, Д. Швець на мікрорівні інформаційну безпеку визначає як механізм контролю та забезпечення дотримання балансу між законністю та рівноправністю особи та держави в інформаційній сфері; на макрорівні дане поняття визначає як систему заходів, яка забезпечує захист особи та держави від інформаційного впливу [46].

Деякі науковці не підтримують таке трактування й розділяють інформаційну безпеку на елементи. Так, А. Фатьянов пропонує визначати інформаційну безпеку як стан захищеності інформації від будь-яких впливів та маніпуляцій. За дослідником поняття містить в собі два елементи:

-забезпечення безпеки даних від несанкціонованих впливів, блокування, модифікації чи цілковитого знищення;

-відсутність прихованих впливів на свідомість людини чи на іншу інформацію [47].

Варто виокремлювати таку складову інформаційної безпеки як небезпечна інформація для суспільства та держави, від якої необхідно захищати державне інформаційне середовище.

До такої інформації відносять:

- дані, що можуть спровокувати расову, релігійну, національну чи соціальну агресію;

- заклики до терористичних атак та військових дій;

- пропагандистські висловлювання, що містять зневагу та ненависть;

- компрометування честі та репутації окремих осіб та держави в цілому;

- неправдиву та недостовірну рекламу;

- інформацію, що чинить деструктивний вплив на свідомість населення [48].

Інформаційну безпеку необхідно розглядати у трьох аспектах [47].

Таблиця 3.1 – Аспекти інформаційної безпеки

АСПЕКТ	ЗНАЧЕННЯ
інформаційно-правовий	являє собою відповідну нормативно-правову базу, яка забезпечуватиме захист інтересів держави та громадянина в інформаційному середовищі
інформаційно-технічний	являє собою захист інформаційного поля від несанкціонованого втручання за допомогою застосування відповідного технічного засобу, хакерських атак через глобальну мережу Інтернет, комп'ютерних вірусів та несанкціонованого використання телевізійних та радіочастот у просторі держави
інформаційно-психологічний	являє собою захист психологічного стану людини від можливих негативних інформаційних маніпуляцій

Вищезазначені інформаційні впливи можуть спричиняти дестабілізацію у суспільстві та провокувати внутрішню боротьбу в країні. Найнебезпечнішими вважають інформаційні впливи, їх об'єктом є конституційні права та свободи громадян, оскільки їх дотримання являє собою головне завдання держави [48].

Як зазначав Г. Почепцов: «Військові використовують інформаційну базу у випадках, коли ведуться конкретні операції та навпаки, вони не використовують інформацію, коли військові дії не відбуваються». Але у сучасних умовах актуалізації інформаційної війни необхідно постійно підтримувати рівень інформаційного поля на належному та достатньо захищеному рівні. Варто приділяти увагу інформаційній взаємодії населення, яке не завжди правильно трактує цю війну. Враховуючи той факт, що громадяни мають власне відношення до даних, що базується на світогляді, рівні освіти та інтересах, фактор інформаційного споживання стає досить суттєвим, що відроджує інтерес до війни поглядів. Сучасні засоби комунікації поєднуються з науковими, збільшуючи наявний інструментарій. Головна роль у використанні технології масової маніпуляції населенням відведена ЗМІ та Інтернет-мережі [36].

Так, наприклад, за результатами дослідження Національної ради з проблем телебачення та радіо у 2018 році, в українських інформаційних каналах було присвячено лише 22 години ефірного часу проблематиці ситуації на сході України. Потреби в інформаційному забезпеченні населення кардинально відмінні від того інформаційного забезпечення, що надають інформаційні канали. Громадянам необхідно бути більш поінформованими щодо ситуації на окупованих та анексованих територіях України. Дослідження показують, що основну частину інформації про події на сході складають офіційні звернення: про кількість обстрілів, загиблих тощо. Однак відсутні пояснення про прийняття тих чи інших рішень [37]. Будь-яка сучасна суспільна організація керується принципами інформаційної війни: один проти всіх, всі проти одного тощо.

Масштаби резонансу українського суспільства та світу викликані забороною в Україні соціальних мереж. Як зазначав Генеральний секретар Ради Європи: «Перекриття доступу до соціальних мереж суперечить політиці вільного суспільства та відкритого доступу до масової інформації». Варто згадати, що у законодавстві існує певний принцип пропорційності, за яким встановлюється баланс між забороною та тим, на що накладено цю заборону [38].

Відомо, що соціальні мережі можуть здійснювати вплив не лише на свідомість суспільства, а й об’єднувати та вербувати людей для акцій протестів та терористичних терактів. Як зазначав А. Вассерман: «соціальні мережі являють собою найкращий з наявних інструмент отримання необхідної інформації та збору даних, а користувачі зазначають інформацію про себе та оточення [39].

Цією виключною особливістю соціальних мереж користуються безліч передових країн світу. Так, наприклад, США ще у 2009 році сформувала свої кібервійська як окремого підрозділу. На сьогоднішній день військові США обговорюють формування нової структури, що керуватиме інформаційними операціями. В РФ також існує підрозділ інформаційних операцій, а до діючого законодавства додано правові механізми, що направлені на протидію інформаційних атак в Інтернеті.

У 2015 році Кабінетом Міністрів України було створено Міністерство інформаційної політики, що займається формуванням та реалізацією державної політики в сфері інформаційного забезпечення та безпеки України. Дана структура в рамках своїх повноважень має вживати необхідних заходів для збору та зберігання інформації [40]. Міністерство інформаційної політики України на сьогодні базується, в основному, на принципах захисту прав та свобод громадян, їх думки та слів. При Міністерстві сформовано Громадську раду, до складу якої входять представники громадських об'єднань, медіа-персони та ЗМІ. Така Рада має на меті встановлювати нагляд за її діяльністю.

До головних завдань Міністерства інформаційної політики України можна віднести: - формування стратегії інформаційної політики України та засад в сфері інформаційної безпеки; - координування органів державної влади в сфері комунікацій та поширення інформації; - протидія інформаційним атакам та агресії.

Щорічно проводиться кілька прес-конференцій, тренінгів та зібрань для підвищення рівня обізнаності українських журналістів щодо своїх прав та свобод. У грудні 2016 року було розпочато курси для цивільних журналістів, що займаються висвітленням подій на окупованих територіях. У березні 2018 року за співпраці турецького інформаційного агентства було проведено тренінг, що мав назву «Журналістика у фінансовій та економічній сфері». За результатами цього заходу співпраця Туреччини та України вийшла на новий рівень, а журналісти мали змогу обмінятись із турецькими ЗМІ досвідом. У травні 2018 року за ініціативою Міністерства інформаційної політики було проведено круглий стіл на тему «Свобода слова». У ході якої перший заступник Міністра інформаційної політики назвала головну мету діяльності: «забезпечення усіх необхідних умов для вільної журналістики».

Протягом своєї діяльності Міністерство інформаційної політики ухвалило багато постанов та законопроєктів щодо інформаційної сфери України. У 2016 році – про надання фінансової допомоги кримськотатарському телеканалу ATR, що є єдиним у світі кримськотатарським, який поширює інформацію щодо історії

та культури кримських татар. У лютому було сформовано Міжвідомчу робочу групу, завданням якої було формування проєктів законів у сфері свободи слова. У 2017 році адміністрація міністерства звернулася до керівництва Facebook із пропозицією ввести в дію, на платформі соціальної мережі, антифейковий механізм. Оскільки дана мережа набирає все більшої популярності серед мешканців України та представників ЗМІ, висвітлювана у ній інформація повинна також бути достовірною та правдивою.

2 серпня 2017 року відбулась презентація видання МІП «Рекомендації в аспекті інформаційної безпеки в Інтернеті у часи конфлікту». У цьому виданні автори надають рекомендації громадянам щодо безпечної поведінки у мережі під час збройного протистояння. 6 вересня за підтримки Міністерства закордонних справ Чехії було презентовано проєкт «Довіряй, але перевіряй». Організатори проєкту мали на меті озвучити проблему медіаграмотності.

Міністерством інформаційної політики України було видано посібник із повним тлумаченням визначень, що мають відношення до інформаційного та збройного конфлікту, що має назву «АБВ. Збройний конфлікт у термінах». Даний посібник орієнтований на журналістів, державних діячів та службовців, які пов’язані зі збройними конфліктами. Також Міністерство, на своєму офіційному сайті у розділі «ООС», надає посилання на цінні інтернет-ресурси, які необхідні в умовах інформаційної війни. Серед посилань є сайт CERT-UA – підрозділу Державного центру захисту інформації, що займається попередженням та врегулюванням інформаційних загроз. Перейшовши за посиланням можливо повідомити структурний підрозділ про наявність кіберінциденту. На інтернет-ресурсі «Лікбез» можливо простежити бойові дії на території України. «Dokaz» висвітлює матеріали, що доводять присутність російських військ на території України, щодо терористичних атак та злочинів окупантів. Разом із цим подано посилання на такі матеріали як: «Як протидіяти російській пропаганді» та «Як працює російська пропаганда» [42]. Разом із цим у 2017 році Указом Президента України було накладено санкції на 468 українських та російських компаній [41].

У питанні інформаційної взаємодії з окупованими територіями України Міністерство інформаційної політики проводить активну діяльність. Так, наприклад, у тому ж 2017 році було проведено замовлення нових радіо частот у Луганській та Донецькій областях. Також Міністерство інформаційної політики є ініціатором надання дозволів на тимчасове мовлення у телевізійному просторі окупованих територій.

На сьогодні повністю заборонити щось в Інтернеті неможливо. Українські державні органи вжили мало заходів для роз'яснення громадянам реальної загрози соціальних мереж. Головною зброєю, у ході інформаційної боротьби, для України має бути навчання громадян критичному мисленню, усвідомлення отриманої інформації та її перевірка на достовірність і правдивість.

Для ефективної боротьби із тероризмом та сепаратизмом необхідно використовувати різні джерела інформації, особливу увагу приділяючи соціальним мережам. За допомогою останніх можливо завчасно виявити та ліквідувати терористичну атаку, передбачити виникнення антидержавних настроїв. Однак, варто враховувати окремі випадки, коли державні інтереси не співпадають з інтересами тих, хто цією державою керує. Обмеження чи цілковита заборона доступу до соціальних мереж може відіграти негативну роль для спецслужб. Наслідками такої заборони можуть бути зменшення ефективності роботи цих спецслужб та відсутність результатів діяльності.

Варто зазначити, що як економічні експансії, збройні конфлікти, так й інформаційні війни мають однаковий характер. В окремих випадках рівень ефективності інформаційної війни може перевищувати рівень ефективності збройної операції. Як зазначають дослідники, держава не може здійснювати опір збройній агресії, коли 40 % її населення знищено чи зруйновано 60 % її промислових об'єктів. За даними аналітиків, при відключені комп'ютерних мереж, 20 % середніх компаній зруйнуються, діяльність третини банків зупиниться, а через кілька днів свою роботу припинить половина підприємств країни. Яскравим прикладом такої масштабної хакерської атаки може бути атака, що проводилась влітку 2017 року із використанням вірусу «NotPetya», який

вразив комп'ютерні системи ІТ-компаній декількох країн світу. Під цю атаку потрапили нафтові, енергетичні, телекомунікаційні та фармацевтичні компанії, а результати цієї атаки відчули на собі майже половина населення України.

Як зазначав Сунь-Цзи у своїй книзі «Мистецтво війни»: «Щоб залишатись невидимим для противника, необхідно шукати та збирати інформацію про нього». Він розвивав теорію необхідності формування розвідувальної системи для отримання інформації не лише про ворогів, а й про друзів, для підвищення рівня безпеки країни. За його словами, ефективний підхід до ведення війни вимагає ретельного формування стратегії військової кампанії [43].

Проводячи паралель між цими словами та сучасними подіями можна дійти висновку, що постійний моніторинг соціальних мереж спецслужбами дозволить виявляти та нейтралізувати інформаційні атаки. Подібна співпраця військових підрозділів України та ІТ-компаній показує, що під час проведення розвідувальних операцій дозволила виявити та заблокувати 31 сайт, на яких здійснювали свою діяльність терористичні організації. Значна кількість прихованої інформації формується шляхом збору та аналізу інформації, яку розділяють на відкриту – доступну інформацію; відкриту для громадськості – дані та факти, що відкриті для широкого загалу [44]. В окремих випадках дані з відкритих джерел, отримані у результаті розвідувальних операцій, можуть значно перевищувати за цінністю дані, які мають певний рівень секретності.

Аналізуючи діяльність ЗМІ України, особливо у їх прямих трансляціях та експертних шоу, можливо завчасно виявити наміри держави та напрямки діяльності військових угрупувань на початковому рівні та отримати інформацію, яка належить до конфіденційної та цілком таємної. В Україні відсутні випадки притягнення до відповідальності осіб, причетних до оприлюднення конфіденційної інформації. Для вирішення цієї проблеми необхідно внести відповідні зміни до діючого законодавства у цій сфері. До іншої проблеми інформаційної безпеки відносять стан її інформаційної системи та рівень розвитку стратегічно важливих галузей науки, рівень культурно-освітнього розвитку громадян. Варто зазначити, що ефективне функціонування

інформаційної системи повинно здійснюватися з дотриманням законів України у сфері інформаційної безпеки. Слід приймати необхідні рішення щодо недопуску неправомірного використання інформаційної системи чи поширення заборонених даних [45].

На сьогоднішній день законодавство України регулює інформаційну діяльність та питання інформаційної безпеки. Закон України «Про інформацію» встановлює визначення понять «інформація», «документ» [49].

Закон України «Про доступ до публічної інформації» встановлює порядок забезпечення гарантіями та правами кожного на доступ до публічної інформації [50]. Закон України «Про телебачення і радіомовлення» діє на основі Закону України «Про інформацію» та врегульовує відносини на телевізійному та радіомовному просторі [51]. Закон України «Про друковані засоби масової інформації в Україні» врегульовує діяльність друкованих ЗМІ. Відповідно до цього закону, на пресу накладаються обмеження у їх діяльності [52]. Закон України «Про підтримку ЗМІ та соціальний захист журналістів» визначає порядок надання підтримки українським засобам масової інформації [53].

Закон України «Про висвітлення діяльності органів державної влади України засобами масової інформації» врегульовує питання опису діяльності органів влади у ЗМІ. Будь-яку інформацію про діяльність державних органів ЗМІ має отримувати від відповідальних інформаційних служб держвлади [54]. Закон України «Про особливості держполітики із забезпечення суверенітету України на тимчасово окупованих територіях» описує окуповані території та державну політику по відношенню до них. Врегульовує питання забезпечення захисту прав та свобод населення тимчасово окупованих територій [55].

Щоб інформаційна система безперервно функціонувала її необхідно забезпечувати безперебійною роботою та цілісністю й стійкістю функціонування, безпекою, відповідно до вимог законодавства. При формуванні інформаційної системи необхідно враховувати майбутні та можливі її розширення. Особливу роль тут відіграватиме забезпечення безпеки інформаційної системи від незаконного проникнення до неї сторонніх осіб.

Користувачам інформаційних систем необхідно забезпечувати автоматичний пошук інформації, на основі їх запитів, та надавати цю інформацію в доступному та зрозумілому вигляді. Програмне та технологічне забезпечення повинно також забезпечувати користувачів загальнодоступною інформацією.

Для забезпечення ефективного використання інформаційної системи необхідно застосовувати оперативне відновлення системи, здійснювати моніторинг поточного стану системи, безперервно відстежувати стан апаратно-програмного забезпечення цієї системи, контролювати та аналізувати продуктивність її складових частин та виявляти загрози, які обмежуватимуть її діяльність. Також необхідно формувати резервну копію даних, що міститься в інформаційній системі та забезпечувати безстрокове її зберігання, дотримуватись встановлених законодавством правил інформаційної безпеки, вести журнал обліку проведених операцій, що дозволятиме здійснювати моніторинг дій в інформаційній системі [45].

Варто також посилювати боротьбу з впливом іноземних ЗМІ через соціальні мережі на громадян. Для усунення такого негативного впливу через соцмережі необхідно не обмежувати їхню діяльність, а навпаки, взаємодіяти із розробниками соціальних мереж в контексті дотримання ними встановлених законодавством правил для перетворення їх в інструмент поширення правдивої та достовірної інформації.

Для захисту інформаційного поля та нацбезпеки України необхідно:

- -змінювати підходи до інформаційної політики, оновлюючи законодавчу та нормативно-правову бази;
- -здійснювати захист інформаційного простору держави;
- -просувати український варіант інформації на територію агресора, із використанням сучасних технологій;
- -зменшувати ролі олігархів у ЗМІ;
- -формувати позитивний імідж України;
- -проводити люстраційні заходи серед керівників українських ЗМІ;

●-встановлювати обмеження для російських інформаційних каналів, що мають вплив на окуповані території України;

●-контролювати іноземні ЗМІ;

●-здійснювати діяльність в інформаційному просторі в державних інтересах;

●-організовувати та проводити розвідувальні операції, що пов’язані з проникненням у державні органи влади інших країн;

●-контролювати висвітлення правдивої інформації суспільству із використанням закликів не купувати російське, замінюючи українським, що є якісний та перевіреним;

●-блокувати інтернет каналів, які загрожують національній безпеці країни;

●-стимулювати наукові дослідження у сфері національної політики та інформаційної безпеки;

●-вдосконалювати рівень підготовки фахівців в інформаційній галузі [45].

Доповнювати та постійно оновлювати законодавчу базу в інформаційній сфері, оскільки закони та розпорядження не охоплюють усіх питань. Наявне законодавством не врегульовується діяльність Інтернету та соціальних мереж, які є інформаційними засобами впливу. Проблема взаємодії користувачів соціальними мережами між собою, керівництва соцмереж та державної влади, перевірки достовірності та правдивості висвітлюваної інформації в Інтернеті є не вирішеними та потребують уваги державних органів влади.

ВИСНОВКИ

У процесі досягнення мети магістерської роботи було послідовно вирішено сформульовані завдання дослідження.

1. Дослідження поняття «інформаційної війни» у першому розділі дозволило встановити підходи до його визначення, розглянути роботи дослідників та науковців, що займались вивченням даного поняття. Також встановлено ряд завдань інформаційної війни, зокрема такі як: маніпуляційні дії, із громадською думкою для формування напруги у політичній сфері; здійснення руйнівного впливу на політичну силу країни шляхом послаблення її можливостей; зменшення значення відкриттів та досягнень у науковій сфері тощо. Встановлено, що інформаційна війна включає в себе і активно використовує психологічні операції, фізичні руйнації та прямі інформаційні атаки. В своїй основі інформаційні війни мають три складові елементи, що відрізняються власним технологічним наповненням: хай-тек, хай-х'юм, хай-сенсоро. Також визначено обов'язкові складові інформаційної війни, такі як інформація та комунікація.

Поняття «інформаційна зброя» виступає головним елементом інформаційної війни. Мішенню такої зброї було визначено національну інформаційну структуру та її засоби.

Форми та методи інформаційної війни можна подати у вигляді пропаганди, чуток, провокацій, диверсифікацій, маніпуляційних дій, дезінформації, залякування, глузування, фальшування. Зазначений список не є повним і з розвитком суспільства постійно поповнюється та розширюється у своїй міждисциплінарності.

2. Аналіз інформаційної війни в історичному аспекті, наведений у другому розділі роботи, дозволив показати етапи розвитку даного поняття та встановити відмінні риси кожного з цих етапів. Так, розглянуто форми інформаційної війни у часи первісного суспільства, коли формувались прототипи міст та взаємодій.

Визначено роль первісної мови, мовлення та образотворчого мистецтва в інформаційному розвитку суспільства.

Простежено хід історичного розвитку у часи Античності, Середньовіччя та нового часу, їх особливості в інформаційному аспекті та вплив на формування сучасного поняття інформаційної війни. Визначено, що вже наприкінці XX ст. суспільство розпочало перехід до цифрової епохи. Разом з тим збільшилась кількість інформаційних атак, конфліктів та війн, що поступово перейшли в Інтернет площину. У ході таких змін було встановлено, що поняття «кібервійни» також набуло відмінного значення та стало складовою «гарячої» війни.

3. Дослідження інформаційної національної безпеки України та впливів на неї з боку інших держав, наведено у третьому розділі, дозволило визначити використовувані методи інформаційної війни проти країни та методи протидії таким атакам сьогодні. Визначено ряд напрямів у маніпуляційних діях щодо України, до яких віднесено поступове зменшення важливості України на міжнародній арені; формування стереотипу вторинності держави; підвищення ролі російської мови та інші. Також визначено складові рефлексивного методу в інформаційній війні проти України у вигляді заперечення військових дій чи приховування наявності військ на території Донбасу; приховування головної та реальної мети військових конфліктів з країною; проведення масштабної пропаганди серед населення.

Встановлено роль та значення українських та закордонних засобів масової інформації у ході інформаційної війни. Виділено та проаналізовано ряд інформаційних атак в Інтернет просторі, що дозволило запропонувати механізми протидії та захисту інформаційного простору держави.

Визначено поняття «інформаційної безпеки», що являє собою стан захищеності національних інтересів у інформаційному просторі. Перераховано ряд інформаційних впливів, що можуть спричиняти дестабілізацію у суспільстві та провокувати внутрішню боротьбу в країні. До них відносять: інформаційно-правовий, інформаційно-технічний, інформаційно-психологічний аспекти. Проаналізовано заходи, що були впроваджені у ході підтримки інформаційної

безпеки та протидії інформаційним атакам з боку інших держав: формування та впровадження законів та законодавчих проєктів в аспекті інформаційного середовища; визначення ролі засобів масової інформації, їх підтримка та врегулювання діяльності на державному рівні. Також зазначено заходи, що є необхідними для формування та підтримки інформаційної національної безпеки України: зміна підходів до інформаційної політики, оновлення законодавчої бази; просування українського варіанту інформації на території агресора; проведення люстраційних заходів серед керівництва українських засобів масової інформації; контроль висвітлення правдивої інформації суспільству; блокування та контроль каналів, що загрожують інформаційній національній безпеці країни; вдосконалення та підвищення рівня підготовки фахівців в інформаційній галузі.

Встановлено, що у сучасних умовах актуалізації інформаційної війни необхідно постійно підтримувати рівень державного інформаційного поля на належному та достатньо захищеному рівні. Також необхідно доповнювати законодавчу базу в аспекті врегулювання діяльності соціальних мереж, взаємодії всередині інформаційно-комунікаційних мереж між користувачами, відповідальності за розповсюдження викривленої та неправдивої інформації.

Відповідно до поставленої мети та завдань у ході дослідження було охарактеризовано стан сучасного законодавства України щодо питання врегулювання інформаційного протиборства, виокремлено проблеми інформаційного протиборства України, запропоновано рекомендації щодо врегулювання питань протиборства.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Сасин Г.В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). Ужгород, 2015.

2. Черешкин Д.С. Реалии информационной войны. *Конфидент*. 2012. №4. С. 9-12.

3. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі: навчальний посібник. Київ: ВІКНУ, 2016. 286 с.

4. Макаренко Л.П. Еволюція форм та методів ведення інформаційної війни. ДВНЗ «Київський університет управління і підприємництва». Київ, 2014.

5. Кузнецов П.А. Информационная война и бизнес. *Конфидент*. 2012. № 4. С. 21-24.

6. Курбан О.В. Діагностика та моделювання PR-процесів: навчальний посібник. Київ: Українська конфедерація журналістів, 2012. 160 с.

7. Доктрина інформаційної безпеки України: Затверджена указом Президента України від 8 лип. 2009 р. № 14/2009. URL: http://zakon.rada.gov.ua/laws/show/514/2009.

8. Рижиков М.М. Міжнародна інформаційна безпека: Сучасні виклики та загрози. К.: Центр вільної преси, 2015.

9. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни. Вінниця: Віндрук, 2014.

10. Бебік В.М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рілейшнз: монографія. Київ: МАУП, 2005. 440 с.

11. Рыбаков Б.А. Язычество древних славян. Москва: Академический проект, 2013. 627 с.

12. Информационно-психологическая безопасность в эпоху глобализации: учеб. пособие. / под. ред. В.М. Петрик, В.В. Остроухов, А.А. Штоквиш. Киев: Белоцерковская книжная фабрика, 2008. 544 с.

13. Королько В.Г. Основы паблик рилейшнз. М.: Рефл-бук; Киев: Ваклер. 2000. 528 с.

14. Мак-Люен М. Галактика Гутенберга: становлення людини друкованої книги. Київ: Ніка-Центр, 2001. 464 с.

15. Березкин Г.А. Уроки и выводы из войны в Ираке. Военная мысль. 2003. №7. С.58-65.

16. Вєдєнєєв Д.В, Биструхін Г.С., Семука А.І. Гострі когті орла. Сили спеціальних операцій США: історія та сучасність. Київ: К.І.С., 2010. 400 с.

17. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). Мн.: Харвест, 1999.

18. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії. К.: ВКФ “Сатсанга”, 2000.

19. Петрик В.М., Остроухов В.В., Штоквиш О.А. та ін. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: навч. посіб. / за ред. В. М. Петрика. К.: Росава, 2006.

20. Почепцов Г.Г. Психологические войны. М., К., 2000.

21. Багиров Р.З. Политическая коммуникация в обеспечении военной безопасности Российской Федерации: автореф. дис. на соискание науч. степени канд. полит. наук спец. 23.00.02 «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии». М., 2009. 21 с.

22. Горбенко А. СМИ в сфере информационного противоборства. Власть. 2008. № 11. с. 23-26.

23. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: www.justinian.com.ua/article.php.

24. Манойло А.В. К вопросу о содержании понятия «информационная война». URL: http://ashpi.asu.ru/ic/?p=1552.

25. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році». К.: НІСД, 2016. 688 с.

26. Масова інформація в радянському промисловому місті: Досвід комплексного соціологічного дослідження / під заг. ред. Б.А. Грушина, Л.А. Оконнікова. М.: Эскимо, 2006. 347 с.

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

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

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

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

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

32. 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.

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

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

35. Почепцов Г. Росія і Україна у співставленні їх комунікативно-пропагандистських можливостей. URL: http://osvita.mediasapiens.ua/material/33291

36. Присяжнюк М.М., Бєлошевич Я.С. Інформаційна безпека України в сучасних умовах: *Вісник Київського національного університету імені Тараса Шевченка*. Військово-спеціальні науки. 2013. Вип. 30. С. 37-41.

37. Дуцик Д. Інформаційний вакуум: як українські телеканали висвітлюють події на Донбасі та в Криму. URL: https://hromadskeradio.org/programs/kyiv-donbas/informaciynyy-vakuum-yak-ukrayinski-telekanalyvysvitlyuyut-podiyi-na-donbasi-ta-v-krymu.

38. Власенко В. Генсек Ради Європи: Блокування соціальних мереж не відповідає принципу свободи ЗМІ. URL: http://p.dw.com/p/2d5iH.

39. Вассерман А.А. Социальные сети и дезинформация. URL: http://plaza152.ru/video/jXccNMj2MlA.

40. Питання діяльності Міністерства інформаційної політики України: Постанова Кабінету Міністрів України від 14.01.2015 № 2. *Офіційний вісник України*. 2015. № 6. Ст. 124.

41. В Україні набув чинності указ про блокування ВКонтакте і Одноклассников. URL: https://www.unian.ua/politics/1926399-v-ukrajini-nabuv-chinnosti-ukaz-pro-blokuvannya-vkontakte-i-odnoklassnikov.html.

42. Міністерство інформаційної політики України. URL: https://mip.gov.ua/

43. Сунь-цзы. Искусство войны. Київ : Центрполиграф, 2014. 192 с.

44. Ржевська Н.Ф., Кожушко О.О. Розвідка відкритих джерел. URL: http://ena.lp.edu.ua/bitstream/ntb/19232/1/53-Rzhevska-257-261.pdf

45. Остапов С. Е., Євсеєв С.П., Король О.Г. Технології захисту інформації : навчальний посібник. Х.: Вид. ХНЕУ, 2013. 476 с.

46. Швец Д.Ю. Информационная безопасность РФ в современных международных отношениях. М., 2005.

47. Фатьянов А.А. Тайна и право (основные системы ограничения на доступ к информации в российском праве): монография. М., 1999. 285 с.

48. Савин Л. В. Сетецентричная и сетевая война. Введение в концепцию. М.: Евразийское движение, 2001. 130 с.

49. Про інформацію: Закон України від 02.10.1992 № 2657-XII.

50. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI.

51. Про телебачення і радіомовлення: Закон України від 21.12.1993 № 3759-XII.

52. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.1992 № 2782-XII.

53. Про державну підтримку засобів масової інформації та соціальний захист журналістів : Закон України від 23.09.1997 № 540/97-ВР.

54. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації : Закон України від 23.09.1997 № 539/97-ВР.

55. Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях : Закон України від 18.01.2018 № 2268-VIII.

56. Гібридна війна: in verbo et in praxi. Вінниця:«Нілан-ЛТД», 2017. URL: https://jmonographs.donnu.edu.ua/article/view/3781

57. Ковальська Л.А. Комунікативні особливості функціонування документально-інформаційного ресурсу. Бібліотекознавство. Документознавство. Інформологія. Київ, 2021. № 1. С. 27-34.

58. Ковальська Л.А. Джерелознавчий дискурс історії радянського Руху Опору (1941–1945 рр.). Донецьк-Вінниця: ТОВ «Нілан-ЛТД», 2015. 462 с.

59. Kovalska L., Anisimova O., Peleshchyshyn O. Opportunities of Social Networks in Educational Activities. Proceedings of the 2nd International Workshop on Control, Optimisation and Analytical Processing of Social Networks (COAPSN 2020). Lviv, Ukraine, May 21, 2020. 137-151.

60. Бойко Ю.В. Соціальні мережі як зброя та інструмент впливу в умовах інформаційної війни. Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса. Том 1 / Ред. кол. Хаджинов І. В. (голова) та ін. Вінниця : ДонНУ імені Василя Стуса, 2021. Вип. 13. Т. 1. 304 с. С. 235-238.

61. Бойко Ю.В. Реалізація громадянських ініціатив засобами соціальних мереж. VI Міжнародна науково-практична конференція «Документно-

інформаційні комунікації в умовах глобалізації: стан, проблеми і перспективи». Полтава: Полтавська політехніка імені Юрія Кондратюка, 2021.

62. Бойко Ю.В. Трансформація інформаційної війни в історичній ретроспективі. Всеукраїнська науково-практична конференція «Прикладні аспекти сучасних міждисциплінарних досліджень». ДонНУ імені Василя Стуса. Вінниця, 2021.

63. Трансформаційні процеси у суспільній та соціокультурній сферах України: монографія / авт. колектив: Анісімова О.М., Ковальська Л.А., Лукаш Г.П., Прігунов О.В., Щербіна О.С., Яворська Т.М. Вінниця: ДонНУ імені Василя Стуса, 2021. 176 с.