Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Києво-Могилянська школа врядування імені Андрія Мелешевича

Магістерська робота
Освітній ступень - магістр

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СВОБОДИ СЛОВА В КОМУНІКАЦІЯХ ПІД ЧАС ВІЙНИ В УКРАЇНІ

ENSURING INFORMATION SECURITY AND FREEDOM OF SPEECH IN COMMUNICATIONS DURING WARTIME IN UKRAINE

Виконала здобувачка освітньо-наукової
програми «Суспільна політика і врядування»
_____ Тетяна ЗАГОРЕЦЬ

Науковий керівник
професор кафедри суспільного врядування,
доктор наук з державного управління,
кандидат технічних наук, професор
_____ Геннадій РЯБЦЕВ

Рекомендована оцінка
_____
Рецензент
_____ Дмитро ЗОЛОТУХИН
Секретар ЕК
_____
«___»_____2024

Київ – 2024

Декларація

Академічної доброчесності

Студента НаУКМА

Я, Загорець Тетяна Олександрівна, студентка 2022-2024 року навчання факультету правничих наук, спеціальність 281. Суспільна політика і врядування, адреса електронної пошти t.zahorets@ukma.edu.ua

- Підтверджую, що написана мною кваліфікаційна (випускова) робота на тему «ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СВОБОДИ СЛОВА В КОМУНІКАЦІЯХ ПІД ЧАС ВІЙНИ В УКРАЇНІ» відповідає вимогам академічної доброчесності та не містить порушень, передбачених п. 1.3 Тимчасового положення про порядок перевірки письмових робіт студентів НаУКМА на відповідність вимогам академічної доброчесності, зі змістом якого ознайомлена;

- Заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії;

- Згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності у будь-який спосіб, а також на архівування моєї роботи в базі даних цієї системи*.

10.05.2024 _____ Тетяна ЗАГОРЕЦЬ

АНОТАЦІЯ

Загорець Т.О. Забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в Україні. – Кваліфікаційна магістерська робота на правах рукопису.

Кваліфікаційна магістерська робота на здобуття ступеня вищої освіти другого (магістерського) рівня галузі знань 281 «Публічне управління та адміністрування». – Національний університет «Києво-Могилянська академія». Факультет правничих наук, Києво-Могилянська школа врядування імені Андрія Мелешевіча, Київ, 2024.

Магістерська робота присвячена аналізу та вивченню проблеми забезпечення інформаційної безпеки та свободи слова під час війни в Україні. Розглядаються теоретичні аспекти інформаційної безпеки та її взаємозв'язок із свободою слова, важливість інформації та свободи слова під час війни, а також державна політика щодо їх забезпечення. Значна увага приділяється зарубіжному досвіду в цій сфері. Досліджується вплив інформаційної війни на забезпечення інформаційної безпеки та свободи слова в Україні. Особливий акцент зроблено на аналізі явища «інформаційна війна», її поняття та особливості в Україні.. Здійснюється аналіз стейкхолдерів та середовища політики в сфері інформаційної безпеки та свободи слова, а також визначаються складові механізму їх забезпечення. Пропонуються конкретні пропозиції та рекомендації щодо забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в Україні.

Робота має на меті поглиблене розуміння проблеми забезпечення інформаційної безпеки та свободи слова під час війни в Україні та розробку практичних рекомендацій для її вирішення.

Ключові слова: інформаційна безпека, свобода слова, інформаційна війна, комунікації, органи влади.

ANNOTATION

Zahorets T.O. Ensuring information security and freedom of speech in communications during wartime in Ukraine. – Qualification Master's thesis as a manuscript. Qualification Master's thesis for the degree of higher education of the second (master's) level in the field of knowledge 281 "Public Administration and Administration". – National University "Kyiv-Mohyla Academy". Faculty of Law, Kyiv-Mohyla School of Governance named after Andriy Meleshevych, Kyiv, 2024.

The Master's thesis is devoted to the analysis and study of the problem of ensuring information security and freedom of speech during wartime in Ukraine. The theoretical aspects of information security and its relationship with freedom of speech are considered, as well as the importance of information and freedom of speech during wartime, and the state policy regarding their provision. Significant attention is paid to foreign experience in this field. The impact of information warfare on ensuring information security and freedom of speech in Ukraine is investigated. Special emphasis is placed on analyzing the phenomenon of "information warfare," its concepts, and peculiarities in Ukraine. An analysis of stakeholders and the policy environment in the field of information security and freedom of speech is carried out, and the components of the mechanism for their provision are determined. Concrete proposals and recommendations are offered for ensuring information security and freedom of speech in communications during wartime in Ukraine.

The thesis aims to deepen understanding of the problem of ensuring information security and freedom of speech during wartime in Ukraine and develop practical recommendations for its resolution.

Keywords: information security, freedom of speech, information warfare, communications, government bodies.

ЗМІСТ

ВСТУП

В сучасному світі інформація є ключовим ресурсом, який може використовуватися як для досягнення мирних цілей, так і для ведення війни. Завдяки інформації можна як розпочати, так і виграти війну, не зробивши жодного пострілу. Використання інформації для розпалювання внутрішніх протиріч є основою тактики «інформаційної війни» (так званої гібридної війни), де безпосередньо військові дії є лише однією зі складових стратегії.

Починаючи з 2014 року, з боку російської федерації постійно здійснюються інформаційні атаки, спрямовані на спотворення фактів та явищ, просування в інформаційному просторі пропаганди національної ворожнечі, насильства та сепаратизму. Ці атаки впливають не лише на свідомість громадян України, а й на світову спільноту, весь медіапростір.

Отже, в умовах воєнного стану в Україні інформація є стратегічним інструментом перемоги.

Правовий режим воєнного стану впливає на загальний обсяг прав людини та громадянина. Інформаційна безпека держави, яка знаходиться у воєнному стані, потребує комплексних дій щодо її захисту, у тому числі, через звуження прав та свобод суб’єктів на її території. Окрему групу у цих обмеженнях займають інформаційні права та свободи людини і громадянина. Через це на сьогодні важливим завданням є забезпечення інформаційної безпеки України та винайдення балансу між реалізацією права на свободу слова та інформаційною безпекою під час війни.

Отже, проблема забезпечення інформаційної безпеки та свободи слова в комунікаціях є актуальною для України під час війни.

Актуальність даного дослідження полягає в комплексному аналізі існуючого стану інформаційної безпеки України, визначення загроз в забезпеченні інформаційної безпеки держави і громадян під час війни, вивчені впливу інформаційної війни на комунікації в Україні та реалізації права на свободу слова під час війни.

Об’єктом наукового дослідження механізм забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни як протидія інформаційній війні Російської Федерації проти України.

Предмет дослідження – інформаційна безпека та свобода слова в комунікаціях під час війни в Україні.

Мета магістерського дослідження - дослідження системи забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в Україні для розробки рекомендацій щодо впровадження політики в сфері протидії інформаційній війні Російської Федерації проти України.

Відповідно до мети дослідження, сформовані наступні **завдання магістерського дослідження**:

1. Провести аналіз різних підходів до визначення інформаційної безпеки та свободи слова у контексті воєнного конфлікту для розуміння основних термінів та концепцій, які лежать в основі розробки ефективних стратегій забезпечення безпеки та свободи слова під час війни.

2. Вивчити роль інформації та свободи слова під час війни, зокрема їх ключову роль у забезпеченні безпеки та вільного інформаційного обміну задля визначення важливості цих аспектів та їх впливу на ефективність захисту свободи слова в умовах воєнного конфлікту.

3. Проаналізувати державну політику України з питань забезпечення інформаційної безпеки та свободи слова під час війни для оцінки існуючих стратегій та політичних заходів і виявлення їх ефективності.

4. Дослідити зарубіжний досвід забезпечення інформаційної безпеки для визначення найбільш ефективних практик для використання цього досвіду у вдосконаленні стратегій та політики в Україні.

5. Вивчити поняття та особливості інформаційної війни, а також її вплив на інформаційну безпеку та свободу слова в Україні для розуміння механізмів інформаційної війни та її наслідків для інформаційної безпеки та свободи слова.

6. Проаналізувати вплив інформаційної війни на забезпечення інформаційної безпеки та свободи слова в Україні для виявлення основних загроз та визначення найбільш уразливих аспектів.

7. Проаналізувати стрейкхолдерів та середовище політики в сфері забезпечення інформаційної безпеки як передумови формування пропозицій щодо курсу дій в цій сфері.

8. Вивчити складові механізму забезпечення інформаційної безпеки та свободи слова під час війни в Україні для розуміння завдань, що стоять перед органами влади в сфері забезпечення інформаційної безпеки та свободу слова в умовах війни.

9. Розробити рекомендації органам влади щодо політики забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни на основі проведеного аналізу.

В різні роки дані питання досліджувалися як зарубіжними так і українськими дослідниками.

В українській науковій літературі проблемі правового забезпечення обігу інформації посвячені роботи низки знаних науковців, серед яких В. Богданович, Р. Калюжний, В. Ліпкан, І. Сопілко та ін. Проблеми забезпечення інформаційної безпеки покладені в основу досліджень В. Гурковського, В. Копилова, Б. Кормича, В. Настюка, М. Швеця, А. Селіванова. Сучасні особливості інформаційного суверенітету та доктрини інформаційної безпеки України досліджують В. Бондаренко Ю. Горбань, М. Дмитренко, Ф. Медвідь, О. Черевко та ін.

Права людини в умовах інформаційного суспільства досліджували такі зарубіжні вчені, як І. Браун, В. Дрейк, Р. Йоргенсен, Д. Лайон, Л. Лессіг, К. Расерока. Сутність, класифікація та ефективність застосування інформаційних прав в Україні є у сфері наукових інтересів вітчизняних вчених серед яких І. Арістова, Т. Костецька, А. Марущак та багато інших авторів.

Тема інформаційної війни досліджувалася багатьма науковцями: Г. Почепцовим, Є. Магдою, О. Данильяном, О. Дзьобань, І. Сопілко, В. Хорошко,

Ю. Хохлачовою, І. Жаровською, Н. Ортинською, О. Марунченко, О. Саган, О. Курбаном, В. Новородовським, М. Гетьманчуком, М. Зубарєвою тощо.

Науково-практична новизна дослідження полягає в аналізі існуючих теоретичних досліджень через призму повномасштабної війни в Україні.

Науково-практична значущість дослідження полягає в систематизації теоретичних засад, виокремленні інформації задля глибшого розуміння проблематики забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в Україні.

Методологічна основа дослідження забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в Україні базується на комбінації кількох підходів та методів дослідження:

1. Аналіз концептуальних та теоретичних підходів.

Дослідження базується на аналізі та узагальненні наукової літератури щодо концепцій інформаційної безпеки, свободи слова, комунікативного середовища під час війни та особливостей інформаційної війни.

2. Історичний підхід.

Дослідження враховує історичний контекст українського суспільства та попередні дослідження у цій галузі для зрозуміння еволюції понять і практик забезпечення інформаційної безпеки та свободи слова.

3. Порівняльний аналіз.

Дослідження включає порівняльний аналіз інформаційної політики та практик інших країн, особливо тих, що пережили воєнні конфлікти та інформаційні війни.

4. Емпіричний метод.

Для отримання конкретних даних та інформації про практичні аспекти досліджуваної проблематики використовуються емпіричні методи, такі як спостереження, інтерв'ювання, результати опитувань та соціальних досліджень тощо.

5. Стратегічний аналіз.

Дослідження використовує стратегічний аналіз для оцінки та прогнозування можливих ризиків, загроз та можливостей у галузі інформаційної безпеки та свободи слова під час війни.

6. Контент-аналіз.

У дослідженні контент-аналіз використаний для аналізу медіа-змісту, законодавчих актів, офіційних заяв тощо, щоб з'ясувати, які теми або дискурси домінують у питаннях інформаційної безпеки та свободи слова під час війни в Україні.

7. Системний метод.

У дослідженні системний підхід використаний для вивчення взаємозв'язків між різними аспектами інформаційної безпеки та свободи слова, такими як законодавство, практичні заходи, реакція громадськості тощо.

8. Структурно-функціональний метод.

У дослідженні цей метод використаний для аналізу ролі різних інституцій та механізмів у забезпеченні інформаційної безпеки та свободи слова під час війни, розуміння їх функцій та взаємодії.

Ці методи допоможуть провести глибокий та систематичний аналіз теми дослідження, виявити ключові патерни та фактори, що впливають на інформаційну безпеку та свободу слова в умовах війни, та виконати всі поставлені дослідженням завдання.

Структура магістерської роботи складається з титульного аркушу, змісту, вступу, трьох розділів: в першому розділу – 4 підпункти, в другому – 2 підпункти, третьому - 3 підпункти, висновків, списку використаних джерел. Загальний обсяг кваліфікаційної (магістерської) роботи становить 91 сторінку.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СВОБОДИ СЛОВА

1.1. Визначення інформаційної безпеки – підходи та аспекти

Інформаційна безпека – проблема, вивченням якої займається декілька дисциплін. Як науковий напрямок, вона має кілька аспектів - правовий, економічний, психологічний, управлінський, культурологічний, організаційно-технічний та інші.

Науковці, розглядаючи тему інформаційної безпеки звертають увагу на розповсюдження інформаційних технологій в кожній сфері життєдіяльності суспільства. Навіть озброєнні конфлікти переходять в новий інформаційний простір, коли інформація з фронту отримується в режимі онлайн, що в свою чергу створює багато інформаційного шуму та дезінформації. Однак за останні роки, коли в геополітичному просторі світу інформаційні технології та інформація в цілому отримали визначальне значення, саме правовий аспект вивчення інформаційної безпеки особистості, суспільства і держави виходить на перший план.

Варто зазначити, що у науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека».

В наш час термін «інформаційна безпека» широко застосовується в наукових статтях, навчальних посібниках та публікаціях, а також займає ключове місце в нормативно-правових документах різних сфер і рівнів. «Однак в інтерпретаціях поняття немає єдності, в тому числі через визначення поняття різними мовами. Тобто можна сказати, що вчені які показують саме відсутність єдиної загально-централізованої дефініції у сфері інформаційної безпеки, вказують на недоліки законодавчого визначення прямо пояснюють методологічну невизначеність положень та термінів, що може знижувати ефективність наукових досліджень у галузі»[1].

Поняття «інформаційна безпека» з’явилося наприкінці 80-х у праці німецького вченого Г.Одермана. У ній йдеться про важливий інформаційний

компонент у міжнародній безпеці та робиться спроба розглянути проблеми безпеки, які пов’язані з інформаційними загрозами комплексно. А у вітчизняній літературі починаючи з кінці 1991 – початку 1992 спостерігається тенденція до відкритого дослідження проблеми інформаційної безпеки як окремого питання [2].

На думку більшості дослідників під інформаційною безпекою слід розуміти стан захищеності національних інтересів України в інформаційній сфері, що включає в себе збалансованість інтересів особи, суспільства та держави від внутрішніх та зовнішніх загроз..

На думку В. Цимбалюка та А. Бабінської, у запозиченнях із Інтернету «інформаційну безпеку України слід розглядати як стан захищеності її національних інтересів в інформаційній сфері, які в свою чергу визначаються сукупністю збалансованих інтересів особи, суспільства й держави» [3].

О. Ніщименко визначає інформаційну безпеку «станом захисту національних інтересів України, які складаються з збалансованих інтересів особи, суспільства та держави від загроз (внутрішніх і зовнішніх), що відповідає принципам національної безпеки в сучасній інформаційній сфери» [4].

О. Кісілевич-Чорнойван підкреслює, що ««інформаційна безпека – це складова частина національної безпеки, яка, по-перше, відображає стан захищеності життєво важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму нанесення шкоди через неповність, не своєчасність та не достовірність інформації або негативного інформаційного впливу через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації». По-друге, «стан захищеності інформаційного середовища/простору загалом, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави» [5].

Досліджуючи питання інформаційної безпеки Л. Кочубей зазначає, що це «стан захищеності життєво важливих інтересів, включаючи інформаційну

озброєність держави, суспільства, окремої особистості, за якого жодні інформаційні виклики неспроможні спричинити деструктивні думки і дії» [6].

Згідно ширшого тлумачення інформаційної безпеки - є невід'ємною, наскрізною характеристикою сучасного суспільства загалом.

В Україні чимало науковців застосовують інтегральний підхід. Так, В. Ліпкан, вважає, що «інформаційна безпека визначатиметься за допомогою окреслення найбільш важливих її сутнісних ознак з урахуванням постійної динаміки інформаційних систем і становлення не лише інформаційного суспільства а й інформаційної цивілізації» [7].

Розглядаючи правову галузь, В. Гурковський зазначає, «національна інформаційна безпека України – це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державо-утворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів» [8].

На думку А. Нашинець-Наумової «Інформаційна безпека: питання правового регулювання», від розуміння інформаційної безпеки, як юридичної концепції соціальної реальності, залежить методологія, тому що вчення про сутність – це вчення про метод його вивчення» [9].

Д. Ловцов та інші розглядають розуміння інформаційної безпеки в контексті «засобу соціальної діяльності, яка спрямована на пізнання суспільства, його функціонування тощо; також запровадження нових теорій і концепцій на практиці, через науково-правовий метод» [10].

Інший підхід науковця В. Антонюка розглядає інформаційну безпеку, як «явище суспільного життя, тобто не тільки як науковий пошук істини»[11].

З точки зору П. Біленчука, «безпека в інформаційній сфері передбачає забезпечення інформаційного суверенітету; удосконалення державного

регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження сучасних технологій у цій сфері, наповнення інформаційного простору достовірною інформацією; забезпечення конституційного права громадян на свободу слова, доступу до інформації, недопущення протиправного втручання органів державної влади у діяльність засобів масової інформації; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери держави» [12].

Про інформаційний суверенітет також пише і О. Вайцеховська [13] – «Осмислення сукупності інформаційних процесів щодо забезпечення їх безпеки має велике значення як для окремого суспільства, так і міжнародного співтовариства в цілому».

Такі науковці як Н. Нижник, Г. Ситник, В. Білоус під інформаційною безпекою розуміють «стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни» [14].

На думку В. Ярочкіна та Т. Шевцової «інформаційна безпека – це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення й прав суб’єктів, що беруть участь в інформаційній діяльності». У даному визначенні інформаційна безпека зводиться до захисту інформації, що не зовсім відбиває її сутність [15].

Л. Харченко, Н. Ліпкан, О. Логінов визначили, що «інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України» [16].

В правовому вимірі інформаційна безпека є невід’ємною частиною сучасної системи управління правової держави і вагомим чинником формування

громадянського суспільства, а також входить до ключового розуміння питання національної безпеки. На думку А. Нашинець-Наумової «правовим відображенням інформаційної безпеки є сукупність правових умов, що забезпечують оптимальне функціонування і розвиток суб'єктів в інформаційному середовищі. Таке визначення по суті дозволяє говорити про інформаційно-правову безпеку й ототожнює її з режимом законності в інформаційній сфері» [9].

З правової точки зору поняття «інформаційна безпека» міститься в декількох законодавчих актах. Конституція України визначає: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу»[17, ст. 17].

Стратегія інформаційної безпеки (далі - Стратегія)[18], містить наступне визначення поняття ««інформаційна безпека України» - це складова частина національної безпеки України, стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належим чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існування ефективної системи захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Тобто відповідно до визначення, одним із елементів інформаційної безпеки є стан захищеності демократичного ладу, що сприяє забезпеченню конституційних прав і свобод людини».

За висновком А. Нашинець-Наумової система забезпечення інформаційної безпеки – це внутрішня структура, систематизована сукупність, єдність,

взаємозв'язок і диференціація окремих її елементів (об'єкт, суб'єкти, основні характеристики, рівні інформаційної безпеки та перелік загроз) [9].

Об'єктом системи забезпечення інформаційної безпеки є безпосередньо інформаційна безпека. До суб'єктів такої системи можна віднести всі органи та інституції, які в державі дотичні до забезпечення інформаційної безпеки.

Науковці пропонують розглядати такі рівні інформаційної безпеки: нормативно-правовий рівень – закони, нормативно-правові акти тощо; адміністративний рівень – дії загального характеру, які вживаються органами державного управління; процедурний рівень – конкретні процедури забезпечення інформаційної безпеки; програмно-технічний рівень – конкретні технічні заходи забезпечення інформаційної безпеки.

У свою чергу В. Ліпкан пропонує розглядати такі рівні інформаційної безпеки: «стратегічний рівень – Рада національної безпеки і оборони України та Кабінет Міністрів України; тактичний рівень – центральні органи виконавчої влади; оперативний рівень – місцеві органи виконавчої влади» [19].

Як зазначає А. Нашинець-Наумова «законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Більшість людей не здійснюють протиправних дій не тому, що це технічно неможливо, а тому, що це засуджується і / або карається суспільством, тому, що так чинити не прийнято…

…До адміністративного рівня інформаційної безпеки відносяться дії загального характеру. Головна мета заходів адміністративного рівня – сформувати програму робіт в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ…

….Процедурний рівень, орієнтований на людей, а не на технічні засоби. Саме люди формують режим інформаційної безпеки, і вони ж виявляються головною загрозою, тому «людський фактор» заслуговує особливої уваги. Слід усвідомити ту ступінь залежності від комп'ютерної обробки даних, в яку потрапило сучасне суспільство. ..

…Програмно-технічний рівень, тобто рівень, спрямований на контроль комп'ютерних сутностей – обладнання, програм та/або даних, утворюють останній і найважливіший рубіж інформаційної безпеки» [20].

Доречним є віднесення до рівнів забезпечення інформаційної безпеки ті, які пропонує розглядати В. Цимбалюк. За основу поділу він визначає такий критерій, як середовище, в якому знаходиться інформація: «а) соціальне середовище (окрема людина, спільноти людей, держава); б) інженерно-технологічне (машинне, апаратно-програмне, автоматичне, телекомунікаційне) середовище; в) соціотехнічне (людино-машинне) середовище. Кожен зазначений рівень щодо середовища об'єктивно доповнює і взаємо обумовлює інші рівні, в основі, утворюючи триєдину гіперсистему – систему забезпечення інформаційної безпеки» [21].

Аналізуючи поняття «інформаційна безпека», можемо зробити висновок, що для одних науковців воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію тощо.

1.2. Ключова роль інформації та свободи слова під час війни

На сьогодні роль інформації – критична як ніколи.

У сучасних умовах застосування інформації як засобу ведення війни може викликати наслідки, цілком порівнянні за силою своєї дії з «традиційною» зброєю. Аналіз використання сучасних технологій іншими державами вимагає здійснення системи спеціальних заходів щодо забезпечення інформаційної безпеки, в т.ч. міжнародної [22].

На думку І. Котерліна «сьогоднішні воєнні реалії чітко демонструють, що інформація є зброєю «масового ураження». Тому необхідно створити ефективний механізм, який би забезпечив державну інформаційну безпеку і дотримання прав людини та водночас дозволив би людям не відчувати ефекту посягань на свободи та демократію» [23].

На думку директора Українського інституту національної пам'яті Антона Дробовича, «полем бою є не тільки терени України. В інформаційному просторі

це, мабуть, найбільша медійна війна в історії людства. Це дуже публічна війна. Такого не було під час Другої світової. Навіть війна в Сирії, де Росія теж свій п’ятак вставила, не було стільки людей, які в зоні військових дій із гаджетами і Інтернетом, які це покажуть. Неймовірна кількість зафіксованих матеріалів із вебкамер, які стежать, як мародерять росіяни. Такого не було ніколи» [24].

Саме тому багато дослідників уважають, що забезпечення військової безпеки в XXI ст. все більше залежатиме від інформаційних чинників. Відомий американський футуролог О. Тоффлер у книзі «Війна та Анти-війна» [25] зазначає, що «інформація стає найважливішим військово-стратегічним ресурсом щонайменше або навіть важливішим, аніж традиційні види озброєнь і військової техніки. А це означає, що держава, яка дбає про свій оборонний потенціал, має приділяти величезну увагу розвитку методів інформаційної протидії та інформаційного впливу».

Відповідно до Конституції України «кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя» [17, ст. 34].

Оскільки в законодавстві відсутні чіткі критерії того, чи шкодять певні слова або тексти національній безпеці чи збереженню територіальної цілісності, виникає проблема у практичному застосуванні цієї статті Конституції України в контексті запровадження обмежень свободи слова. Ця проблема є об’єктивною для воєнного стану.

«Кожна людина має право на свободу вираження своїх поглядів шляхом збирання та розповсюдження інформації та ідей, без будь-якого втручання держави». У 1948 році стаття 19 Загальної декларації прав людини проголосила

це право як принцип демократичного статусу кожної вільної особи, зазначивши, що це право включає свободу дотримуватися своїх переконань та шукати, одержувати та поширювати інформацію та ідеї будь-яким способом та незалежно від кордонів [26]. Це ж саме тлумачення міститься в частині 2 статті 19 Міжнародного пакту про громадянські та політичні права 1966 року, який розширив поняття свободи слова, включивши такі форми самовираження, як друковані засоби та інші художні форми [27]. Таким чином, право на свободу вираження поглядів охоплює всі можливі форми його реалізації, включаючи свободу журналістики, викладення своїх думок та ідей у друкованих медіа, в онлайн-медіа та в інших формах мистецтва. Обидва міжнародні акти встановлюють загальносвітові основи справедливого та демократичного порядку, проте текст Пакту розширює поняття свободи слова, зазначаючи, що вона охоплює різноманітні форми самовираження.

З введенням воєнного стану з 24.02.2022 року згідно Указу Президента України «тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30–34, 38, 39, 41–44, 53 Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану»» [28].

Одним із завдань держави сьогодні є створенням належних умов для вільного вираження кожною особою своїх поглядів та переконань, усунення перешкод при реалізації цього права та притягнення винних осіб до відповідальності. Однак гарантуючи свободу слова українська держава зіткнулася із іншою проблемою – спотворення інформації та використання її проти України у якості зброї в інформаційній війні або поширення інформації, може загрожувати національній безпеці громадян України.

Так, Саломе Самадашвили наголошує, що «російська пропаганда ефективно використовує демократію і свободу слова для просування своїх пропагандистських інтересів на шкоду демократії і свободі слова» [29].

Тому на сьогодні не менш важливим завданням є забезпечення інформаційної безпеки України та віднайдення балансу між реалізацією права на свободу слова в комунікаціях та інформаційною безпекою країни.

На думку авторів «в умовах війни свобода слова, як одна з найважливіших свобод, завжди проходить випробування перед суспільством, яке ставить досить прагматичні питання: чи може поступитися держава свободою слова в обмін на безпеку та суспільну злагоду? чи є свобода слова нагальною потребою та невід'ємним елементом демократичної держави в умовах кризи?» [32].

Тому корисною з огляду на цю ситуацію буде згадка відомої «теорії чотирьох цінностей» американського професора Т.Емерсона, який виокремлював «чотири суспільні цінності, на охорону яких спрямована свобода слова:

- забезпечення розвитку особистості;
- здобуття знань і встановлення істини;
- забезпечення участі всіх членів суспільства у процесі прийняття державних рішень;
- формування більш здатного до змін, а відповідно – більш життєздатного суспільства через баланс здорових публічних обговорень та необхідною згодою громадян стосовно прийняття рішень» [30].

Що стосується міжнародної практики обмеження свободи слова, то варто зазначити наступне. Правомірність обмежень свободи слова підлягає відомому стандарту ЄСПЛ, який розглядає наступні компоненти втручання держави у реалізацію прав людини і основоположних свобод:

- чи було втручання в свободу слова «встановлене законом»;
- чи переслідувало таке втручання «правомірну мету»;
- чи було таке втручання «необхідним у демократичному суспільстві».

Практика ЄСПЛ знайшла своє відображення в Рекомендації Комітету міністрів Ради Європи «Про захист свободи вираження поглядів та інформації в кризові часи»:

«Держави-члени не повинні обмежувати доступ громадян до інформації в кризові часи та виходити за межі обмежень, передбачених у статті 10 Європейської Конвенції про права людини й розтлумачених у практиці Європейського суду з прав людини. Держави-члени не повинні запроваджувати в кризові часи обмеження на свободу вираження поглядів та інформації на невиразних умовах. Підбурюванням до насильства та порушення громадського порядку потрібно надавати пропорційне та чітке визначення» [31].

Як вірно відмічено авторами «не зважаючи на свою надзвичайну важливість, національна безпека не може застосовуватися як правомірна підстава без будь-яких обмежень для втручання у свободу слова. Одне з перших таких обмежень викладено в рішенні Верховного Суду Нідерландів ще у 1916 р. Тоді суд визнав, що «публікація не може бути заборонена для оприлюднення тільки на тій підставі, що вона може загрожувати національній безпеці». На думку Суду, уряд мав довести, спираючись на власний досвід, що можна обґрунтовано вважати, що за наявних обставин такий наслідок матиме місце в разі оприлюднення такої публікації. Ця логіка згодом була підтримана як національними європейськими судами, так й ЄСПЛ (Observer and Guardian v. United Kingdom (1991)» [32].

Також цікавим для нас є Рабатський план дій [33], який надає розгорнуту точку зору міжнародних експертів щодо речей, які має заборонити держава, не порушуючи при цьому свободу слова.

Пункт 14 Рабатського плану дій серед таких речей зазначає «висловлювання, що підпадають під визначення «мови ворожнечі». Вони можуть бути обмежені «... на різних підставах, таких як повага до прав інших, громадський порядок, а іноді навіть міркування національної безпеки. Держави також зобов’язані «заборонити» висловлювання, що зводяться до «спонукання» до дискримінації, ворожнечі або насильства».

Проте обмеження свободи слова має бути винятковою мірою. Саме тому, на думку авторів Рабатського плану дій, обмеження повинні відповідати наступним вимогам: «вони мають бути чітко і вузько визначені, відповідати нагальній громадській необхідності, вони повинні найменшою з усіх доступних заходів мірою вторгатися в громадське і особисте життя, не бути занадто широкими (тобто не припускати широких або невизначених обмежень свободи слова), бути співрозмірними в тому сенсі, що користь для інтересів, що захищаються, перевищує збиток, спричинений свободі висловлювання думки» (п.18).

Інформація, представлена у певному вигляді, може впливати на поведінку людей, спонукаючи їх до здійснення дій, які можуть протирічити їхнім інтересам. Це чітко проявилося під час гібридної (інформаційної) агресії РФ проти України у 2013-2014 роках: значна частина населення, через історичні чинники або через слабкість пропагандистських структур України, була під впливом російських ЗМІ, що спричинило розповсюдження антиукраїнських настроїв та підтримку агресора.

Зазвичай першим кроком російської окупації будь-якої території є активізація їхніх медіа, розповсюдження радіопередач та телепрограм, а також розміщення пропагандистської реклами у всьому регіоні. Вони докладають значних зусиль, щоб вплинути на світогляд українських громадян.

Зважаючи на те, що національний інформаційний простір є відкритим, це створює реальну загрозу для інформаційного та психологічного впливу на суспільну свідомість. Тому, якщо не приділяти уваги захисту інформаційного простору під час воєнного стану, можуть скластися умови для маніпулювання інформацією з боку противника.

Поширеним засобом використання інформації з метою цілеспрямованого впливу на свідомість людей та соціуму є пропаганда. «Пропаганда – це контроль свідомості мас шляхом спотворення інформації та нав’язування односторонніх, суб’єктивних, а часом і відверто неправдивих суджень із використанням засобів масової інформації або будь-яким іншим способом масового впливу» [34].

Найбільш небезпечною складовою частиною пропаганди є інформаційно-психологічний вплив. Такий вплив може викликати зміну цінностей, життєвих позицій, орієнтирів, світогляду в цілому. У протистоянні російській агресії населення України постійно піддається інформаційно-психологічним впливам пропаганди РФ.

«Метою негативної пропаганди є розпалювання соціальної ворожнечі, загострення соціальних конфліктів, загострення суперечностей у суспільстві, пробудження в людей низьких інстинктів тощо» [34].

Справедливість тези М. Борщова, за якою «в сучасному світі інформація подається у великих дозах, проблемою стає пошук потрібної інформації, актуальною стає не захист інформації, а захист від інформації» [35].

Доречною є теза Юринця Ю., що «у цьому сенсі слід визнати перспективним вироблення критеріїв відбору та обмеження негативної інформації на основі використання систем автоматичної обробки тексту в інформаційно-пошукових системах. Такі підходи повинні, зокрема, стати частиною державної інформаційної політики у сфері інформаційної безпеки та, зокрема, включатися в офіційні методики здійснення відповідних експертиз» [36].

Таким чином, за переконаннями Залєвської та Удренаса «головним інструментом боротьби України проти російської дезінформації під час воєнного стану є правда, яку потрібно доносити не лише до внутрішньої, а й до закордонної аудиторії. Також велике значення мають медіакультура та медіаграмотність суспільства» [110].

1.3. Державна політика щодо забезпечення інформаційної безпеки та свободи слова під час війни

Цивілізація вже набула такого розвитку, коли інформація стала повноцінним ресурсом. Забезпечення інформаційної політики сьогодні, це час це не менш важливо ніж напрямок державної політики.

Захист національної безпеки визначається Конституцією України як найважливіша функція держави [17, ст. 17]. Основною метою документів, що приймаються в Україні з 1997 року є розбудова напрямків політики національної безпеки та протидія інформаційній експансії іноземних держав.

До основних документів, що становлять законодавчу базу забезпечення інформаційної безпеки, відносяться наступні документи:

- Конституція України;
- Закон України «Про національну безпеку України» [37];
- Закон України «Про інформацію» [38];
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [39];
- Закон України «Про державну таємницю» [40];
- Закон України «Про медіа» [41];
- Закон України «Про захист персональних даних» [42];
- Закон України «Про доступ до публічної інформації» [43];
- Закон України «Про боротьбу з тероризмом» [44];
- Указ Президента України «Про рішення Рад національної безпеки і оборони України від 15.10.2021 «Про Стратегію інформаційної безпеки» [18];
- Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 14.09.2020 «Про Стратегію національної безпеки України» [45];
- Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України» [46];
- Указ в.о. Президента України «Про рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28.04.2014 [47];
- Конвенція Ради Європи «Про кіберзлочинність» [48];
- Рекомендації Комітету міністрів Ради Європи «Про захист свободи вираження поглядів та інформації в кризові часи»;

Прийнята у 2021 році Стратегія передбачає комплексну взаємодію на основі Конституції України, законів України, Стратегії національної безпеки України, Стратегією кібербезпеки України, затвердженою, а також міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України.

Відповідно до п. Загальних положень стратегії метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина.

Стратегія містить основні визначення, що характеризують сферу забезпечення інформаційної безпеки, такі як інформаційна безпека України, інформаційна загроза, інформаційні заходи оборони держави, кризові, аникризові, урядові та стратегічні комунікації, стратегічний наратив.

Як зазначалося вище у розділі 1.1 Стратегія також містить перелік потенційних інформаційних загроз як глобальних, так і національних, серед яких: «інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав» [18].

Відповідно до розділу «Очікувані результати» Стратегії очікуваними результатами реалізації Стратегії визначено захищений інформаційний простір України, ефективне функціонування системи стратегічних комунікацій, здійснення ефективної протидії поширенню незаконного контенту, забезпечення сталого процесу інформаційної реінтеграції громадян України, які проживають на тимчасово окупованих територіях України, та поширення українського телерадіомовлення на територіях України, прилеглих до тимчасово окупованих територій, суттєве підвищення рівня медіа-культури та медіа-грамотності населення, дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя, забезпечення захисту прав журналістів, формування української громадянської ідентичності.

Реалізація Стратегії розрахована на період до 2025 року. На виконання поставлених цілей Кабінетом Міністрів України тільки 30 березня 2023 року було прийнято план заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року [49].

Серед заходів, запланованих в межах окресленого Плану, на думку Р. Грицая «особливої уваги заслуговує проект «Spravdi», що спрямований на протидію дезінформаційним кампаніям та деструктивній пропаганді, фахова підготовка спеціалістів з раннього виявлення, прогнозування та запобігання гібридним загрозам, а також забезпечення реалізації Національного проєкту з медіаграмотності «Фільтр» [108].

У той же час, ефективне протистояння інформаційній агресії, зокрема з боку РФ, може бути ускладненим, якщо в суспільстві відсутнє критичне мислення та уміння критично оцінювати інформацію. Додатковим механізмом протидії російській пропаганді можуть стати незалежні ініціативи, що виконують завдання боротьби з інформаційними загрозами шляхом перевірки та спростування маніпулятивної інформації та підвищення рівня медіаграмотності населення.

Оскільки інформаційна безпека є невід'ємною складовою національної безпеки, то законодавча визначеність щодо параметрів інформаційної безпеки є критичною для реагування на загострення збройного конфлікту і ведення нового типу війни на сьогоднішній день.

Державна політика, а саме правове забезпечення інформаційної безпеки України є актуальною саме зараз, оскільки країна знаходиться у воєнному стані та протистоїть не тільки військовим загрозам, а й інформаційним атакам з боку РФ. В тому числі актуальність цього питання зумовлена євроінтеграційними процесами в які активно залучена Україна.

О. Стоєцький визначає «інституційний механізм інформаційної безпеки як організовану державою сукупність суб'єктів державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та

завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства України» [50].

Відповідно до Стратегії інституційною базою забезпечення інформаційної безпеки в Україні, складають наступні органи:

- Кабінет Міністрів України;
- Рада національної безпеки та оборони України;
- Міністерство культури та інформаційної політики України (далі – МКІП);
- Центр протидії дезінформації;
- Міністерство закордонних справ України;
- Міністерство оборони України;
- Служба безпеки України;
- розвідувальні органи;
- Національна рада України з питань телебачення і радіомовлення;
- інші органи державної влади та органи місцевого самоврядування;
- наукові та науково-дослідні установи, які забезпечують науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики.

Центральним органом виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері, є МКІП. Відповідно до Положення [51] до повноважень МКІП відносяться:

- «визначає перспективи та пріоритетні напрями розвитку у сферах культури та мистецтв, інформаційного суверенітету (щодо повноважень з управління цілісним майновим комплексом Українського національного інформаційного агентства «Укрінформ»), інформаційної безпеки України;
- бере участь у формуванні державної інформаційної політики;
- вживає заходів щодо захисту прав громадян на вільне збирання, зберігання, використання й поширення інформації, зокрема на тимчасово окупованих територіях, відповідно до покладених на МКІП завдань;

- здійснює в межах повноважень, передбачених законом, координацію діяльності органів виконавчої влади та взаємодію з органами місцевого самоврядування з питань, віднесених до компетенції МКІП;

- надає методичну та практичну допомогу засобам масової інформації у сфері інформаційного суверенітету України (щодо повноважень з управління цілісним майновим комплексом Українського національного інформаційного агентства «Укрінформ») та інформаційної безпеки;

- бере участь у формуванні єдиного інформаційного простору, сприянні розвитку інформаційного суспільства;

- розробляє заходи щодо запобігання внутрішнього й зовнішнього інформаційного впливу, який загрожує інформаційній безпеці держави, суспільства, особи;

- розробляє та вносить на розгляд Кабінету Міністрів України проєкти нормативно-правових документів щодо інформування громадськості з питань європейської та євроатлантичної інтеграції України;

- розробляє плани заходів щодо сприяння незалежності засобів масової інформації, захисту прав журналістів та споживачів інформаційної продукції;

- організовує проведення досліджень впливу результатів діяльності засобів масової інформації на суспільну свідомість; сприяє розбудові в Україні системи державних стратегічних комунікацій;

- розробляє разом з МЗС плани заходів та програмні документи щодо позиціонування України у світі;

- сприяє дотриманню в Україні свободи слова; розробляє та виносить на розгляд Кабінету Міністрів України програмні документи у сфері захисту інформаційного простору України від зовнішнього інформаційного впливу;

- забезпечує моніторинг інформації у вітчизняних та іноземних засобах масової інформації;

- утворює спеціалізовані експертні ради»[51, с. 3].

Комплексність функціоналу Міністерства виокремлює особливість його позиції в системі забезпечення інформаційної безпеки країни.

Важливим чинником вдосконалення функціонування інституційного механізму забезпечення інформаційної безпеки як цілісної системи є посилення координації всіх його складових частин, представлених як гуманітарним, так і силовим блоками відомств. Відповідно до Стратегії Рада національної безпеки і оборони України є координаційним органом з питань національної безпеки і оборони при Президентові України та виконує функцію координації діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері. Повноваження РНБО закріплені Конституцією України [17, ст. 107], а також Законом України «Про Раду національної безпеки і оборони»[52].

Ще одним органом, що відповідає за забезпечення виявлення, прогнозування та запобігання інформаційним загрозам є Центр протидії дезінформації при Раді національної безпеки та оборони. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

1.4. Зарубіжний досвід забезпечення інформаційної безпеки

Вивчаючи питання інформаційної безпеки слід приділити увагу міжнародному досвіду забезпечення інформаційної безпеки людини, суспільства і держави для запозичення кращих практик та стратегій. Для того щоб перейти до більш конкретних прикладів держав та інституцій слід розглянути інформаційну безпеку через призму міжнародного права.

Сучасна людина очікує отримати від держави та міжнародних організацій захисту їх миру, безпеки від загроз, які з’явились або трансформувались нового етапу суспільного розвитку. Фактично «інформаційний простів став новим виміром геополітичного суперництва, від якого залежить безпека людей та суспільний розвиток» [53].

Міжнародна інформаційна безпека за термінологією ООН – захищеність глобальної інформаційної системи від терористичних, злочинних і військово-політичних загроз. Сучасні концепції міжнародної інформаційної безпеки в дослідженнях І. Забари охарактеризовані «симетричним усвідомленням і розумінням місця і значення інформаційних технологій, їх взаємодія в кіберпросторі, їх роль в реалізації загальної концепції; необхідність захисту національних, глобальних інформаційно-комунікаційних мереж і систем; чисельність та важливість загроз; неефективності існуючих стратегій; необхідність об'єднання з ціллю збереження і розширення внеску у забезпеченні безпеки та цілісності держав; необхідність співпраці в розробці міжнародних стратегій зменшення ризиків для інформаційно-комунікативних технологій» [54].

Відповідно до дослідження Є.А. Макаренко «міжнародна інформаційна безпека розглядається як взаємодія акторів для підтримки сталого миру на основі захисту інформаційної сфери, інфраструктури на глобальному рівні, суспільної відповідальності й свідомості світової спільноти від інформаційних загроз: реальних і потенційних» [55].

Основні міжнародні нормативно-правові норми для розуміння забезпечення міжнародної інформаційної безпеки закріпленні у Статуті ООН, а також в ряді інших нормативно-правових актах.

На сьогоднішній день співпраця з НАТО вийшла на значно новий рівень, враховуючи відкриту війну Росії проти України, тому необхідно зрозуміти суть інформаційної політики і забезпечення безпеки інформації у системі цієї організації.

Засади політики НАТО щодо забезпечення безпеки інформації прописані у Документі C-M(2002)49-REV1 [56]. Принципом безпеки інформації в системі Альянсу є зберігання степені захисту інформації протягом усього цикли її використання, починаючі від джерела, при цьому контроль має унеможливити її витік.

В організації існує Комітет внутрішньої безпеки НАТО, завдання якого в тому числі пов’язані із забезпеченням захисту інформації. Це є дорадчим органом при Північноатлантичній Раді з питань безпеки. Втім, усередині Альянсу функції керівництва виконує національний уповноважений орган з безпеки інформації.

Взагалі в Європейському Союзі відсутня єдина модель національної системи забезпечення інформаційної безпеки. Європейські країни будують власні моделі правового забезпечення, протидії кіберзагрозам тощо. Як і по відношенню до НАТО, Україна має орієнтуватись на інформаційні стратегії країн-учасниць Європейського Союзу, зокрема провідним орієнтиром мають стати країни Центральної Європи, адже в них є успішний досвід будування оптимальної моделі інформаційного суспільства. Так, вони створюють розвинену інфраструктура інформаційних технологій.

Ідея забезпечення міжнародної інформаційної безпеки вперше отримала практичну реалізацію в Резолюції Генеральної Асамблеї ООН A/RES/53/70. Цей документ започаткував спільне обговорення питань створення абсолютно нового міжнародно-правового режиму, структурним елементом якого в перспективі стали інформація, інформаційна технологія і методи її використання [57]. Резолюція Генеральної Асамблеї ООН A/RES/54/49 вперше вказала на загрози міжнародній безпеці інформаційного простору стосовно не лише до цивільної, а також до військової сфери [58].

За матеріалами Яковлева П., важливим є досвід забезпечення інформаційної безпеки Сполученими Штатами Америки (США), як одної із самих впливових у військовому відношення країною. США одними з перших створили особливу систему захисту національного інформаційного суверенітету і безпеки інформаційних ресурсів.

Після Другої світової війни основні законодавчі принципи забезпечення інформаційної безпеки в США було сформовано, коли американська інформаційна система зіткнулася з руйнівним впливом радянської пропаганди. Структурно законодавство Сполучених Штатів у цій сфері включає як

федеральні закони, так і закони окремих штатів. Незважаючи на значні різниці між законами штатів, акти з інформаційного законодавства є одними з найбільш уніфікованих. Правову базу адміністрування інформаційної безпеки в США становлять закони «Про охорону особистих таємниць» (1974), «Про таємницю» (1974), «Про висвітлення діяльності уряду», «Про право на фінансову таємницю» (1978), «Про доступ до інформації про діяльність ЦРУ» (1984), «Про безпеку комп'ютерних систем» (1987), «Про комп'ютерне шахрайство та зловживання» (1986). Пізніше, з прийняттям у 1987 Закону «Про забезпечення безпеки ЕОМ», вперше у правовій системі США з'явився інститут «інформації обмеженого доступу», під якою розуміють несекретну, але важливу з точки зору національної безпеки несекретну інформацію урядових відомств, а також інформаційні дані, що формуються і циркулюють або обробляються в інформаційно-телекомунікаційних системах корпорацій і приватних фірм, що працюють на замовлення уряду США. Також важливе значення мають Директиви президента США, який очолює Раду національної безпеки. [109].

За матеріалами інтернет «у 1990-х на хвилі активізації і глобалізації інформаційних відносин було введено у дію федеральні закони «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997)»» [59]. В останнє десятиліття XX ст. в сфері забезпечення інформаційної безпеки в США все більшу роль починають відігравати військові, оскільки інформаційні технології стають повноцінною складовою військових потенціалів. У 1992 р. було введено у дію Директиву Міністерства оборони США TS «Інформаційна війна», якою визначено складові «інформаційної війни»: «психологічний вплив на супротивника, оперативна безпека, введення супротивника в оману, електронне втручання, інформаційна розвідка, виведення з ладу системи управління вірогідного супротивника, інформаційний захист власної системи управління під час бойових зіткнень. Фактично, введення цієї Директиви на юридичному рівні інформаційну безпеку прирівняло до військової безпеки. Більш того, основним концептом державного регулювання інформаційної безпеки США стало управління інформаційними ресурсами таким чином, щоб

одночасно убезпечити від посягань власну систему інформаційної безпеки і вивезти з ладу систему інформаційної безпеки ймовірного супротивника, взяти під контроль його стратегічні комунікації» [60]. Слід зазначити, що «американська модель забезпечення інформаційної безпеки цілком допускає ведення інформаційних війн, що включає у себе планування і проведення активних інформаційно-психологічних операцій як інструменту зовнішньої політики. При цьому, як зазначають експерти використання подібних методів не призводить до виникнення прямої воєнної конфронтації з державами і в цілому мирні відносини з ними зберігаються» [61; 62; 109].

При Бараку Обамі «цифрова інфраструктура США була оголошена «стратегічною національною цінністю», а захист цієї інфраструктури – національним пріоритетом» [63]. В основу цієї тези американський лідер поклав напрацювання наукової доктрини американського дослідника аспектів забезпечення інформаційної безпеки Маршалла Макклюєна про те, що «в наш час економічні зв‘язки і відносини усе більше набирають форму обміну знаннями, а не обміну товарами. Відповідно, боротьба за гуманітарні ресурси, капітал, ринки збуту стають другорядними, тоді як головним зараз стає доступ до інформаційних ресурсів, знань, що призводить до того, що війни ведуться вже більше в інформаційному просторі та за допомогою інформаційних видів озброєнь» [64].

У 2010 році президент США підписав «Ініціативу зі всеосяжної національної кібербезпеки», що доповнила Військову доктрину США. Це відображало зростаючу увагу до кібербезпеки та потребу уніфікованого підходу до захисту інформаційних ресурсів країни. Нові стратегії та технології, такі як програма «Ейнштейн» для виявлення втручань у державні інформаційні мережі, стали важливими складовими системи забезпечення безпеки.

США також долучилися до боротьби з російською пропагандою в інформаційній сфері. У грудні 2014 року Конгрес США прийняв резолюцію, в якій закликав президента та Держдепартамент розробити стратегію виробництва та поширення новин та іншої інформації російською мовою у країнах з

російськомовним населенням. Також було виділено кошти на програми російською мовою. У березні 2016 року законопроект «Про боротьбу з дезінформацією та пропагандою» було подано до американського Сенату. У документі наголошується на необхідності координування дій з країнами-союзницями та країнами-партнерами, передусім тими, які є мішенню для операцій інших держав з дезінформації, міжнародними організаціями та суб'єктами, такими як The NATO Strategic Communications Centre of Excellence, European Endowment for Democracy, European External Action Service Task Force on Strategic Communications.

У США за забезпечення інформаційної безпеки відповідають: президент США, Агентство національної безпеки (АНБ), Національне управління кібербезпеки відділу внутрішньої безпеки США, Федеральне бюро розслідувань (ФБР) та Центральне розвідувальне управління (ЦРУ). При цьому АНБ координує більше ніж 150 державних організацій і ще більшу кількість приватних, що задіяні в системі забезпечення інформаційної безпеки.

Також цінним для дослідження є досвід Європейського союзу в сфері боротьби з дезінформацією Росії.

Європейський Союз працює над протидією дезінформації, яка поширюється Росією. У вересні 2015 року було створено East StratCom Task Force - робочу групу зі стратегічних комунікацій ЄС. Ця група покликана підвищити ефективність комунікації та просування політики ЄС у відношенні до країн Східного партнерства.

Першим офіційним російськомовним сайтом ЄС став запущений групою у лютому 2018 року сайт European Foreign Affairs Service (EFAS). На сайті оприлюднюють новини та щотижневі дайджести з аналізом прикладів російської пропаганди: від огляду оцінок резонансних PanamaPapers до спотворень перекладу, мовних та стилістичних маніпуляцій, а також інших прийомів з арсеналу російських (і не тільки) преси і телебачення.

На початку квітня 2016 Єврокомісія ухвалила та передала на розгляд Європейському парламенту та Європейській раді «Спільні принципи протидії

гібридним загрозам — відповідь Європейського Союзу» (далі - Спільні принципи ЄС), як протидію розгортання Росією інформаційної агресії в Європі.

У Спільних принципах ЄС наголошується на необхідності вироблення державами-членами узгоджених механізмів реалізації стратегічних комунікацій для підтримки встановлення справжності та протидії дезінформації з метою (публічного) викриття гібридних загроз (п. 3.2). Документ також визначає, що діяльність у сфері стратегічних комунікацій передбачає тісну взаємодію з НАТО (п. 6). До якнайшвидшого застосування Спільних принципів ЄС закликає і резолюція Європарламенту «Стратегічні комунікації ЄС як протидія пропаганді проти третіх сторін».

Метою діяльності The NATO Strategic Communications Centre of Excellence є розвиток спроможності НАТО у сфері стратегічних комунікацій. Цей центр займається науково-аналітичною, навчально-методичною та інформаційно-комунікативною діяльністю. Він розробляє спеціальні навчальні курси зі стратегічних комунікацій, випускає журнал Defence Strategic Communications, проводить дослідження, організовує конференції та семінари з різноманітною тематикою: від ролі сприйняття в сучасному світі до російської інформаційної війни проти України. Центр досліджує також маніпулятивні техніки, перетворення соціальних медіа на зброю та існуючі практики НАТО та її союзників у сфері стратегічних комунікацій.

Інші країни також приймають заходи для протидії російській пропаганді. У Німеччині, наприклад, Федеральний уряд посилив заходи боротьби з шпигунством, пропагандою та дезінформацією Росії. Велика Британія включила проблему російської дезінформації до звіту Комітету з питань оборони Палати громад. У відповідь на цей документ уряд Великої Британії прийняв рішення збільшити фінансування BBC World Service для вироблення програм мовлення російською.

Питання боротьби з дезінформацією з точки зору міжнародного досвіду є дуже важливим при виборі засобів такої боротьби. Демократичні країни, як правило, застосовують більше контрзаходів, які публічно обговорюються

(робочі групи, курси медіаграмотності тощо). Держави авторитарного штибу, як правило, ухвалюють нові закони або поширюють діючі положення на випадки дезінформації та використовують більш жорсткі адміністративні методи.

Нечіткі визначення понять «суспільний інтерес», «громадська безпека», «брехня» в законах іноді використовуються як політичний інструмент для обмеження свободи ЗМІ. Таким чином, застосовується різний рівень обмежень щодо засобів масової інформації. Іноді доходить до кримінального переслідування.

Контроль за поширенням інформації та протидія навмисному поширенню дезінформації стикається з цілою низкою морально-етичних, юридичних, технічних та інших дилем. Не обходиться і без політики, що часто робить дискусію неконструктивною.

Висновки до першого розділу

Отже, підсумовуючи вище зазначене, поняття «інформаційна безпека» є складною конструкцією, що зумовлюється комплексною соціально-правовою природою, завдяки різноманіттю інформаційних відносин в суспільстві; відмінністю суб'єктів інформаційних відносин з власними інтересами, правами та обов'язками залежно від галузі використання.

Можна також зазначити, що дослідження інформаційної безпеки, її нормативно-правовий статус все ще недостатньо систематизовані, не зважаючи на критичну актуальність інформаційної безпеки в контексті воєнного стану в Україні. Тобто механізми забезпечення інформаційної безпеки потребують додаткового аналізу та підходів для їх формування для вирішення поточних завдань щодо захисту країни.

Роль інформації під час війни – критична, і зазвичай розглядається в контексті інформаційної війни або протиборства.

На думку А. Нашинець-Наумової «першочерговими завданнями держави щодо забезпечення інформаційної безпеки у соціальній та гуманітарній сферах є неухильне забезпечення конституційного права кожного на одержання,

використання, поширення та зберігання інформації, на вільне вираження своїх поглядів на основі ефективного використання новітніх засобів обміну інформацією; вироблення та просування на світовому рівні власного інформаційного продукту» [9].

На думку авторів «прагнення органів влади до перемоги у інформаційній війні наразі призводить до спроб недостатньо обґрунтованого обмеження права на свободу слова, в тому числі шляхом встановлення кримінальної відповідальності за поширення або сприяння поширенню суспільно важливої інформації про проведення воєнних дій. У зв'язку з цим наявна необхідність єдиних стандартів об'єктивності та збалансованості критеріїв оцінки обмеження свободи слова, а також механізмів реагування на мову ворожнечі, контроль за дотриманням яких має здійснювати як держава, так і громадянське суспільство» [32].

Законодавець за роки незалежності сформував потужну правову базу у сфері інформаційної безпеки. Однак, незважаючи на це, практична реалізація правових норм в період воєнного стану знаходиться на досить низькому рівні. Зважаючи на те, що стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, то завданням для української влади повинен стати розвиток ефективного діалогу з ЄС у питаннях забезпечення інформаційної безпеки з врахуванням гармонізації законодавства України з європейським та запозиченням кращих практик правозастосування в цій сфері.

Зарубіжний досвід забезпечення інформаційної безпеки був досліджений задля запозичення найкращих практик ЄС та США в контексті перспективи набуття Україною членства в НАТО та ЄС. Розуміючи ситуацію в світі, де інформаційна безпека стає одним із найважливіших аспектах забезпечення національної та міжнародної безпеки в цілому, Україна навіть під час дії воєнного стану повинна продовжувати адаптувати своє законодавство до міжнародних норм, та якнайшвидше впроваджувати реальні реформи в цьому секторі.

РОЗДІЛ 2. КОМУНІКАЦІЙНІ ЗАГРОЗИ ПІД ЧАС ВІЙНИ В УКРАЇНІ

2.1. Інформаційна війна: поняття та особливості її ведення в Україні

Термін «інформаційна війна» в останні роки все більше стає поняттям у науковому дискурсі, розширюючи своє значення з терміну публіцистичної лексики до складного феномена, що охоплює різноманітні аспекти нашого сучасного життя.

Г. Почепцов говорить про інформаційну війну як «комунікативну технологію впливу на масову свідомість із короткочасними і довгостроковими цілями». Окремим типом інформаційних воєн він виокремлює смислову війну, яка розрахована на більший сегмент населення, ніж інформаційна війна, та на довготривалий період.

«Кожен тип війни спрямований на власний тип простору. Звичайна війна – на простір фізичний, інформаційна – на інформаційний, смислова – на простір когнітивний…Тут можна зауважити, мовляв, інформаційна війна теж має за мету «поцілити в голову людині». …

Інформаційні війни більш помітні, ніж смислові, тому в цьому випадку швидше починають бити на сполох. Смислові війни закриті ореолом естетичної привабливості, тому вони залишаються більш непоміченими» [65].

Агресивно-військовий характер інформаційних впливів знайшов відображення навіть у термінології, яка використовується в описанні явищ інформаційної війни. Ця термінологія сама по собі надає чітке уявлення про цілі і засоби, що ставить перед собою ворожа інформаційна діяльність. Зокрема, рекомендовано розрізняти наступні явища [66-70]:

- «акти зовнішньої інформаційної агресії – акції, реалізація яких може мати негативний вплив на безпеку інформаційного простору держави;
- інформаційна війна – комплекс заходів щодо інформаційного впливу на масову свідомість для зміни поведінки людей і нав’язування їм цілей, які не входять до числа їхніх інтересів, а також захист від подібних впливів.

Під час такої війни використовуються інформаційні технології, що впливають на інформаційні системи, маючи на меті введення в оману масової чи індивідуальної свідомості, виведення з ладу або десинхронізацію процесів управління суспільством та його складовими, передовсім військовими».

На думку Г. Почепцова, «головною відмінністю інформаційної війни є опора на поняття комунікативного резонансу, коли рівень впливу, який вимагається для досягнення певної мети, набагато нижче одержуваного в результаті ефекту. Комунікативний резонанс дозволяє істотно збільшувати охоплення населення, оскільки воно хоче в даний момент почути саме це:

- психологічна війна – комунікативні технології, що спрямовані на внесення змін у поведінку індивіда за допомогою модифікації його моделі світу, що здійснюється шляхом внесення змін в інформаційні потоки;

- стратегічна інформаційна війна – інформаційна війна, під час якої здійснюється вплив на інформаційний та культурний простір об’єкта з метою їх трансформації, що призводить до змін у культурних цінностях, світобаченні та поведінці об’єкта інформаційної агресії;

- інформаційна операція – використання можливостей електронної зброї, комп’ютерних мережевих операцій, психологічних операцій, операцій з військової дезінформації і дезорганізації та операцій безпеки для використання можливостей впливу на людську свідомість з метою руйнування, розкладання або й взагалі перехоплення впливу на прийняття рішень противника, і захисту свого власного рішення» [66].

О. Марунченко в дисертаційному дослідженні акцентує, що «незважаючи на різні тлумачення поняття «інформаційна війна», основною ознакою цього типу кампаній є гостра, агресивна взаємодія протиборчих сторін в інформаційній сфері, яка негативно відбивається на стані політичних комунікацій суспільства в цілому». На його думку, через високу інтенсивність суперечки інформаційні війни погано піддаються управлінню та свідомому регулюванню [71].

Україна виявилася неготовою до викликів інформаційної війни з боку Росії. Як зазначає Ю. Горбань «антиукраїнська пропагандистська кампанія виявила

недостатню сформованість наукових і методологічних обґрунтувань та пояснень щодо дій у подібних ситуаціях, продемонструвала слабку координованість дій державних органів влади, громадянського суспільства, експертного та наукового середовищ, журналістів щодо протидії таким кампаніям» [72].

Як свідчить теорія і практика протидії інформаційним загрозам, для подолання окресленим проблем необхідним є міждисциплінарний підхід, оскільки дані проблеми стосуються інформаційного права, інформаційних технологій, соціології, психології, військової науки. Як зазначає Ю. Турченко «політико-правове регулювання інформаційних відносин в Україні перебуває у стадії формування, відповідно, правовий вакуум позначається і на процесі реформування військової сфери… Провідним інструментом реалізації національних інтересів у галузі суспільно-політичних відносин, як інформаційна сфера, повинно стати право» [73].

Дослідник гібридних воєн Євген Магда на прикладі України чітко і методично показує методи гібридної війни, які застосовуються Росією починаючи з 2013 року. По суті, всі ці методи є складовими інформаційної війни, мета якої передбачає розхитування ситуації всередині держави, а також створення її негативного іміджу на міжнародній арені. Серед зазначених методів хочеться виділити такі:

- ««криве дзеркало» – перекручування та пересмикування фактів;
- «килимове бомбардування дезінформацією» призводить до панічних настроїв та появи численних ліній розколу в українському суспільстві, що має призвести до дестабілізації ситуації всередині країни»;
- «перетягування Заходу» – спроби створити проросійську коаліцію, лобіювання інтересів Росії діючими та колишніми європейськими політиками разом з поширенням інформаційної кампанії щодо формування позитивного образу Росії в Європі;
- «заперечення очевидного» має на меті створювати видимість відсутності агресії» [74].

Володимир Путін у своїй промові-посланні Федеральним зборам РФ 21 лютого 2023 року використав більшість цих методів, проголошуючи, що «США та НАТО прискорено розгортали біля кордонів нашої країни свої армійські бази, секретні біолабораторії, під час маневрів освоювали театр майбутніх воєнних дій, готували підвладний ним київський режим, поневолену ними Україну до великої війни». «Це вони розв'язали війну. А ми використовуємо силу, щоб її зупинити», – запевняв російський диктатор [75].

Методи, які застосовує агресор, дають можливість викривляти оцінку того, що відбувається, деморалізувати громадян. Всі методи ведення інформаційної війни спрямовані на формування стійкої суспільної думки в потрібному маніпуляторам напрямі і закладаються необхідні установки поведінки у свідомості громадян для можливого подальшого управління ними. На думку Євгена Магди «інформаційна війна – це узгоджена діяльність з використання інформації як зброї для ведення бойових дій» [74].

Головним стратегічним національним ресурсом стає інформаційний простір, тобто інформація, мережева інфраструктура та інформаційні технології.

Аналізуючи роль соціальних мереж у сфері інформаційних воєн та місце в ній Росії, В. Новородовський припускає, що «використовуючи facebook як основну інформаційну платформу, створювалася основа для конфлікту» [76]. І мова йде не лише про російсько-українську війну, але й конфлікт у Грузії, Нагорному Карабасі, Придністров'ї. Російські пропагандисти, використовуючи соціальні мережі «вконтакте» та «одноклассники», які були популярні в Україні на початку 2000-х років, формували через певні спільноти меседжі, що були спрямовані на дезорганізацію та дезорієнтацію суспільства. В результаті маніпуляцій та впливу на суспільну свідомість «відбулося поширення ідей «русского мира», що зумовлювало маргіналізацію певних прошарків суспільства і створювало передумови для розгортання сепаратистських рухів на території іншої країни» [76]. Застосування інформації та дезінформації як зброї є потужним елементом путінського режиму в системі просування власних цінностей та наративів.

Найбільш «проникливою» сферою застосування інформаційної зброї є людська свідомість. «Впливаючи на неї відбувається нагромадження нестійкого сприйняття світу, розгубленості, тривожності. Ми можемо з впевненістю сказати, що інформаційна зброя постає в сьогоденні як новий і унікальний вид зброї. Її унікальність у прихованому характері, масштабі застосування та збереженні матеріальних та людських цінностей. «Інформаційна зброя розглядається як засіб ведення інформаційної війни, що є лише ключовим елементом повномасштабної війни» [77].

На думку групи дослідників, «не можна недооцінювати можливості інформаційної зброї у сучасній війні, оскільки це може призвести до фатальної помилки під час подальшої воєнно-політичної боротьби» [77].

Про важливість соціальних мереж та інтернет-майданчиків у розрізі питання інформаційних воєн говорить О. Саган [78]. В умовах інформаційної агресії, на її переконання, «знаково-символічна сфера людини, у якій ключову роль відіграють мова, символічна культура, цінності, зазнає впливу вибірковості значень подій і речей. Вони формують так би мовити, «мозаїчну свідомість», характерною особливістю якої є втрата особистістю змоги критично мислити та адекватно оцінювати реальність. Людина легко піддається мові ворожнечі, а також радикальному та екстремістському впливам. Специфіка організації блогосфери та особливості інтернет-культури перетворили соціальні мережі на небезпечний інструмент пропаганди екстремізму, тероризму та рекрутування молодих людей до лав терористичних організацій» [78].

Разом із тим, мережі Інтернет створюють для поширення небажаного контенту незрівнянно більші можливості, ніж телебачення та радіо. О. Верголяс звертає увагу, що «on-line соціальна мережа, з точки зору інформаційних та комунікативних технологій, створює умови для використання значно більшої кількості інструментів інформаційно-психологічного впливу аніж off-line в силу технологічних можливостей з розміщення та доставки аудіо-та відеоінформації до адресата. On-line мережі мають значно більший спектр можливостей з

розміщення та доставки інформації до адресата найрізноманітнішого характеру (відео, картинки, світлини, текст, аудіо).

Швидкість поширення інформації в on-line мережі значно більша ніж в off-line мережі в силу простоти передачі та мовлення. Окрім цього, варто зазначити такий важливий момент, що виробництво, поширення та доставка до адресата інформаційної продукції (контенту) для поширення в on-line мережі вимагає значно меншої витрати людських та матеріально-технічних ресурсів ніж в on-line мережі, у першу чергу за рахунок швидкості поширення та надзвичайно низьких витрат на мультиплікацію інформаційних матеріалів» [70].

Отже, інформаційні мережі створюють усі можливості для доставки ворожого культурного та/або інформаційного контенту.

В основі будь-якої війни лежить боротьба смислів, що відображаються у способі життя та цінностях протиборчих сторін. У цьому руслі О. Курбан [79] розглядає сучасні інформаційні війни, а саме як «протистояння ідей, образів, ідеологій і міфів».

З урахуванням викладеного, а також з огляду на позицію, висловлену у дисертаційному дослідженні М. Кубявки, можна дійти слушного висновку, що «на сучасному етапі швидко зростає значення непрямих (м'яких) методів впливу на перебіг політичних та економічних процесів в державах. Провідне місце серед, так званих м'яких методів впливу звісно посідають інструменти інформаційного впливу… Подібна тенденція спостерігається в усьому світі, а 95 % всіх підривних зусиль по відношенню до іншої держави займає інформаційна війна» [80].

В. Загурська-Антонюк наголошує, що «одним із механізмів розв'язання питання протидії інформаційним загрозам є обмеження доступу до інформації або її викривлення, спотворення у процесі «інформаційної війни», яка стала «моторошною» реальністю в сучасних геополітичних стосунках Україна – Росія». Але тут же цей автор вказує, що такі обмеження можуть «виявитися неприпустимими у цивілізованих демократичних суспільствах, які прагнуть до демократичних цінностей» [81].

Дослідивши основниі поняття та категорії інформаційної війни, перейдемо до аналізу правових засад протидії її проявів.

Термін «інформаційна війна» з'явилося в офіційних документах України у 2012 році. Згідно з Указом Президента України «Про Стратегічний оборонний бюлетень України» (що на сьогодні втратив чинність) «інформаційна війна – форма протиборства між суб'єктами (державами, блоками, партіями тощо), що передбачає інформаційний вплив на населення з використанням засобів масової інформації, комп'ютерних мереж тощо з метою формування відповідної суспільної думки, підриву морального духу як усього суспільства, так і окремих його інституцій».[82] Сьогодні чинним є Стратегічний оборонний бюлетень України, затверджений Указом Президента України від 17 вересня 2021 року № 473/2021, який на жаль, вже не містить терміну «інформаційна війна», хоча апелює до понять «ведення протиборства в інформаційному просторі та кіберпросторі», «кіберборотьба», «кіберзброя» [83].

М. Сенченко справедливо відзначає, що «Україні для ефективного протистояння інформаційній війні з боку Росії потрібно мати хоча б: 1) ефективну систему ведення інформаційної війни; 2) ефективну правову концепцію інформаційної війни; 3) стратегію ведення інформаційної війни [84]. Лише та держава може розраховувати на лідерство в економічній, військово-політичній чи інших сферах, мати стратегічну й тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби» [85].

Інформаційна безпека України передбачає «головне стратегічне завдання: створити потужний національний інформаційний простір як головний аспект, що засвідчує присутність країни на світовій інформаційній арені. Реалізація такого завдання зумовлює потребу створення системи протидії будь-якій інформаційній загрозі та захисту власних інформаційних ресурсів, середовища та інфраструктурної складової країни. Застосування Росією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену

протиборства. Саме проти України Росія використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України» [86].

Таким чином, оволодіння сучасними методами ефективної інформаційної війни та захисту від інформаційних впливів супротивника стає одним із найважливіших аспектів національної безпеки у цифрову епоху. Рано чи пізно, державам необхідно буде прийняти правові рішення, спрямовані на обмеження поширення контенту ворога з метою забезпечення власної безпеки, з урахуванням конвенційних зобов'язань демократичної держави.

Особливості інформаційної війни в Україні.

Поширення сепаратистських ідей і загострення конфлікту на сході України спричинили надмірна концентрація медіа у власності олігархів: «у 2013 р. приблизно 75 % телевізійного ринку і ТОП-10 телеканалів належали чотирьом медіагрупам, власники яких використовували їх здебільшого не як бізнес-ресурс, а як інструмент політичного та електорального впливу. При цьому (тенденція не подолана й досі) українські мовники масово розміщували російський аудіовізуальний контент, зокрема відверто антиукраїнського змісту. За різними оцінками, у 2013 р. вони витратили на його закупівлю від 65 до 300 млн дол. США» [69]. До того ж російські телеканали транслювалися по кабельним і супутниковим мережах.

Проблемою для інформаційної безпеки України стало також нерівномірне транслювання національного телерадіомовлення на всій території країни в цифровому та аналоговому форматах. Низка прикордонних районів та інших областей масово не отримували український контент, а замість цього легко отримували неофіційні трансляції суміжних держав, включаючи Росію.

Інформаційний аспект гібридної війни став ключовим в агресії Росії проти України. Використовуючи багаторічну підготовку та інформаційно-психологічну обробку, а також книги, телесеріали, фільми, псевдонаукові та

наукові дослідження тощо, активну кампанію в соціальних мережах, Росія змогла дезорганізувати частину населення та зменшити підтримку дій керівництва держави. Крім того, у зоні конфлікту застосовувалися радіоелектронна боротьба, захоплення телекомунікаційних об’єктів та кібератаки проти державних установ та критичних інфраструктурних об'єктів.

З 2014 року проблема недостатньої готовності держави реагувати на нові загрози в інформаційній безпеці стала очевидною. Процес переосмислення цієї ситуації, особливо на рівні нормативно-правових актів, ще не завершився й залишається актуальним і сьогодні.

Ще однією серйозною проблемою стала фізична втрата здатності реалізувати концепцію єдиного інформаційного простору держави. Окупаційний режим на підконтрольних йому територіях налаштував жорсткий контроль над інформаційним простором, а спроби української сторони забезпечити там свою інформаційну присутність не увінчалися успіхом. Росія здійснює «інформаційну окупацію» на тимчасово окупованих територіях України.

Для протидії інформаційній війні, яку провадить Російська Федерація на міжнародній арені, посилюється інструментарій інформаційної роботи з закордонними аудиторіями. Наприклад, у 2015 році було прийнято Закон України «Про іномовлення», і запущено «Мультимедійну платформу іномовлення України» (МПІУ) з каналом іномовлення UA|TV.

Однією з важливих проблем залишається протидія російським фейкам, як важливого інструменту російської інформаційної агресії проти України. Необхідним є чітке визначення аудиторій, на які спрямовані фейки з боку Росії, та створення ефективного контенту для протидії ним.

Сучасна війна - це боротьба за цінності, наративи та громадську думку, де інформація є основною зброєю. Захист інформаційного простору потребує глибокого перегляду ролі медіа у суспільстві. Ця задача може бути вирішена лише шляхом широкої дискусії про соціальну відповідальність журналістів та побудову ефективної системи саморегуляції медіа.

«Дезінформація, пропаганда, фейки, вербальне озброєння та роззброєння, лінгвістична агресія та лінгвістичний збиток, інформаційне гетто, мова ворожнечі тощо - це складники воєнного протистояння» [87].

Воєнна агресія Росії супроводжувалася з початку воєнного конфлікту так званими «непрямими або нелінійними» діями. Воєнна доктрина російської федерації передбачає використання широкого спектра «невійськових» дій для ведення війни. В 2013 році очільник російського Генштабу Валерій Гєрасімов виступив з доповіддю Російській академії військових наук. У виступі були перераховані та роз'яснені стратегії розвитку російської нелінійної військової доктрини, яка була реалізована під час російського вторгнення до України у 2014 році. Після цього почало широко вживатися словосполучення «доктрина Герасімова». За його словами, «невійськові засоби перевищили вплив військової сили для досягнення стратегічних і політичних цілей» [88]. З цього, до речі, випливає те, що, використовуючи дезінформацію як зброю, РФ воює не лише там, де використовується її армія. Певною мірою використання дезінформації — це можливість провадити своєрідну форму війни практично з усім цивілізованим світом.

«Доктрина Гєрасімова» аналізується фахівцями із прив'язкою до китайської доктрини «необмеженої війни». Вона інтегрує використання ЗМІ, дезінформацію, приховані джерела, невдоволення меншин, управління сприйняттям, обман, а також психологічні та кібероперації [89]. З'явилася вона на світ майже через 5 років після «Мюнхенської промови» російського диктатора Володимира Путіна, який фактично кинув виклик світовому порядку, що був встановлений після Холодної війни.

Це стало частиною міксу невійськових дій у рамках війни, таких як: використання історичної пам'яті (в цьому разі - власного трактування історії) і наратив про захист співвітчизників за кордоном; психологічний терор; мережева війна (домінування в інформаційному просторі та протидія ворожим медіа); проактивне нав'язування основних наративів, які домінують в інформаційному та віртуальному просторі; пропагандистські заходи і їх висвітлення як

російською, так і іноземними мовами; протести за кордоном, інспіровані з Росії тощо.

Варто також розуміти, що «доктрина Герасімова» передбачає можливість проведення операцій по всій ворожій території. Отож, коли російські сили вторгнення не змогли пройти всією територією, дезінформаційні кампанії можна проводити, орієнтуючись на тотальне поширення всім ворожим простором. Це значна перевага саме інформаційних інструментів ведення війни перед лінійними військовими силами та засобами.

Це той приклад, який також підкреслює загально соціальний підхід до конфлікту з боку росіян. Вони воюють, намагаючись забезпечити рефлексивний контроль над супротивником, захопити керування його сприйняттям ситуації та навколишнього світу. Головна мета — змусити приймати рішення, вигідні для агресора. Масове поширення дезінформації має забезпечити досягнення мети.

Воно є частиною «механізму рефлексивного контролю», до якого входять такі елементи, як власне «дезінформація, введення в оману, стримування, відволікання уваги, виснаження, розкол, перевантаження (зокрема інформацією), умиротворення, спроби паралізувати, тиснути, здійснювати навіювання, провокувати» [89].

У рамках інформаційної війни використовують перевірені підходи до формування інформаційних повідомлень: однобічність подачі інформації, блокування частини інформації, власне дезінформація, замовчування незручних для РФ тем або подій, заперечення завданої шкоди («ми обстрілюємо військові, а не цивільні об’єкти») тощо. Також використовуються медійники на місцях, які інтегровані в суспільство, ринок медіа, але поширюють російські наративи.

Росія витратила величезні ресурси на поширення дезінформації у світі. Влітку 2020 року з’явився звіт компанії Graphika, який показав масштаб цього процесу. У ньому йдеться про шестирічну кампанію, яка здійснювалася сімома мовами на трьох сотнях платформ. Початок кампанії припав на січень 2014 року, напередодні першого вторгнення РФ до України.

Більшість контенту було присвячено дискредитації України.

Атакувалися й інші держави. «Основні зловмисні наративи, які просувалися, були такими:

1. Україна — це failed state;
2. НАТО і США — агресори;
3. Європа розділена і слабка;
4. Допінгові скандали навколо російських спортсменів — це русофобія;
5. Вибори на Заході несправедливі;
6. Розпалювання ненависті до мусульман;
7. Підживлення теорій змови;
8. Туреччина — агресор;
9. Росія - жертва;
10. Дезінформація про COVID-19 тощо» [90].

В 2018 році з’явилися результати розслідування, яке показало, що половина російськомовних новин на теми НАТО і країн Балтії були створені ботами, а між деякими медіа в цих країнах і Кремлем є прямий зв’язок. У відповідь на загрозу російської дезінформації в Литві створили платформу Demaskuok.It (українською - «розвінчування»). Вона використовує автоматизовану систему для аналізу статей у російських та литовських ЗМІ, відмічаючи їх за допомогою специфічних ключових слів та вказуючи на можливе поширення дезінформації. [91].

Росіяни за роки своєї агресивної пропагандисте для діяльності створили величезну мережу майданчиків для поширення дезінформації в Україні. Це численні інформаційні сайти (так звані «сайти-сміттярки»). За деякими підрахунками таких працює або працювало понад 220. Це російські сайти, російські «жовті» сайти і місцеві сторінки (з українською вебадресою), але вони також розміщують російську пропаганду. Цікаво те, що найбільше цих ресурсів було створено в 2014 році.

У лютому 2022 року російську пропаганду поширювало майже 250 сторінок у соціальній мережі Facebook. На них підписані в сукупності приблизно 15 мільйонів користувачів. Проте тільки деякі з них мають умовно західне коріння.

Наприклад, працюють начебто в США чи Польщі [92]. Це не рахуючи роботу проросійських телеканалів, політичних партій, громадських організацій, філії російської церкви РПЦ (УПЦ МП), мережі блогерів, публічних експертів (політологів, аналітиків тощо).

У січні 2021 року Інститут масової інформації заявив, що «кількість дезінформації в онлайн-медіа зросла майже втричі за два роки» [93]. Це напередодні першого в 2021 році надпотужного сплеску російської навколовоєнної істерії.

Через рік вийшов звіт медіа-дослідницької організації Mythos Labs, який показав черговий стрибок активності російської дезінформаційної мережі. Кількість акаунтів у Twitter, які поширюють наративи проросійської пропаганди, зросла з 58 у листопаді 2021 року до 697 на початку січня 2022 року. Кількість нових облікових записів, які виявляли в ході дослідження, щотижня зростала. Зростання тривало безперервно упродовж грудня 2021 року, в на початку січня 2022 року. Обсяг твітів про Україну за обліковими записами, що поширювали російську пропаганду і дезінформацію, в грудні зріс на 375% порівняно з листопадом і на 3270% порівняно з вереснем 2021-го. Частка англомовних твітів, опублікованих такими акаунтами, зросла до 57% у грудні проти 34% у листопаді 2021-го [94].

2.2. Вплив інформаційної війни на забезпечення інформаційної безпеки та свободи слова під час війни в Україні

В сучасних воєнних реаліях важко та навіть недоречно заперечувати роль інформації як інструменту в інформаційній війні. Сьогодні, коли практично кожен може виступати як джерело інформації та впливати на суспільну думку, розповсюдження деякої інформація може не відповідати потребам, які визначаються національною безпекою.

Право, як інструмент регулювання суспільних відносин, має бути використане для належного вирішення питань, пов'язаних з забезпеченням інформаційної безпеки. Проте введення повної цензури або «законів військового

часу» не є оптимальним виходом. Влада демократичної держави повинна відповідати на вимоги суспільства щодо забезпечення демократичних прав і свобод, навіть у надзвичайних ситуаціях, таких як воєнний стан.

Інформаційна війна викликала потребу глобальної ревізії як інформаційного простору, так й інформаційної політики держави. Причинами цього стало два фактори.

«По-перше – це надзвичайно активне застосування з боку РФ практично усіх методів інформаційної війни: дезінформування, пропаганди, диверсифікації громадської думки, маніпулювання, психологічного та психотропного тиску; поширення чуток.

По-друге, ані органи влади, ані громадянське суспільство виявилися не готовими протистояти гібридному збройному конфлікту в інформаційній сфері» [32].

Правові засади захисту населення від інформаційних загроз були задекларовані в низці нормативних актів, але не виконані належним чином.

«Вразливість вітчизняного інформаційного простору стала очевидною вже у 2014 році з оглядом на відсутність чітко сформованих політико-правових механізмів державного управління інформаційно безпекою України; відсутність програм захисту населення від деструктивних впливів інформаційної війни, масової просвіти населення, включно з дітьми шкільного віку, студентською молоддю, пенсіонерами» [32]. Також виявилась досить слабкою координація дій державних органів влади з громадянським суспільством, експертним середовищем та журналістами.

Сучасні тенденції у сфері інформаційного простору відкрили перед науковцями безліч можливостей для вивчення комунікаційних систем. Міжнародна спільнота, а також кожна країна окремо, стикаються з проблемою тотального інформаційного протистояння. Журналістика фактично стала четвертою владою, а інформація стала найціннішою валютою. Війна тепер ведеться не за території, а за думки населення. Нова ера стрімкого розвитку глобальних технологій і соціальних медіа призвела до виникнення таких

термінів, як «постправда» та «фейк». Завдяки цьому головним у системі глобальної безпеки стало питання, як захистити себе й країну в умовах тотального інформаційного протистояння.

З введенням воєнного стану з 24.02.2022 року згідно Указу Президента України «тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30–34, 38, 39, 41–44, 53 Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану»» [28].

Обмеження інформаційних прав стосується наступних норм Конституції – статті 31 (право на таємницю листування), статті 32 (право на невтручання в особисте життя), статті 34 (право на свободу думки та слова), статті 41 (право на розпорядження результатами своєї інтелектуальної та творчої діяльності).

Це необхідне, по-перше, через неможливість захисту прав громадян України на непідконтрольних територіях та місцях ведення бойових дій. По-друге, такі обмеження є підґрунтям для прийняття нормативно правових актів, направлених на захист інформаційної безпеки держави. Завершення воєнного стану автоматично поверне дію норм вищеназваних норм.

Під час війни перевага інтересів держави означає можливість збереження основоположних прав багатьох людей через забезпечення життєздатності самої держави.

З моменту оголошення воєнного стану, приймаються зміни до нормативно правових актів з врахуванням реалій війни, що стосуються врегулювання деяких аспектів інформаційних правовідносин щодо заборони поширювати певну інформацію, враховуючи її суспільно-небезпечний характер; врегулювання важливих моментів щодо технічного фіксування інформації в умовах воєнного стану; встановлення чи посилення відповідальності за поширення певної

інформації; врегулювання процесуальних дій щодо вилучення інформаційних даних.

Так, Верховна Рада ухвалила законопроєкт про кримінальну відповідальність за незаконну фото- та відеозйомку переміщення ЗСУ та міжнародної військової допомоги під час воєнного стану [95].

22.03.2022 р. набув чинності Закон, яким спрощено проведення слідчих дій та тимчасового доступу до речей і документів, слідчий може здійснити фіксацію комп'ютерних даних на місці обшуку, навіть якщо про це не сказано в дозволі, та яким внесено зміни до Кримінально-процесуального кодексу України [96].

Посилено кримінальну відповідальність за виготовлення та поширення забороненої інформаційної продукції відповідно до Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» [97].

Негативним антидемократичним передвісником погіршення ситуації в сфері забезпечення свободи слова під час війни є запуск Єдиного телемарафону за рішенням Ради Національної безпеки і оборони [98]. Відповідно до цього Рішення декілька каналів без рішення жодного уповноваженого органу або суду було вимкнуто, а телеканал «Інтер» став частиною проєкту «Єдині новини #UAразом», хоча до нього існує багато питань [99-100]. Таке рішення української влади за більше ніж 2 роки його дії багаторазово піддавалося критиці з боку журналістів та громадянського суспільства.

Як показало експертне кількісне опитування журналістів [101] «однією із форм цензури 62 % опитаних медійників вважають єдиний телемарафон, створений на початку повномасштабного вторгнення, протилежної думки дотримувалися 18 %, а ще 20 % журналістів не змогли дати відповіді на це питання. 2/3 також переконані в тому, що єдиний марафон має бути припинений, і всі мовники можуть вести мовлення самостійно, проти виступають 11 %, а 23 % не визначилися зі своєю позицією з цього питання».

Проте більшість опитаних журналістів вважають, що «в Україні навіть в умовах воєнного стану зберігається свобода слова. Вона існує з суттєвими обмеженнями стосовно висвітлення обставин війни, проте зберігається».

Відносно невелика частина респондентів – учасників фокус-груп вважає, що «в Україні нині критична ситуація зі свободою слова». На їхню думку, це пов'язано з роботою єдиного телевізійного марафону в наявному форматі та утисками опозиційних ЗМІ, які не включені до цього марафону, передовсім телеканалів, афілійованих із екс-президентом Петром Порошенком. На місцевому рівні владні еліти, на їхню думку, теж намагаються взяти під контроль незалежні ЗМІ.

Водночас окремі респонденти зазначали, що «і до початку російського повномасштабного вторгнення в Україні не було повноцінної свободи слова».

При цьому значна частина журналістів погоджується з тезою, що «в умовах повномасштабної війни в Україні не може бути такої само свободи слова у її традиційному розумінні, яка була до російського вторгнення. Обмеження висловлювань стосуються практично всієї сфери бойових дій та дотичних до неї аспектів» [101].

Частина журналістів наголошувала на тому, що «медіа під час такої війни і мають працювати по-іншому – насамперед на підтримку бойового духу та віри у перемогу».

Цікавим є питання сприйняття не тільки свободи слова під час війни в Україні, а й ставлення спільноти журналістів до можливої наявності «воєнної цензури». «Воєнну цензуру – обмеження поширення інформації про хід бойових дій, ситуації в армії тощо – більшість респондентів не вважає критичною для свободи слова. Наявна воєнна цензура, хоча й існує – все ж напряму пов'язана з безпекою держави та людей, тому очевидно, що вона існує в країні, яка веде інтенсивні бойові дії» [101].

При цьому учасники фокус-груп все ж убачали проблему у ситуаціях неузгодженості щодо того, що саме можна чи не можна висвітлювати в медіа, а також у спробах окремих чиновників приховати суспільно значущу інформацію,

посилаючись на її значення для обороноздатності країни (що далеко не завжди так) [101].

«Висвітлення проблемних питань у збройних силах чи у веденні бойових дій в умовах війни є вкрай складним. По-перше, значна частина інформації таємна і не може бути розголошеною. По-друге, публічне висвітлення проблемних аспектів (як-от імовірна корупція в армії), може суттєво вплинути на бойовий дух. В таких випадках самоцензура впливає на дії журналістів навіть більше, ніж у цивільних питаннях» [101].

Водночас респондентам не вистачає більш адекватної комунікації з органами військового та цивільного управління. «Різні державні інституції по-різному ставляться до журналістської роботи та часто суперечать одна одній. Стосовно дозволу працювати в певних місцях або висвітлювати ті чи інші аспекти війни представники різних державних органів можуть мати кардинально різні позиції» [101].

Журналісти звернули увагу також на те, що «в Україні відсутні єдині стандарти того, який обсяг інформації подають державні органи. Як приклад, різні військові адміністрації та місцева влада публікують різні обсяги інформації про обстріли, їхні наслідки та географічні прив’язки. Стандартизація подачі цієї інформації спростила б діяльність журналістів та зменшила ризики поширення даних, чутливих для національної безпеки» [101].

Деякі з учасників фокус-групових досліджень вважають, що «обмеження свободи слова, накладені вимогами воєнного часу, будуть достатньо швидко припинені після закінчення війни, зокрема і через тиск країн Заходу». Також є сподівання на те, що «безальтернативність європейської та євроатлантичної інтеграції після війни матиме конкретні вимоги стосовно свободи ЗМІ та реформ у галузі медіа» [101].

Висновки до другого розділу

Російська агресія, особливо її нелінійні аспекти, завжди були спрямовані на розкол українського суспільства, легітимізацію агресії на міжнародному рівні та

зміну реакції цивілізованого світу на експансивну війну, що може мати глобальні наслідки.

Загрози інформаційної безпеки - це сукупність дій або подій, які можуть привести до порушення достовірності, цілісності, конфіденційності інформації, яка зберігається, передається або оброблюється.

Основними загрозами інформаційній безпеці є:

- збільшення кількості глобальних дезінформаційних кампаній та обмежені можливості органів влади реагувати на них;
- інформаційна політика Російської Федерації;
- соціальні мережі як суб'єкти впливу в інформаційному просторі;
- інформаційний вплив Російської Федерації як держави-агресора на населення України, в т.ч. на тимчасово окупованих територіях України;
- несформованість системи стратегічних комунікацій;
- недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;
- недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам.

Перемога України в інформаційній війні, де роль інформації стає вирішальною, особливо у сучасних умовах, є одним із ключових факторів перемоги у війні проти РФ. Це особливо важливо для країни, яка змушена вести асиметричну війну проти держави з переважаючим військовим потенціалом. Від того, як світове суспільство сприймає події в Україні, залежить як рівень політично-соціальної підтримки, так і обсяги фінансової й військової допомоги Україні.

Воєнний стан не став приводом для свавільного владного трактування прав та обов’язків суб’єктів із хаотичним встановленням обмежень і заборон.

РОЗДІЛ 3. ПРОПОЗИЦІЇ ТА РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СВОБОДИ СЛОВА В КОМУНІКАЦІЯХ ПІД ЧАС ВІЙНИ

3.1. Аналіз стейкхолдерів та середовища політики та в сфері забезпечення інформаційної безпеки та свободи слова

Починаючи з 2014 року, з боку Російської Федерації постійно здійснюються інформаційні атаки на медіапростір України та світу. У зв'язку з цим можна виділити наступні симптоми проблемної ситуації, які викликають занепокоєння у суспільстві:

1. Інформаційні атаки та спотворення фактів**,** що включає в себе маніпулювання інформацією для просування певних політичних агенд, зміни у свідомості громадян та створення дезінформації.

2. Пропаганда ворожнечі та сепаратизму, дезинформаційні кампанії, що висвітлюють подій у сприятливому світлі для ворога.

3. Вплив на свідомість громадян та світову спільноту, оскільки інформаційні атаки не обмежуються лише впливом на свідомість громадян нашої країни, а також впливають на світову спільноту та медіапростір загалом, що може призвести до спотворення загального розуміння подій та ситуації.

4. Потреба в стратегічному захисті інформації**.** Умови воєнного стану підкреслюють стратегічне значення інформації як інструменту перемоги. Це підкреслює необхідність ефективного захисту інформаційної безпеки як чинника успішного ведення війни.

Тому проблема забезпечення інформаційної безпеки в комунікаціях є надзвичайно важливою для України під час війни.

До **політико-адміністративні дієвців** (творців політики) відносяться:

Міністерство культури та інформаційної політики України	- здійснює в межах компетенції нормативно-правове регулювання у сфері інформаційної безпеки України; - визначає перспективи та пріоритетні напрями розвитку у сфері інформаційної безпеки України;

	- разом із МЗС України сприяє популяризації та формуванню позитивного іміджу України у світових інформаційних ресурсах та національних інформаційних ресурсах іноземних держав з метою захисту її політичних, економічних та соціально-культурних інтересів, зміцнення національної безпеки і відновлення територіальної цілісності України.
Кабінет міністрів України	- забезпечує формування та реалізацію інформаційної політики держави, забезпечує інформаційний суверенітет, фінансування програм, пов'язаних з інформаційною безпекою, спрямовує і координує роботу міністерств, інших органів виконавчої влади у цій сфері. - Кабінет Міністрів України розробляє та затверджує план стратегічних заходів з щодо забезпечення інформаційної безпеки та виконання Стратегії інформаційної безпеки України.
Міністерство оборони України	- забезпечує моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері; - здійснює підготовку та проведення інформаційних заходів оборони держави, координацію залучення до них суб'єктів забезпечення національної безпеки держави; - забезпечує розвиток та функціонування системи стратегічних комунікацій сил оборони; - забезпечує здійснення правових, організаційних, технічних, інформаційних та інших дій щодо забезпечення власної інформаційної безпеки, у тому числі захисту єдиного інформаційного середовища сил оборони, зокрема в місцях дислокації, розгортання та застосування угруповань, військових частин та підрозділів Збройних

	Сил України, інших військових формувань, утворених відповідно до законів України; - забезпечує зв'язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації у районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях; - здійснює протидію інформаційним операціям та іншим заходам інформаційного впливу, спрямованим проти Збройних Сил України та інших військових формувань, утворених відповідно до законів України; - забезпечує донесення достовірної інформації до військовослужбовців Збройних Сил України, інших складових сил оборони.
Служба безпеки України	- здійснює моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері; - забезпечує протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації.
Рада національної безпеки та оборони	- відповідно до Конституції України та у встановленому законом порядку здійснює координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері, зокрема з використанням спроможностей Центру протидії дезінформації.

Перелік компонент середовища і ключові елементи кожної компоненти.

Компонента середовища	**Елементи компонент середовища**	**Характеристика елемента**
1. Компонента середовища «Соціальна»	1.1. Медіаграмотність та рівень свідомості громадян 1.2. Соціальна стабільність та рівень довіри в суспільстві	1.1. Рівень обізнаності населення з питаннями інформаційної безпеки та його реакція на інформаційні атаки 1.2. Вплив інформаційних конфліктів на стабільність суспільства, рівень довіри між громадянами та державними органами
2. Компонента середовища «Економічна»	2.1. Економічна нестабільність та залежність від зовнішнього фінансування 2.2. Рівень фінансування заходів забезпечення інформаційної безпеки	2.1. Вплив інформаційних атак на зміну сприйняття країни та надання фінансової допомоги 2.2. Відсутність бюджету на заходи забезпечення інформаційної безпеки та побудову системи стратегічних комунікацій
3. Компонента середовища «Політична»	3.1. Воєнний стан 3.2. Стан законодавства та наявність політичної волі	3.1. Недостатня увага до заходів забезпечення інформаційної безпеки порівняно з веденням воєнних дій та забезпеченням національної безпеки країни 3.2. Повільне втілення Стратегії інформаційної безпеки та виконання плану заходів забезпечення інформаційної безпеки

4. Компонента середовища «Фізична»	4.1. Стан інформаційної інфраструктури 4.2. Кіберінфраструктура та протидія кіберзагрозам	4.1. Відсутність єдиного медіапростору та розбудованої системи комунікацій, особливо у прифронтових та ТОТ 4.2. Поточний рівень захищеності від кібератак та виробленість кіберзаходів – у процесі становлення

Результати аналізу впливу компонент і елементів середовища

Компонента	**Елемент**	**Вплив на проблему**
1. Компонента середовища «Соціальна»	1.1. Медіаграмотність та рівень свідомості громадян 1.2. Соціальна стабільність та рівень довіри в суспільстві	1.1. Низький рівень сприяє поглибленню проблеми 1.2. Зріст довіри може сприяти вирішенню проблеми
2. Компонента середовища «Економічна»	2.1. Економічна нестабільність та залежність від зовнішнього фінансування 2.2. Рівень фінансування заходів забезпечення інформаційної безпеки	2.1. Сприяє поглибленню проблеми 2.2. Сприяє поглибленню проблеми
3. Компонента середовища «Політична»	3.1. Воєнний стан 3.2. Стан законодавства та наявність політичної волі	3.1. Сприяє поглибленню проблеми 3.2. Сприяє поглибленню проблеми
4. Компонента середовища «Фізична»	4.1. Стан інформаційної інфраструктури 4.2. Кіберінфраструктура та протидія кіберзагрозам	4.1. Сприяє поглибленню проблеми 4.2. Є сприятливим щодо послаблення проблеми – з урахуванням можливої

Компонента	Елемент	Вплив на проблему
		динаміки цього елемента (змін у часі)

Перелік стейкголдерів – організованих заінтересованих груп (неурядові організації та ін.):

1. Громадянські організації в сфері захисту свободи інформації (Інститут масової інформації, Центр громадянських свобод).

2. Журналістські об’єднання (Національна спілка журналістів України тощо).

3. Цифрові правозахисні організації (Digital Security Lab Ukraine, Центр Стратегічних комунікацій).

4. Медіа-платформи та інтернет-провайдери.

Аналіз впливу та прихильності стейкхолдерів

Стейкголдер	Опис впливу (влади)	Опис прихильності (інтересу)
1. Громадянські організації в сфері захисту свободи інформації (Інститут масової інформації, Центр громадянських свобод)	- мають великий вплив на формування громадської думки та здатні мобілізувати громадянське суспільство для захисту свободи слова та інформаційної безпеки - їхні дії та позиції можуть створювати тиск на урядові органи та вимагати від них прийняття конкретних заходів для покращення ситуації	- прихильні до підтримки свободи слова, прав людини та громадянського суспільства - зацікавлені в запобіганні цензурі та обмеженнях у доступі до інформації

Стейкголдер	Опис впливу (влади)	Опис прихильності (інтересу)
2. Журналістські об’єднання (Національна спілка журналістів України тощо)	- мають значний вплив на формування повістки в медіа та вирішення питань свободи слова - можуть впливати на редакційну політику медіа та створювати обставини для виведення інформаційних тем на перший план	- прихильні до захисту професійних стандартів та свобод в медіа - зацікавлені в уникненні тиску та перешкод у виконанні своїх професійних обов’язків
3. Цифрові правозахисні організації (Digital Security Lab Ukraine, Центр Стратегічних комунікацій)	- спеціалізуються на кібербезпеці та інформаційній безпеці, що дає їм авторитет у питаннях цифрової безпеки та захисту приватності - можуть впливати на формування політики та розробку технічних стандартів у цих областях	- прихильні до захисту приватності, кібербезпеки та інтернет-свободи - зацікавлені в запобіганні кібератакам, цензурі в інтернеті та масовому контролі за інформацією
4. Медіа-платформи та інтернет-провайдери	- мають значний технічний та інформаційний вплив, оскільки вони забезпечують доступ до інформації для мільйонів користувачів - їхні дії щодо фільтрації, блокування або відображення контенту можуть мати	- прихильні до забезпечення доступу до інформації та свободи вираження в інтернеті - зацікавлені в ефективному функціонуванні своїх

Стейкголдер	Опис впливу (влади)	Опис прихильності (інтересу)
	значний вплив на доступність інформації та свободу слова в інтернеті	платформ та мереж для користувачів

Результати аналізу впливу стейкголдерів через очікувану поведінку

Стейкголдер	Очікувана поведінка стейкголдера – щодо існування проблеми та спроб її вирішення
1. Громадянські організації в сфері захисту свободи інформації (Інститут масової інформації, Центр громадянських свобод)	Вимагатимуть від уряду прийняття конкретних заходів для захисту прав на доступ до інформації та свободи вираження у випадку погіршення ситуації щодо забезпечення інформаційної безпеки в комунікаціях
2. Журналістські об’єднання (Національна спілка журналістів України тощо)	Вимагатимуть від уряду створення умов для вільної журналістської діяльності та захисту журналістів від тиску у випадку погіршення ситуації щодо забезпечення інформаційної безпеки в комунікаціях
3. Цифрові правозахисні організації (Digital Security Lab Ukraine, Центр Стратегічних комунікацій)	Активно моніторять інтернет-простір та виявляють випадки порушення інформаційної безпеки Залучатимуть увагу до важливості захисту приватності та кібербезпеки в умовах конфлікту
4. Медіа-платформи та інтернет-провайдери	Забезпечують доступ користувачам до інформації без обмежень та цензури

Стейкголдер	Очікувана поведінка стейкголдера – щодо існування проблеми та спроб її вирішення
	Розроблятимуть та впроваджуватимуть технічні заходи для захисту користувачів від кіберзагроз та інших порушень інформаційної безпеки

Ставлення громадськості

Назва групи громадськості	**Ознаки, за якими індивіди включаються до складу групи, за можливості – оцінка чисельності**	**У чому інтерес до проблеми (до її існування та до можливого вирішення)**
Інтернет-активісти	Це індивіди, які активно ведуть блоги, беруть участь у підписанні петицій та в інших громадських заходах в мережі Чисельність цієї групи може бути значною, оскільки в Інтернеті діє велика кількість активних користувачів, які все більше приймають участь в медіа активностях	Інтерес до проблеми виникає внаслідок обмежень інформаційної свободи та безпеки в Інтернеті, які впливають на їхню можливість вільного вираження думок та обміну ідеями. Вони цікавляться можливими способами забезпечення інформаційної безпеки та свободи інформації
Медіаграмотні громадяни	Це індивіди, які мають високий рівень медіаграмотності та розуміють роль та вплив інформаційної безпеки в суспільстві. Вони критично	Інтерес до проблеми випливає з розуміння важливості правдивої та об’єктивної інформації для функціонування

	ставляться до інформації та здатні аналізувати та оцінювати її достовірність Чисельність цієї групи може бути помірною, оскільки медіаграмотність. Як і критичне мислення не є загальною характеристикою для всіх громадян	демократичного суспільства. Вони цікавляться можливими шляхами підвищення медіаграмотності та захисту від маніпуляцій/дезінформації в інформаційному просторі
Особи без критичного мислення	Це індивіди, які мають обмежений рівень критичного мислення та легко віддаються впливу маніпуляційних технік. Вони можуть вірити фейкам, міфам та стереотипам, не перевіряючи їх достовірність Чисельність цієї групи може бути великою, оскільки деякі індивіди можуть мати обмежений доступ до освіти або інших джерел інформації, що сприяє формуванню необ'єктивних уявлень	Майже не бачать існування проблеми, та не мають інтересу до її вирішення. Інтерес до проблеми може виникати хвилеподібно, після викриття недостовірної чи маніпулятивної інформації, що може спонукати їх до підвищення власної медіаграмотності
Вороги України	Особи, які створюють та поширюють фейки, дезінформацію та пропаганду, мають значний вплив на суспільну думку, формуючи негативний образ України як країни агресора або	Можуть продовжувати активно розповсюджувати дезінформацію та проводити пропагандистські кампанії з метою збільшення негативного ставлення до

	нестабільної держави. Така діяльність може призвести до збільшення внутрішніх конфліктів, підтримки сепаратистських рухів та загрози національній безпеці, зменшення підтримки партнерів. Вони прихільні до поширення фейків та дезінформації, оскільки це допомагає їм досягти своїх політичних та військових цілей. Вони мають інтерес у погіршенні іміджу України та збільшенні дестабілізації суспільства через пропаганду нетерпимості, сепаратизму та ненависті. Чисельність групи оцінити важко, оскільки це можуть бути як громадяни України, так і громадяни Росії або інших недружніх країн.	України та підтримки сепаратистських рухів. Також можливе збільшення активності в інформаційній сфері з метою використання фейків для дискредитації уряду України та владних інституцій. Вони можуть реагувати негативно на будь-які спроби України чи її союзників боротися з дезінформацією та пропагандою, намагаючись активно перешкоджати впровадженню заходів з протидії цим явищам.

3.2. Складові механізму забезпечення інформаційної безпеки та свободи слова під час війни в Україні

На думку А. Нашинець-Наумової «під час війни захист інформаційної безпеки держави є пріоритетним завданням державних органів. Підчас воєнного стану публічно-правовий захист виходить за межі традиційного регулювання і втручається у приватно-правові відносини, в тому числі це стосується права на

свободу слова. Держава повинна бути спроможною не тільки забезпечувати збереження фундаментальних демократичних засад існування суспільства, а й уникати прийняття волюнтаристських рішень» [9].

Механізми забезпечення інформаційної безпеки України можна розділити на два рівні – законодавчий та адміністративний. Виходячи з цього основними задачами для забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни є:

- на законодавчому рівні – створити механізм, що дозволяє узгодити процес розробки законів з реаліями воєнного часу, що допоможуть посилити інформаційну безпеку без необґрунтованого обмеження права на свободу слова;

- на адміністративному рівні – сформувати програму заходів в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи поточний стан справ.

Виходячи з переліку завдань та очікуваних результатів, що вже зафіксовані у Стратегії інформаційної безпеки, можна дійти наступних висновків.

Пріоритетні напрями забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в України:

1. Удосконалення законодавства України у сфері забезпечення інформаційної безпеки з метою побудови стратегічних комунікацій та забезпечення загальної спрямованості діяльності різних суб'єктів реалізації управлінських рішень в межах єдиних завдань (побудова one voice);

2. Законодавче закріплення обмеженого переліку правопорушень в сфері інформаційної безпеки та обмеження свободи слова в комунікаціях, що будуть відповідати принципам законності, співрозмірності та необхідності запровадження таких обмежень, та посилення відповідальності за такі порушення;

3. Вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва у зазначеній сфері.

На думку А. Нашинець-Наумової «запорукою створення надійної системи забезпечення інформаційної безпеки в країні є пошук принципово нових,

нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління загрозами та небезпеками в сфері інформаційної безпеки» [9].

3.3. Рекомендації органам влади

Відповідно до Стратегії [18] «стратегічні комунікації - скоординоване і належне використання комунікативних можливостей держави - публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави».

Також важливо зазначити, що стратегічна ціль 6 згідно цієї Стратегії – «*створення ефективної системи стратегічних комунікацій»*.

Відповідно до Стратегії «основною метою створення та розвитку системи стратегічних комунікацій є гарантування ефективної інформаційної взаємодії та діалогу між органами державної влади, органами місцевого самоврядування та суспільством з питань, що стосуються кризових ситуацій, а також утвердження позитивного іміджу України, інформаційне сприяння просуванню інтересів держави у світі. Ефективна побудова своєї міжнародної інформаційної діяльності дасть змогу Україні здійснювати проактивні інформаційні заходи, інформувати світову спільноту про події в Україні та на її тимчасово окупованих територіях, прогрес у реформах та позитивні внутрішні зміни в державі попри наявну збройну агресію проти України, про ключові рішення органів державної влади щодо стратегічних питань розвитку держави, що сприятиме кращому розумінню міжнародними партнерами внутрішньої і зовнішньої політики держави, забезпечить міжнародну підтримку та покращить імідж України як надійного і передбачуваного партнера».

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань, передбачених Стратегією:

- «визначення системи взаємодії з питань реагування на кризову ситуацію, післякризову комунікацію, запобігання настанню кризи шляхом аналізу передумов кризи та криз, що мали місце в минулому;

- налагодження ефективної взаємодії між органами державної влади вищого рівня, центральними органами виконавчої влади та обласними державними адміністраціями з метою вироблення представниками держави єдиної позиції з питань, що виникають під час кризової ситуації та в післякризовий період;

- налагодження ефективної взаємодії між представниками держави та громадськістю шляхом забезпечення системного діалогу між державними органами та засобами масової інформації, журналістами, представниками нових медіа з питань, що виникають під час кризової ситуації та в післякризовий період;

- забезпечення стабільного функціонування системи іномовлення України шляхом створення та поширення інформаційного продукту каналами супутникового, ефірного наземного аналогового і цифрового мовлення, мовлення в кабельних мережах за межами України, зокрема англійською, російською та іншими мовами;

- створення в системі іномовлення України та забезпечення функціонування служби державного радіомовлення на зарубіжні країни;

- забезпечення присутності програм вітчизняних телекомпаній у багатоканальних мережах інших держав шляхом сприяння створенню загальнонаціональними телеканалами супутникових іноземних версій (з урахуванням мови країни розповсюдження) для поширення програм за межами України;

- забезпечення інформування світової спільноти про події в Україні та донесення офіційної позиції України до представників іноземних держав і засобів масової інформації;

- використання знака (бренду) України "Ukraine Now" з метою популяризації та просування інтересів України у світі;

- розробка та поширення позитивних наративів та інформаційних кампаній за кордоном, які сприятимуть підвищенню рівня впізнаваності та кращому розумінню України серед іноземних аудиторій, а також утвердженню іміджу

України як демократичної європейської держави, яка рухається до повноправного членства в ЄС та НАТО, є невід'ємною частиною європейського політичного, економічного, культурного, освітнього та інформаційного простору, бере участь у розв'язанні глобальних проблем і ділиться досвідом у сферах, що є актуальними для міжнародної спільноти».

«Стратегічна комунікація є інструментом, який комплексно використовує образи, слова та дії для впливу на сприйняття цільової аудиторії, зміни її поведінки та досягнення національних стратегічних інтересів. Стратегічна комунікація наголошує на координації між органами державної влади, а також на узгодженості між питаннями інформації та практичними діями, що може допомогти державі у вирішенні поточних і майбутніх викликів безпеці та реагуванні на них, та використовувати для національного розвитку та реалізації визначених стратегій. Ефективна стратегічна комунікація також може допомогти мінімізувати загрози національній безпеці та допомогти у плануванні та впровадженні політики держави» [102].

«На разі центральна (чи, швидше, – першочергова) проблема державного страткому – навіть не вироблення того самого наративу (гранд – чи малого), а проблема ефективної координації суб’єктів страткому у різнорівневих системах із власною ієрархією, системою прийняття рішень, традиціями та навіть цілями. І основне завдання держави (принаймні – на нинішньому етапі) – забезпечити єдність дій цих структур у межах єдиного вектора діяльності. Ця координація має включати як загальну практичну координацію дій, так і створення тієї самої системи єдиних меседжів, що не суперечать один одному» [103].

Таким чином для забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в Україні є побудова системи стратегічних комунікацій та створення one voice.

«One voice – технологія донесення головних повідомлень для досягнення конкретних цілей. У політиці – як у найвищих державних органах, так і в органах місцевого самоврядування, технологію one voice застосовують для успішної розбудови проєктів та досягнення завдань. Діяльність лідера – це ідеї й майбутнє,

за яке відповідальний керманич має боротися. Поки він не пояснить людям свої ідеї, нічого не буде» [104].

В умовах війни стратегічні комунікації повинні займати перше місце в побудові комунікаційної стратегії «держава – суспільство».

Найголовніше в комунікаціях під час війни це швидкість та доступність інформації. Держава має мобілізувати всі свої зусилля та спрямувати їх на створення системи оперативного інформування громадян - створити джерело верифікованого органами державної влади контенту, який буде зрозумілий кожному громадянину та не буде спотворений каналами комунікації. Таке джерело повинно транслювати всю необхідну інформацію, починаючи від оперативної інформації та подачі новин і закінчуючи практичними порадами та оповіщеннями про загрозу ракетного удару.

Наразі важливими джерелами офіційної інформації є щоденні звернення Президента Володимира Зеленського, брифінги членів команди Офісу Президента, звернення голів обласних військових адміністрацій, інформація про гуманітарні коридори, про військову економіку, телеграм канали підрозділів Збройних сил України. Вони позбавляють страху залишитися поза інформаційним полем і страху невідомості, інформують про реальну ситуацію, розвінчують російські фейки та підкріплюють віру в перемогу України.

«Українські стратегічні комунікації посилили позитивні наративи українців про ефективне використання допомоги Заходу проти росії. Військові лідери мають професійно передавати наративи своїм збройним силам, громадянському суспільству та політичним лідерам усередині країни та в усьому світі. Стратегічні комунікації, якщо їх правильно використовувати в новому бойовому просторі, забезпечує ефективну передачу повідомлень аудиторії. Крім того, стратегічні комунікації вимагають планування на стратегічному, оперативному та тактичному рівнях для досягнення бажаних результатів впливу» [105].

«Стратегічні комунікації стали ефективною небойовою зброєю проти ворога та його прихильників, водночас роблячи ініціативи противника менш ефективними. Інтернет і масові комунікації поступилися місцем когнітивній

війні, яка є цифровою та віртуальною діяльністю, що здійснюється для маніпулювання подразниками навколишнього середовища з метою контролю психічних станів і поведінки ворогів, а також послідовників у війні» [106].

«Такі дії стратегічних комунікацій можуть бути синергетичними, впливаючи на свідомість прихильників за допомогою спеціального повідомлення, яке формує інформаційне середовище. Військовий конфлікт в Україні продемонстрував, наскільки потужними є кампанії впливу, наскільки важливою є готовність протистояти їм і наскільки інструментальними можуть бути соціальні медіа для досягнення стратегічних цілей. Завдяки ефективній стратегічній комунікації українці захопили цифровий простір за допомогою виважених наративів. Це сприяло ізоляції росії, водночас посилюючи західну допомогу в Україну» [107].

Стратегічні комунікації представляють собою важливий інструмент для збільшення довіри та залучення громадської підтримки, сприяючи урядовим структурам у веденні ефективного та прозорого спілкування. Ці комунікаційні стратегії можуть бути потужним засобом у протидії дезінформації та втручанню окремих держав, які намагаються підривати національну безпеку України. Шляхом впровадження ефективних комунікаційних стратегій, урядові органи можуть активно поширювати правдиву інформацію, викривати маніпуляції та переконувати громадськість у своїх намірах та діях. Впровадження стратегічних комунікацій надасть змогу зменшити негативний вплив безпекових чинників на інформаційні права громадян під час війни, шляхом формування верифікованого органами державної влади джерела контенту та застосування технології one voice.

Проте існують певні виклики, які потрібно враховувати при впровадженні стратегічних комунікацій, такі як швидкість та обсяг інформації, яку необхідно опрацювати. Це вимагає застосування нових підходів у використанні технологічних засобів, удосконалення нормативно-правової бази, моніторингу та оцінювання ефективності стратегічних комунікацій, а також посилення співпраці з міжнародними партнерами у сфері національної безпеки.

Висновки до третього розділу

Проблеми, пов'язані з інформаційною безпекою, варто включити до порядку денного таких органів влади, як:

- Міністерство культури та інформаційної політики;
- Національна рада з питань телебачення та радіомовлення;
- Комітет з питань свободи слова та інформаційної політики;

Органом влади, що забезпечує інформаційну безпеку, є МКІП, оскільки воно має найбільші повноваження у цій сфері.

Елементи середовища:

1. Сприятливими компонентами середовища є наявність великої кількості медіа, активна громадська підтримка та увага громадськості та фахового середовища до інформаційної свободи.

2. Негативною перешкодою може бути відсутність ефективного законодавства щодо захисту інформаційної безпеки, інформаційних прав громадян та відсутність політичної волі до втілення плану заходів щодо забезпечення інформаційної безпеки, вплив політичного тиску на медіа, економічно залежні медіа.

Стейкхолдери:

1. Зацікавлені у вирішенні проблеми: громадські організації, журналісти, цифрові правозахисні організації та медіа-платформи.

2. Можуть перешкоджати: урядові структури, які можуть бути зацікавлені у контролі над інформаційним простором під час війни.

Також необхідно врахувати ставлення громадськості та діяльність так званих «ворогів України», та необхідність впровадження заходів протидії фейкам, пропаганді та дезінформації.

Запорукою створення надійної системи забезпечення інформаційної безпеки в країні є пошук принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління загрозами та небезпеками в сфері інформаційної безпеки.

Основним завданням для органів влади є побудова системи стратегічних комунікацій для своєчасного виявлення й ліквідації загроз і ризиків негативного впливу «інформаційної зброї», реалізації державної політики протидії «інформаційній війні», та здійснення на всіх рівнях ефективного захисту інформаційного суверенітету держави.

Стратегічні комунікації представляють собою важливий інструмент для збільшення довіри та залучення громадської підтримки, сприяючи урядовим структурам у веденні ефективного та прозорого спілкування. Шляхом впровадження ефективних комунікаційних стратегій, урядові органи можуть активно поширювати правдиву інформацію, викривати маніпуляції та переконувати громадськість у своїх намірах та діях. Впровадження стратегічних комунікацій надасть змогу зменшити негативний вплив безпекових чинників на інформаційні права громадян під час війни, шляхом формування верифікованого органами державної влади джерела контенту та застосування технології one voice.

ВИСНОВКИ

В ході магістерського дослідження (розділ 1) було проведено теоретико-понятійний аналіз явища інформаційна безпека та досліджено різні підходи та аспекти явища інформаційної безпеки. Було встановлено, що поняття «інформаційна безпека» є складною конструкцією, що зумовлюється комплексною соціально-правовою природою, завдяки різноманіттю інформаційних відносин в суспільстві, відмінністю суб'єктів інформаційних відносин з власними інтересами, правами та обов'язками залежно від галузі використання. Для побудови ефективної системи інформаційної безпеки під час війни важливо запровадити таку державну політику, яка буде ґрунтуватися на відповідних нормативно-правових актах та одночасно буде містити технічно спроможну систему для підтримання інформаційної безпеки у кризовий час.

Також було вивчено ролі інформації та свободи слова під час війни та встановлено, що на сьогодні роль інформації – критична як ніколи, та закони воєнного часу не повинні встановлювати необґрунтованих обмежень свободи слова.

Наступним було досліджено державну політику щодо забезпечення інформаційної безпеки та свободи слова під час війни, встановлено законодавчі та інституційні засади її функціонування. Виявлено, що наразі сформована потужна правова база у сфері інформаційної безпеки. Однак, незважаючи на це, практична реалізація правових норм в період воєнного стану знаходиться на досить низькому рівні. Встановлено, що завданням для української влади повинен стати розвиток ефективного діалогу з ЄС у питаннях забезпечення інформаційної безпеки з врахуванням гармонізації законодавства України з європейським та запозиченням кращих практик правозастосування в цій сфері.

Зарубіжний досвід забезпечення інформаційної безпеки був досліджений задля запозичення найкращих практик Європейського союзу та США в контексті перспективи набуття Україною членства в НАТО та Європейському Союзі.

Встановлено, що основою забезпечення інформаційної безпеки є впровадження системи стратегічних комунікацій.

В розділі 2 магістерської роботи було досліджено поняття «інформаційна війна» та окреслено вплив інформаційної війни на забезпечення інформаційної безпеки та свободи слова під час війни в Україні. Встановлено, що перемога України в інформаційній війні, де роль інформації стає вирішальною, є одним із ключових факторів перемоги у війні проти РФ.

Проаналізовані основні загрози інформаційного середовища:

- збільшення кількості глобальних дезінформаційних кампаній та обмежені можливості органів влади реагувати на них;
- інформаційна політика Російської Федерації;
- соціальні мережі як суб'єкти впливу в інформаційному просторі;
- інформаційний вплив Російської Федерації як держави-агресора на населення України, в т.ч. на тимчасово окупованих територіях України;
- несформованість системи стратегічних комунікацій;
- недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;
- недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам.

. Досліджено особливості інформаційної війни в Україні – відсутність єдиного національного медіапростору та інфраструктури для його забезпечення, олігархізація медіа, відсутність національної ідеї та метанаративу в Україні, ріст фінансування дезинформаційних кампаній Російської Федерації, обмеження інформаційних прав через введення воєнного стану в Україні.

Завдяки проведеному аналізу загроз та особливостей виявлено основні напрямки розвитку політики в сфері забезпечення інформаційної безпеки, як способу нейтралізації цих загроз.

В розділі 3 магістерського дослідження здійснено аналіз стейкхолдерів та середовища політики забезпечення інформаційної безпеки. Встановлено, що органом влади, що відповідає за забезпечення інформаційної безпеки та свободи

слова в комунікаціях під час війні в Україні є МКІП, оскільки воно має найбільші повноваження у цій сфері. Негативною перешкодою для впровадження політики може бути відсутність ефективного законодавства щодо захисту інформаційної безпеки, інформаційних прав громадян та відсутність політичної волі до втілення плану заходів щодо забезпечення інформаційної безпеки, вплив політичного тиску на медіа, економічно залежні медіа. Також при впровадженні політики необхідно врахувати ставлення громадськості та діяльність так званих «ворогів України», та необхідність впровадження заходів протидії фейкам, пропаганді та дезінформації.

Досліджено механізм забезпечення інформаційної безпеки та його рівні. Встановлено, що основними завданнями в цій сфері є побудова системи стратегічних комунікацій для своєчасного виявлення й ліквідації загроз і ризиків негативного впливу «інформаційної зброї», реалізація державної політики протидії «інформаційній війні», та здійснення на всіх рівнях ефективного захисту інформаційного суверенітету держави.

Надані обґрунтовані рекомендації щодо політики забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в Україні. Визначено, що впровадження системи стратегічних комунікацій (one voice) є найкращою альтернативою для своєчасного виявлення й ліквідації загроз і ризиків негативного впливу «інформаційної зброї», реалізації державної політики протидії «інформаційній війні», та здійснення на всіх рівнях ефективного захисту інформаційного суверенітету держави. Впровадження стратегічних комунікацій надасть змогу зменшити негативний вплив безпекових чинників на інформаційні права громадян під час війни, шляхом формування верифікованого органами державної влади джерела контенту та застосування технології one voice.

Підсумовуючи магістерську роботу можна зробити висновок, що незважаючи на складність та багатоаспектність теми, усі поставлені завдання бути реалізовані та всі питання - досліджені.

Забезпечення інформаційної безпеки та свободи слова в комунікаціях під час війни в Україні є складним, проте дуже важливим для дослідження питанням, яке не втратить свою актуальність як під час війни, так і під час повоєнної відбудови.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Олійник О.В. Адміністративно-правові засади інформаційної безпеки. Європейські перспективи. 2012. № 4 (1). С. 65–68.

2. Ліпкан В.А. Національна безпека України: навч. посіб. Київ: КНТ, 2009. 576с.

3. Цимбалюк В. С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. Адміністративне право і процес. 2014. № 2 (8). С. 22-30.

4. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17-23.

5. Кісілевич-Чорнойван О. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. Юриспруденція: теорія і практика. 2009. № 8. С. 11–18.

6. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса. 2015. № 3. С. 220-237.

7. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Київ: КНТ, 2006. 140 с.

8. Гурковський В.Т. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дис…канд. юр. наук, спец.: 25.00.02 – механізми державного управління. Київ. 2004. 225 с.

9. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання. Київ: Видавничий дім «Гельветика», 2017. 168 с.

10. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис…канд. юр. наук, спец.: 12.00.07 -

адміністративне право і процес; фінансове право; інформаційне право. Лівів, 2019. 268 с.

11. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: дис…канд. з держ. управління, спец.: 25.00.02 - механізми державного управління. Київ, 2017. 218с.

12. Правові засади інформаційної безпеки України: монографія. П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука. Харків: 2018. – 289 с.

13. Вайцеховська О.Р. Міжнародний фінансовий правопорядок: теоретичні засади та проблеми в умовах глобалізації: дис…канд. юр. наук. Харків, 2020. 472 с.

14. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник. Н. Нижник, Г. Ситник, В. Білоус. Ірпінь : Акад. ДПС України, 2000. 304 с.

15. Виговська О.С. Теоретико-методологічні підходи до проблеми державного регулювання політики інформаційної безпеки. Актуальні проблеми міжнародних відносин. Випуск 108 (Частина І), 2012. С. 96-101.

16. Інформаційна безпека України: Глосарій. Л.С. Харченко, В.А. Ліпкан, О.В. Логінов. – Київ: Текст, 2004. 136 с.

17. Конституція України: Закон України від 08.06.1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

18. Стратегія інформаційної безпеки: Рішення Ради національної безпеки і оборони України від 15.10.2021, затверджено Указом Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

19. Ліпкан В.А. Теоретико-методологічні засади управління у сфері національної безпеки України: монографія. Національна академія внутрішніх справ України. Київ: [б.в.], 2005. 350 с.

20. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017, 168 с.

21. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. 2004. Вип. 8. С. 32.

22. Бодрук О.С. Воєнно-політичні аспекти забезпечення безпеки. Стратегічна панорама. 2002. №2. С. 65-66.

23. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. Актуальні проблеми вітчизняної юриспруденції № 1. 2022. С. 150-155.

24. «Перша світова медійна війна». З якою назвою напад Росії на Україну увійде в історію і що робити з 9 травня – інтерв'ю з Антоном Дробовичем. URL: https://nv.ua/ukr/world/geopolitics/viyna-v-ukrajini-persha-svitova-mediyna-viyna-drobovich-novini-ukrajini-50235840.html.

25. Toffler A. War and Anti-War. N.Y. : Little, Brown and Company, 1993. 302p.

26. Загальна декларація прав людини: прийнята і проголош. Резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 р. База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/995_015.

27. Міжнародний пакт про громадянські і політичні права: Міжнародний документ. Організація Об'єднаних Націй від 16.12.1966 р. URL: https://zakon.rada.gov.ua/laws/show/995_043.

28. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 № 64/2022. URL: https://www.president.gov.ua/documents/642022-41397.

29. Salome Samadashvili. Strategic Defence for Russia's Undeclared Information War on Europe. Wilfried Martens Centre for European Studies. Rue du Commerce 20. Brussels. 2015. 64 p. URL : https://martenscentre.eu/sites/default/files/publication-files/information-warfare-europe-defence-russia_0.pdf.

30. Thomas T.Emerson, The System of Freedom of Expression. Random House, 1970; Original from, the University of Michigan; Digitized, Oct 24, 2008; 754 pages.

31. Рекомендації Комітету міністрів Ради Європи «Про захист свободи вираження поглядів та інформації в кризові часи». Ухвалено Комітетом міністрів 26 вересня 2007 року на 1005 засіданні постійних представників міністрів. П. 17, 19.

32. Свобода слова в умовах інформаційної війни та збройного конфлікту. А.Б. Блага, О.А. Мартиненко, Б.С. Мойса, Р.В. Шутов; за заг. ред. О.А. Мартиненка. Українська Гельсінська спілка з прав людини. К., 2017. 85 с. з іл.

33. Рабатський план дій із заборони пропаганди національної, расової або релігійної ненависті, що є підбурюванням до дискримінації, ворожнечі або насильства (2014). Висновки і рекомендації чотирьох регіональних експертних нарад, організованих УВКПЛ в 2011 році, прийняті експертами в м. Рабат (Марокко) 5 жовтня 2012 року. URL: http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf.

34. Сулейманова Ш.С., Назарова Е.А. Информационные войны: история и современность: Учебное пособие. М. Международный издательский центр «Этносоциум». 2017. 90 с.

35. Борщов Н.А. Социально-философские проблемы информационного насилия : автореф. дис… канд. философских наук. Саратов, 2004. 20 с.

36. Юринець Ю.Л. Дослідження проблем інформаційної безпеки України на засадах міждисциплінарного підходу: соціологія, психологія, право. Юридичний науковий електронний журнал. №7/2020. С 300-307.

37. Про національну безпеку України: Закон України від 21.06.2018 року № 2469-VIII. Відомості Верховної Ради, 2018, № 31, ст.241.

38. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України, 1992, № 48, ст.650.

39. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України, 1994, № 31, ст.286.

40. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. Відомості Верховної Ради України, 1994, № 16, ст.93.

41. Про медіа: Закон України від 13.12.2022 № 2849-IX. Відомості Верховної Ради України, 2023, №№ 47-50, ст.120.

42. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України, 2010, № 34, ст. 481.

43. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. Відомості Верховної Ради України, 2011, № 32, ст. 314.

44. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-IV. Відомості Верховної Ради України, 2003, № 25, ст.180.

45. Про Стратегію національної безпеки України: Рішення Ради національної безпеки і оборони України від 14.09.2020, затверджено Указом Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

46. Про Стратегію кібербезпеки України: Рішення Ради національної безпеки і оборони України від 14.05.2021, затверджено Указом Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

47. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Рішення Ради національної безпеки і оборони України від 28.04.2014, введено в дію Указом в.о. Президента України від 01.05.2014 №449/2014. URL: https://zakon.rada.gov.ua/laws/show/n0004525-14#Text.

48. Про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 № 994-575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

49. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від

30.03.2023 № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text.

50. Стоєцький О. Суб'єкти забезпечення інформаційної безпеки України: адміністративно-правові засади. Інформаційне право. 2009. № 11. С. 161–164.

51. Положення про Міністерство культури та інформаційної політики, затверджено постановою Кабінету Міністрів України від 16 жовтня 2019 р. № 885. URL: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text.

52. Про Раду національної безпеки і оборони: Закон України від 05.03.1998 № 183/98-ВР. Відомості Верховної Ради України, 1998, № 35, ст.237.

53. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: моногр. Київ: НІСД, 2014. 328 с.

54. Забара І.М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. Теорія і практика правознавства. 2013. Вип. 2. URL: http://nbuv.gov.ua/UJRN/tipp_2013_2_77.

55. Міжнародна інформаційна безпека: Сучасні виклики та загрози. Макаренко Є.А., Рижиков М.М. та ін. Київ: Центр вільної преси, 2006. 916 с.

56. SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO): DOCUMENT C-M(2002)49-REV1. Note by the Secretary General on 20 november 2020. URL: https://www.nbf.hu/docs/C-M(2002)49-REV1.pdf.

57. Резолюция A/RES/53/70 ГА ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». – URL : https://undocs.org/ru/A/RES/53/70.

58. Резолюция A/RES/54/49 ГА ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». – URL: https://undocs.org/ru/A/RES/54/49.

59. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. Інтернет-сайт Центру досліджень соціальних комунікацій НБУВ URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:infor

matsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350.

60. The Administration‘s Priorities on Cybersecurity. White House. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critical-infrastructure.

61. Мануйло А. В. Государственная ифнормационная политика в особенных условиях : монография. Москва: ФИФИ, 2003. С. 293

62. Малик Я., Береза О. Забезпечення інформаційної безпеки України у контексті світового досвіду. Ефективність державного управління. 2012. № 32. С. 20 – 27.

63. International Strategy for Cyberspace. White House. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

64. Щепанківський В. Г. Інформаційна безпека як складова образу країни. Актуальні проблеми міжнародних відносин. 2011. Вип. 102. Ч. 1. С. 219 – 228.

65. Почепцов Г. Г. Смислові та інформаційні війни. Інформаційне суспільство. 2013. Вип. 18. С. 21–27. URL: http://nbuv.gov.ua/UJRN/is_2013_18_6.

66. Почепцов Г.Г. Информационные войны. Київ: Ваклер, 2000. 576 с.

67. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник. За заг. ред. В.О. Жадька; ред.-упор. О.І. Харитоненко, Ю.С. Полтавець. Київ: Вид-во НПУ імені М.П. Драгоманова, 2018. 356 с.

68. Малик Я.Й. Інформаційна війна і Україна. Демократичне врядування. 2015. Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3.

69. Почепцов Г.Г., Чукут С.А. Інформаційна політика : навч. посіб. 2-ге вид. Київ : Знання, 2008. 559 с.

70. Верголяс О.О. Спеціальні інформаційні операції в системі засобів протидії загрозам національній безпеці України. Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2019. № 4. С.7-16.

71. Марунченко О.П. Інформаційна війна в сучасному політичному просторі : дис. … канд. політ. наук, спец : 23.00.02. Одеса, 2012, 208 с.

72. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. Вісник НАДУ. 2015. № 1. С. 136–141.

73. Турченко Ю.В. Засоби масової комунікації як суб'єкт реалізації державної інформаційної політики України в сфері оборони: політико-правове регулювання. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2013. Вип. 43. С. 113–119.

74. Магда Є.В. Виклики гібридної війни: інформаційний вибір. Наукові записки Інституту законодавства Верховної Ради України. 2014. № 5. С. 138-142.

75. «Неонацисти, антиросія, каратели»: путін близько півгодини свого виступу в парламенті присвятив Україні та Заходу. URL: https://www.slovoidilo.ua/2023/02/21/novyna/polityka/neonacysty-antyrosiya-karateli-putin-pivhodyny-svoho-vystupu-parlamenti-prysvyatyv-ukrayini-ta-zaxodu.

76. Новородовський В. Інформаційна безпека України в умовах Російської агресії. Соціум. Документ. Комунікація. Сер. Іст. науки. 2020. Вип. 9. С. 150-179.

77. Хорошко В., Хохлачова Ю., Пірцхалава Т., Іванченко І. Інформаційна зброя як інструмент інформаційної війни. Захист інформації. Том 24, № 2, квітень-червень 2022. С. 50–58.

78. Саган О.В. Протидія медіа-інформаційному тероризму як питання національної безпеки України : автореф. дис. … канд. політ. наук, спец: 21.01.01. Київ, 2021. 22 с.

79. Курбан О. Бойові наративи в системі сучасних геополітичних інформаційних війн (досвід російсько-української гібридної інформаційної війни 2014–2021 рр.). Синопсис: текст, контекст, медіа. 2021. № 27(3). С. 149–158.

80. Кубявка М.Б. Моделі та методи управління інформаційним супроводженням в умовах гібридної війни : дис… канд. техн. наук. Спец. 05.13.06 «Інформаційні технології». Київ, 2017. 199 с.

81. Загурська-Антонюк В.Ф. Політично-інформаційні безпекові механізми в українській державній системі у контексті геополітичних змін. Державне

управління: удосконалення та розвиток. 2020. № 2. URL: http://nbuv.gov.ua/UJRN/Duur_2020_2_10.

82. Стратегічний оборонний бюлетень України: схвалено Указом Президента України від 29 грудня 2012 року № 771/2012. URL: https://zakon.rada.gov.ua/aws/show/771/2012#n16.

83. Стратегічний оборонний бюлетень України: затверджений Указом Президента України від 17 вересня 2021 року № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121.

84. Сенченко М.О. Запорука національної безпеки в умовах інформаційної війни. Вісник книжкової палати. 2014. № 6. С. 3-9.

85. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах. Вісник національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С. 32-46.

86. Доктрина інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.

87. Солонько О. Інфодемія. Київ: Видавництво Марка Мельника, 2023. 392с.

88. Grading Gerasimov: Evaluating Russian Nonlinear War Through Modern Chinese Doctrine. URL: https://smallwarsjournal.com/jrl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine.

89. Quotable: Tony Selhorst on the role of information in the Gerasimov doctrine. URL: https://web.archive.org/web/20161021064317/http://www.publicdiplomacycouncil.org/commentaries/06-25-16/quotable-tony-selhorst-role-information-gerasimov-doctrine.

90. Exposing Secondary Infektion. URL: https://secondaryinfektion.org/report/secondary-infektion-at-a-glance/.

91. Як Литва бореться з російською дезінформацією. URL: http://surl.li/sooxn.

92. Дамоклів меч російської пропаганди, або Як виграти інформаційну війну. URL: https://www.pravda.com.ua/columns/2022/04/18/7340426/

93. Кількість дезінформації в онлайн-медіа зросла майже втричі. IMI. URL: https://www.ukrinform.ua/rubric-society/3174850-kilkist-dezinformacii-v-onlainmedia-zrosla-majze-vtrici-imi.html

94. Russian troll farm activity up by 3,000% since late 2021, research finds. URL: https://english.nv.ua/nation/russian-troll-farm-activity-up-by-3-000-since-late-2021-research-finds-50212317.html

95. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24 березня 2022 року № 2160-IX. URL: https://zakon.rada.gov.ua/laws/show/2160-20#n10.

96. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам: Закон України від 15 березня 2022 року № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

97. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції. Закон України від 3 березня 2022 року № 2110-IX. URL: https://zakon.rada.gov.ua/laws/show/2110-20#Text.

98. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану. Рішення РНБО. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text.

99. Концерн РРТ вимкнув мовлення «Еспресо» в цифровій мережі Т2: відкритий лист телеканалу до Президента, РНБО, СБУ, Міноборони, Нацради.

Еспресо. URL: https://espreso.tv/kontsern-rrt-vimknuv-movlennya-espreso-v-tsifroviy-merezhi-t2-vidkritiy-list-telekanalu-do-prezidenta-rnbo-sbu-minoboroni-natsradi.

100. Детектор медіа. URL: https://detector.media/infospace/article/198490/2022-04-18-opzzh-ne-pratsyuie-shcho-bude-z-interom.

101. Виклики для свободи слова та журналістів в умовах війни: соціологічне дослідження. П. Бондаренко, Т. Печончик, А. Сухарина, В. Яворський; Центр прав людини ZMINA. Київ, 2023.

102. Jing L. Jing N. Research on the Construction of China's Strategic Communication System in Global Security Governance. Open Journal of Political Science. 2023. № 13. P. 271–281.

103. Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця : монографія. Київ : НА СБ України, 2018. 517 с.

104. Мудрак Л. Комунікація і криза. Як громадам протистояти викликам і успішно діяти в періоди кризи: Посібник. Київ, 2020. 112 с.

105. Chiriac O., Matisek J. Strategic Communication And Security Force Assistance: Critical Components For Ukrainian Success? The Defence Horizon Journal, 2022. URL: https://www.thedefencehorizon.org/post/strategic-communication-security-force-assistance-ukraine-sfa-stratcom.

106. Hung T. C., Hung T. W. How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. Journal of Global Security Studies. 2022. №. 4(7). DOI: https://doi.org/10.1093/jogss/ogac016.

107. Keenan L. How Ukraine Seized the Initiative on the Digital Front of the War with Russia. Modern War Institute, 2022. URL: https://mwi.usma.edu/how-ukraine-seized-the-initiative-on-the-digital-front-ofthe-war-with-russia/.

108. Грицай Р.О. ІНФОРМАЦІЙНІ ВІЙНИ: ПОШУК СТРАТЕГІЙ ПРОТИДІЇ. Публічне управління та адміністрування в Україні. Випуск 33, 2023. URL: https://pag-journal.iei.od.ua/archives/2023/33-2023/3.pdf.

109. Яковлєв П.О. ДОСВІД ДЕРЖАВНОГО РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАРУБІЖНИХ ДЕРЖАВ (НА ПРИКЛАДІ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ, КАНАДИ, НІМЕЧЧИНИ, ФРАНЦІЇ). Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО». Випуск 30, 2020. URL: https://periodicals.karazin.ua/law/article/view/16548/15426.

110. Залєвська І.І, Удренас Г.І. Інформаційна безпека України в умовах російської військової агресії. Південноукраїнський правничий правопис. Випуск 1-2, 2022. URL: http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf.