МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ІВАНОВА ЄЛИЗАВЕТА ІГОРІВНА

Допускається до захисту:
В.о. завідувача кафедри
міжнародних відносин і зовнішньої політики,
доктор економічних наук,
доц. В.В. Лимар
«_____» _____ 20__ р.

ВОЄННО-ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ ЗА УМОВ ЕСКАЛАЦІЇ КОНФЛІКТУ НА СХОДІ УКРАЇНИ

Спеціальність 291

«Міжнародні відносини, суспільні комунікації та регіональні студії»

Магістерська робота

Керівник:
Фротвейт М.М., доктор політичних наук, професор

Оцінка: __/ __/___
(бали за шкалою ЄТКС/ за національною шкалою)

Голова ЄК д.п.н., професор Федуняк С.Г
(підпис)

Вінниця 2022

Іванова Є. І. Воєнно-інформаційна безпека України за умов ескалації конфлікту на сході України. Спеціальність 291 ««Міжнародні відносини, суспільні комунікації та регіональні студії»». ДонНУ імені Василя Стуса, Вінниця, 2022.

У роботі проаналізовано сучасний стан і загрози інформаційній безпеці в контексті збройних конфліктів, зокрема ескалації війни на Сході України. Висвітлені методологічні аспекти вивчення безпеки інформації, концептуальні підходи вивчення воєнно-інформаційної безпеки під час загострення та прямого ведення війни Росії проти України. Дослідження базується на принципах системності, наукової об'єктивності. Застосовані системні методи. Особлива увага сконцентрована на визначенні механізмів та стратегій забезпечення інформаційної безпеки в Україні на основі вже розроблених прикладів.

Ключові слова: інформація, інформаційна безпека, збройний конфлікт, інформаційне суспільство.

67 с., Бібліографія: 76 найм.

Ivanova Y. I. Ukraine's Defence Information Security in the context of escalation over the conflict in the East of Ukraine. Specialty 291 "International Relations, Public Communications and Regional Studios". Vasil Stus Donetsk National University, Vinnytsia, 2022.

The work provides an analysis of the current state and threats to information security in the context of armed conflicts, in particular the escalation of the war in the East of Ukraine. The methodological aspects of the study of information security, conceptual approaches to the study of military information security during the aggravation and direct conduct of Russia's war against Ukraine are highlighted. The research is based on the principles of consistency, scientific objectivity. Systematic methods are applied. Particular attention is focused on identifying mechanisms and strategies for ensuring information security in Ukraine on the basis of already developed examples.

Keywords: information, information security, armed conflict, information society.

67 p., Bibliography: 76 references.

ЗМІСТ

ВСТУП……..5

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА УМОВ ЗБРОЙНОГО КОНФЛІКТУ ТА КРИТИЧНІСТЬ РОЛІ ІНФОРМАЦІЇ ПІД ЧАС ВІЙНИ……..……8

1.1. Теоретико-понятійний аналіз явища «інформаційна безпека» як предмету дослідження……..8
1.2. Методологія дослідження інформаційної безпеки……14

РОЗДІЛ 2. МЕТОДОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК НЕОБХІДНОЇ СКЛАДОВОЇ ПІД ЧАС ПРЯМОГО ВІЙСЬКОВОГО ВТОРГНЕННЯ……..…22

2.1. Зарубіжний досвід забезпечення інформаційної безпеки……..…22
2.2. Проблематика воєнно-інформаційної безпеки в Україні: становище й потенціал……..…29
2.3. Ключова роль інформації в сучасній війни……35

РОЗДІЛ 3. КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА УМОВ ВЕДЕННЯ ВІЙНИ……..…41

3.1. Державна політика щодо забезпечення воєнно-інформаційної безпеки……41
3.2. Механізми воєнно-інформаційної безпеки в умовах війни……46
3.3. Стратегія та перспективи в забезпеченні воєнно-інформаційної безпеки під час активних бойових дій та післявоєнного врегулювання. ……50

ВИСНОВКИ……..57

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……..……60

ВСТУП

Актуальність теми дослідження.

Людство вже десятиліттями живе в сучасному інформаційному суспільстві, де інформація є невід'ємною частиною нашого життя. Дані й інформаційні потоки охопили всі сфери людської життєдіяльності. Кожен суспільний процес пов'язаний з обробкою, передачею за використанням інформаційних технологій. Неможливо уявити світ без доступу до інформаційних технологій. Рівень суспільного розвитку неустанно йде до повної інформатизації і переходу на виключно інформаційний вимір. Безумовно інформатизація призвела до значних позитивних змін, для автоматизації багатьох процесів.

Сучасні конфлікти внаслідок глобальної інформатизації почали використовувати інформацію як зброю, охопивши до цього недоступні засоби завдати значної шкоди противнику. Так, використовуючи інформаційні впливи, маніпуляцію, пропаганду та інші інформаційні компанії існує критична потреба в забезпеченні надійної інформаційної безпеки. В той час як в контексті ескалації конфлікту в Україні потреба в забезпечення воєнно-інформаційної безпеки стала найбільш актуальною за всі останні роки дослідження проблематики.

Актуальність даного дослідження полягає в комплексному аналізі існуючого стану воєнно-інформаційної безпеки України, розуміння системних недоліків в забезпеченні інформаційної безпеки держави і громадян під час кризисного реагування.

Об'єктом наукового дослідження є воєнно-інформаційна безпека в умовах ведення війни.

Предмет дослідження - вплив воєнно-інформаційної безпеки на забезпечення миру та гарантій безпеки

Мета магістерського дослідження - дослідити вплив воєнно-інформаційної безпеки, її роль в забезпеченні миру та гарантій безпеки

Відповідно до мети дослідження, сформовані наступні завдання:

1. Провести теоретико-понятійний аналіз явища інформаційна безпека як предмету дослідження.
2. Дослідити методологічні засади інформаційної безпеки..
3. Проаналізувати зарубіжний досвід забезпечення інформаційної безпеки.
4. Виокремити проблематику воєнно-інформаційної безпеки в Україні, її становище та потенціал.
5. Виявити роль інформації в сучасній війни.
6. Дослідити державну політику щодо забезпечення воєнно-інформаційної безпеки.
7. Розробити та обґрунтувати механізми воєнно-інформаційної безпеки в умовах війни
8. Проаналізувати стратегію та перспективи в забезпеченні воєнно-інформаційної безпеки під час активних бойових дій та післявоєнного врегулювання.

Хронологічні межі: нижня межа 2014 рік – верхня межа 24 лютого 2022 року.

Науково-практична новизна дослідження полягає в аналізі існуючих теоретичних досліджень через призму ескалації конфлікту як Сході України так і по всій території.

Науково-практична значущість дослідження полягає в систематизації теоретичних засад, виокремленні інформації задля глибшого розуміння проблематики забезпечення інформаційної безпеки.

Структура магістерської роботи складається з титульного аркушу, анотації, змісту, вступу, трьох розділів: в першому розділу – 2 підпункти, в другому і третьому по 3 підпункти, висновків, списку використаних джерел та літератури. Загальний обсяг кваліфікаційної (магістерської) роботи становить 67 сторінок.

РОЗДІЛ 1. Теоретичні засади інформаційної безпеки за умов збройного конфлікту та критичність ролі інформації під час війни

1.1. Теоретико-понятєвий аналіз явища «інформаційна безпека» як предмету дослідження

Науковий прогрес, створення нових засобів комунікації, передачі інформації, використання її у різних форматах створюють в купі нове суспільство в якому ми впевнено живемо. Інформаційне суспільство - це відносно глобальне поняття, яке описує рівень усього людства на даному етапі розвитку. Якщо дивитись з перспективи конкретних суспільств і держави, зокрема, то ми можемо спостерігати реальну різницю інформаційного вибуху, спосіб та етап формування в залежності від регіону, країни, стану її економічного, соціального розвитку тощо. Тобто рівень розвитку й використання інформаційних технологій, сучасних засобів комунікації в світі дуже нерівномірний, наприклад доступ до Інтернету на момент 2022 року - лише 62.5% жителів Землі [74]. Тобто, ми можемо сказати що різні суспільства перебувають на зовсім інших етапах технологічного, інформаційного розвитку. Людина постійно в пошуках інформації, навіть на базовому рівні розвитку: пошук води, полювання на тварин, інформація про інше плем'я чи. Або, що більше стосується сучасної людини – пошук інформації через мережу Інтернет, або передача персональних даних, що в свою чергу безпосередньо пов'язано з діяльністю в інформаційному суспільстві та безпекою даних. За умови формування інформаційного суспільства значення інформації та даних зростає невпинними темпами.

Науковці, розглядаючи тематику інформаційної безпеки звертають увагу на актуальність, розповсюдження інформаційних технологій в кожній сфері життєдіяльності суспільства. Таким чином, питання інформаційної безпеки набуває суттєвого значення і стає предметом правового

регулюванням, важливішим показником гарантування національної безпеки та безпеки держав зокрема, мова йдеться про дотриманням прав і свобод людини. Отже інформаційну безпеку можна розглядати як практичну діяльність людини до держави і суспільства.

Ми впевнено можемо сказати про те, що безпека не вийшла на новий рівень розуміння і відношення до її забезпечення. Правильне розуміння безпеки здатна чинити вирішальний вплив на зміст і розвиток суспільних процесів. Таким чином, виникає актуальність розглядати інформаційну безпеку як окрему наукову категорію і як суспільне явище, яке створює нові умови світового порядку і взагалі формування нових норм і правил суспільних відносин. Додаючи, що сьогодні інформація є зброя і проти кожної зброї має бути визначений механізм регулювання і забезпечення безпеки для мінімізації викликів і наслідків ведення інформаційної війни.

На жаль, українці стали свідками того який вплив має інформація на сьогоднішній день. Отже для повного розуміння процесів, треба розуміти природу і контекст інформаційного протиборства. Взагалі, це природне становище за умов конкуренції сучасного світу, та безпеці приділяється особлива увага залежно від контексту: починаючи від збереження балансу інтересів, завершуючи змінами міжнародного правопорядку та веденням відкритої війни [38].

Інформаційна безпека поняття, яке можна розглядати й тлумачити різними способами. Наприклад, мають місце доктринальні, енциклопедичні так і нормативно-правові визначення. Відповідно методологічні підходи, сфери застосування можуть суттєво відрізнятись. Нас цікавить міжнародний контекст і використання інформації як одного з засобів ведення війни, відповідно це є фокусним показником подальшого дослідження.

Слід розглянути нормативно-правові акти України для визначення інформаційної безпеки з легальної сторони. Стаття 17 Конституції України

свідчить: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу»[22].

Для визначення проблематики вивчення інформаційної безпеки з точки зору законодавства, то в Законі України «Про інформацію» тематика майже не розкрита. Ми виокремлюємо поняття інформаційна безпека, і окреме поняття «захист інформації». Де, під захистом розуміється сукупність правових, організаційних, адміністративних та інших заходів націлених на збереження, цілісність та доступ до інформації. Таким чином, ми можемо сказати що з боку закону ми не враховуємо усі можливі ризики нанесення шкоди інформаційній безпеці у сфері державного управління [17].

Звичайно що, закон не стоїть на місці, а постійно адаптується під нові обставини, умови та, безумовно, технології, які охоплюють усі сфери зокрема безпекові. Так, відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"» «інформаційна безпека України - складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система 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» [66].

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. Таким чином законодавча невпевненість щодо параметрів інформаційної безпеки за останні роки, які вже сьогодні розуміючи, були критичними, ускладнюють негайне реагування на загострення збройного конфлікту і ведення нового типу війни на сьогоднішній день.

Як було зазначено, законодавство постійно розвивається, особливо в інформаційній сфері. На протязі останніх років низка документів були оновлені або створені, задля покращення законодавчого забезпечення інформаційної сфери. Наприклад, Закон України «Про інформацію» [17]. Або, Указ президента "Про Стратегію інформаційної безпеки" [66]. Однак, слід зауважити, що в сучасних умовах війни й подальшого післявоєнного відновлення суспільних процесів необхідною є адаптація та якісні зміни існуючих законів та нормативно-правових актів. Адже, навіть з існуючими правками воно є не повністю визначеним і деякі питання залишаються суперечливими й не систематизованими. А найголовніше, воно є не розповсюдженим на суспільство. Мається на увазі, що суспільство, громадяни, як основні споживачі інформації є не захищеними від інформаційних впливів і атак. Прийдемо приклад, що тільки після початку повномасштабного вторгнення, люди почати отримувати листівки, брошури та повідомлення про проросійськи, ненадійні або брехливі джерела інформації з призовом перестати отримувати інформаційну пропаганду ворога і піддаватись під його вплив. Однак, це розповсюджена ситуація, яка прикладом показує важливість не тільки правового забезпечення безпеки інформації та даних, а й говорить про освітню частину процесу повного забезпечення інформаційної безпеки.

Повертаючись до указу президента від 28 грудня 2021 року, є прописаний пункт, що «інформаційні заходи оборони держави - сукупність скоординованих дій, які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України в мирний час, в особливий період, в

умовах воєнного або надзвичайного стану щодо прогнозування та виявлення інформаційних загроз у воєнній сфері, запобігання, стримування та відсічі збройній агресії проти України, протидії інформаційним загрозам з боку держави-агресора, а також здійснення інших необхідних дій в інформаційному протиборстві» [66].

Тематика досліджень використання інформаційних технологій в науковій літературі представлена технологічними і гуманітарним напрямами. Технологічний підхід розглядає програмно-технічну сторону процесу забезпечення інформаційної безпеки. Гуманітарний, на відміну, розглядає інформаційну безпеку в якості міждисциплінарної галузі.

На думку В.С. Цимбалюка та А.В. Бабінської, 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 [69].

Дослідник О.А. 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 [43, с.19]

Досліджуючи питання інформаційної безпеки Л.О. Кочубей зазначає, що це стан захищеності життєво важливих інтересів, включаючи нформаційну озброєність держави, суспільства, окремої особистості, за якого жодні інформаційні виклики неспроможні спричинити деструктивні думки і дії [45, с. 221-222].

Роблячи висновок, можна сказати, що поняття «інформаційна безпека» є складною конструкцією, що зумовлюється комплексною соціально-правовою природою, завдяки різноманітті інформаційних відносин в суспільства; відмінністю суб’єктів інформаційних відносин з власними

інтересами, правами та обов'язками залежно від галузі використання. Для дослідження інформаційної безпеки використовується весь накопичений досвід, в тому числі історичний, адже використання інформації як зброї почалось ще задовго до появи сучасних технологій.

Сьогодні роль інформації – критична як ніколи. Все частіше озброєнні конфлікти переходять в новий інформаційний простір, коли інформація з фронту отримується за лічені години, що в свою чергу створює багато інформаційного шуму та дезінформації. В стратегії про інформаційну безпеку прописані комплексні інформаційні заходи, які реалізується державою задля запобіганню виникнення кризової ситуації, передбачаючи діалог з громадянами щодо загрози виникнення кризової ситуації і протидії їй. Так, ми бачимо діалог влади, в лиці Президента України, який кожного дня з моменту загострення збройного конфлікту з 24 лютого 2022 року знімає відео-звернення до народу України з метою надійного інформування, запобіганню дезінформації тощо. Що в свою чергу є засобом стратегічної комунікації, коли відбувається скоординоване і належне використання комунікативних можливостей держави.

Інформація не просто стає, вона вже стала одним із найголовніших ресурсів сучасного світу і забезпечення безпеки є ключовим обов'язком держави по відношенню до власних національних інтересів і суверенітету, адже сьогодні ми можемо спостерігати наслідки не системного забезпечення інформаційної безпеки в України, що призвело до нових гібридних викликів в війні Росії проти України.

1.2. Методологія дослідження інформаційної безпеки

Для формування сучасної безпеки держави потрібно шукати нові підходи до інформаційної безпеки, аналіз вже існуючих, їх необхідна модернізація і безумовно розробко нових моделей забезпечення інформаційної безпеки. Процес аналізу й певного переоцінювання сучасної теорії безпеки зумовлює розробку теоретичних засад інформаційної безпеки, їх чітке визначення, моделі правового регулювання в державі й інших інститутах.

Стан сучасного розвитку гуманітарних наук створює середовища плюралізму підходів до розуміння інформаційної безпеки, визначенню її моделі тощо. Якщо порівнювати, то подібне різноманіття думок спостерігається і в інших питаннях: сенс політики, влади в політології, соціології й інших сферах людської життєдіяльності. Неможливо обмежити підходи не тільки через різний рівень інформаційної забезпеченості, а й через різний культурно-соціальний стан держав, їх спроможності забезпечити належний в сучасному світі рівень інформаційної доступності, а відповідно і рівень розвитку інформаційної безпеки.

Відсутність єдиної продуманої та збалансованої правової політики щодо інформаційної безпеки обумовлено різноманіттям поглядів серед вчених щодо визначення інформаційної безпеки. В свою чергу врівноваження відбувається єдністю думок представників державної влади, які слідують європейського стандарту щодо соціальних явищ, таких як наприклад інформаційна безпека. Методологічний аналіз процесу розуміння безпеки зачіпає питання його методології, як пріоритету для теорії права.

Основні теоретичні підходи до природи розуміння інформаційної безпеки:

1.) Дослідник Д.А. 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 [41, с. 95].
2.) Інший підхід науковця В.В. Антонюка розглядає інформаційну безпеку, як явище суспільного життя, тобто не тільки як науковий пошук істини [1, с. 23].

Таким чином, підхід до поняття інформаційної безпеки включає в себе наступні погляди: безпека як система знань і уявлень про розвиток правових явищ. Розуміння інформаційної безпеки в широкому підході можна розподілити на:

1.) Науково-теоретичний;
2.) Професійно-практичний;
3.) Буденно-повсякденне.

На думку науковці А.Ю. 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» [46, с. 9-11].

Тріада соціальних інститутів: людина, суспільство та держава складають три основні безпекові орієнтири, які в свою чергу визначають соціально-політичну сутність безпеки. Безпека людини, суспільства та держави, на думку дослідників є змістом національної безпеки. А саме усвідомленим захистом інтересів, соціальних потреб названих суб'єктів, безпечним їх задоволенням.

Розглядаючи вивчення інформаційної безпеки через призму політологічної науки, то можна звернути увагу, що воно поняття ще недостатньо розвинуте. При цьому актуальність й необхідність цілісного усвідомлення проблематики безпеки у політологічному ключі у зв'язку з проблемами демократії,

політичного режиму, політичних структур та організацій, ідеологій та цінностей.

Якщо повертатись до тріадної структури, яку частково відображають дослідники державного управління. Так, наприклад З. Коваль вважає, що інформаційна безпека держави розуміється як «захищеність інформації та забезпечення цілісності й надійності критичної інформаційної інфраструктури держави від випадкових та навмисних впливів природного чи штучного характеру» [24, с. 11], а інформаційна ж безпека особи та суспільства − як «захищеність психіки і свідомості від небезпечних інформаційно психологічних впливів: маніпулювання, дезінформації, спонукання до запланованих противником дій» [24, с. 11].

Враховуючи, що однією з завдань магістерської роботи є дослідження й аналіз методологічного дослідження інформаційної безпеки, а відповідно і вивчення можливостей протидії інформаційним загрозам, які тільки набувають ще більшого значення й впливу і є поширеними в сучасному глобалізованому світі. Протидія і захист відбуваються на різних рівнях: індивідуальному, громадянському, соціальному та державному. Зазначимо, що рівні взаємопов’язані, що говорить про актуалізацію загальної проблематики інформаційної безпеки, що впливає і взаємодії з різними сферами суспільної життєдіяльності та державно-безпекового функціонування.

Вчений 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» [23, с. 13]. По-друге, «стан захищеності інформаційного середовища/простору загалом, який

забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави» [23, с. 13].

На сьогоднішній день поняття «інформаційна безпека» набула широкого використання в наукових публікаціях, навчально-публіцистичній літератури, і головне в нормативно-правових документах різного рівня і сфери. Однак в інтерпретаціях поняття немає єдності, в тому числі через визначення поняття різними мовами. Іноді відбуваються в розумінні самого терміну «інформаційна безпека». 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 [47].

Зазвичай дослідники запозичують основний зміст визначення терміну з міжнародних стандартів, однак не завжди враховують його багатозначність. Так, поняття ***«information security»*** може перекладатись з англійської і як «інформаційна безпека», і як «безпека інформації», що не є синонімічними і створює зовсім різне тлумачення одного явища. Таким чином, ***герменевтичний підхід*** не є зайвим при виборі методології дослідження інформаційної безпеки.

Зростаюча динаміка, постійне зростання спроможності інформаційних технологій, з кожним роком тільки актуалізує проблематику дослідження інформаційної безпеки. Так, окрім сфери державного управління ми також звертаємося до міждисциплінарного підходу щодо проблем безпеки, таким чином розширюючи горизонти розуміння. Розглядаючи напрацювання ***соціальної філософії***, дослідник В. Триняк зауважує, «складну динамічну структуру інформаційної безпеки, а також системи інформаційних зв'язків визначає велика кількість інформаційних потоків» [64, с. 11].

Особливу увагу слід приділити методології дослідження й проблематиці інформаційно-безпекової ситуації в сучасній системі міжнародних відносин. В цьому контексті це набуває надзвичайної актуальності, адже інформація сьогодні перетворилася на ключовий економічний, політичний, соціальний і навіть військовий інструмент міждержавної взаємодії. Так, важливість і актуальність ефективності інформаційної безпекової політики в міжнародних відносинах України підтверджують події останніх років, в навіть і днів, коли держава потерпає від значних агресивних впливах ззовні. Тож сьогодні нам крайнє важливо підтримувати існуючу стратегію інформаційної безпеки, і в майбутньому через аналіз і моніторинг розробити план удосконалення, підтримки і ресурсне забезпечення розвитку системи інформаційної безпеки держави, яка буде стійка до зовнішній викликові, які з'являються в різних вимірах суспільних відносин.

Втім, важливою складовою інформаційної безпеки є ***феноменологічний***, ***політико-філософський*** вимір. Мова йдеться про те, що сьогодні потрібно розробляти не тільки засоби забезпечення інформаційної захищеності інститутів, а й світоглядно-аксіологічні проблеми забезпечення такої захищеності. Тобто важливо, щоб кожен громадянин усвідомлювали власну відповідальність на лінії інформаційної захищеності власної держави і народу. Таким чином актуалізується загально-філософський зміст, коли інформаційна безпека розглядається у тісному взаємозв'язку з можливостями і проблемами інформаційного суспільства [21].

Ширше тлумачення інформаційної безпеки є не окремою частиною національної, не лише інструментом запобігання загроз, але й невід'ємною, наскрізною характеристикою сучасного суспільства загалом. Як своєрідний показник захищеності громадян, суспільства, держави та глобального співтовариства загалом. Говорячи про широкі категорії у методиках дослідження ми передбачаємо дотримання концептуально-теоретичного *принципу системності*. У дослідженні різних аспектів інформаційної безпеки,

коли ми говоримо про держави, суспільства або окремих людей, жодна складова не може бути осмислена поза рамками системних взаємодій. Так, жоден вузький підхід до безпеки не може бути визнаний абсолютним, а політичний феномен не може бути розглянутий поза контекстом інформаційного суспільства. Системне розуміння інформаційної безпеки пов'язане з глобалізаційними тенденціями, диджіталізацію політики і взагалі усіх сфер життєдіяльності, темпом сучасних політичних відносин і процесів тощо.

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» [33, с. 35]

Політико-правовий зміст інформаційної безпеки, розгляд системоутворюючих принципів нормального, безпечного та законодавчо окресленого соціуму, як частини глобального інформаційного суспільства. 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» [34, с. 35].

Базовий документ зі створення та функціонування системи забезпечення інформаційної безпеки в Україні − Закон України «Про Національну програму інформатизації» від 04.02.1998 р. № 74/98, який прикметно зазнав змін у 2001,

2010, 2012, 2015 та 2020 рр. [18]. Закон визначив окремі поняття та політологічні категорії. Так, визначено наступні поняття:

1. «Інформаційна технологія - цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування» [18];
2. «Інформаційний суверенітет держави - здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою дотримання законів України, прав і свобод громадян, гарантування національної безпеки держави» [18].

Документ став своєрідним посередником між державними управлінцями, громадським сектором, науковцями, міжнародними експертами тощо, щодо проблематики забезпечення інформаційної безпеки.

Підсумовуючі підпункт щодо методологічного дослідження інформаційної безпеки, було охарактеризовано дослідження тематики інформаційної безпеки в залежності від методів та підходів вивчення. Особливу увагу слід окреслити дослідженню інформаційної безпеки через нормативно-правову призму, основні закони, їх стан і актуальність на сьогоднішній день.

В цілому виявлено, що проблематика інформаційної безпеки щільно пов’язана з дослідженням феноменів інформаційного суспільства, стану інформаційного простору, розумінні інформації та в контексті національної безпеки держави.

Можемо підкреслити, що дослідження інформаційної безпеки її нормативно-правовий статус все ще є недостатньою мірою систематизованою, навіть не зважаючи на критичну актуальність інформаційної безпеки в

контексті військового стану нашої держави. Тобто механізми забезпечення інформаційної безпеки потребують додаткового аналізу через практичний досвід застосування в кризовому становище.

РОЗДІЛ 2. МЕТОДОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК НЕОБХІДНОЇ СКЛАДОВОЇ ПІД ЧАС ПРЯМОГО ВІЙСЬКОВОГО ВТОРГНЕННЯ

2.1. Зарубіжний досвід забезпечення інформаційної безпеки

Вивчаючи питання інформаційної безпеки слід приділити окреме значення міжнародному досвіду забезпечення інформаційної безпеки людини, суспільства і держави. Таким чином, аналізуючи вже розроблені системи захисту ми можемо сформувати власну стратегію забезпечення безпеки беручі найкращій досвід партнерів. Втім, для того щоб перейти до більш конкретних прикладів держав та інституцій слід розглянути інформаційну безпеку через призму міжнародного права.

Розробка інформаційної безпеки людини, суспільства та держави ведеться як на національному, так і на міжнародному рівні. До цього в політичному, правовому та науковому дискурсі. Глобальність інформаційного простору з поки що слабкими засобами ідентифікації користувачів, розвиток всесвітніх соціальних мереж тощо призводять до суттєвого впливу на сталий розвиток суспільства. Однією із складнощів забезпечення безпеки є висока вразливість національних і міжнародних інформаційних інфраструктур, часткова неможливість або повна відсутність встановити обмеження для збору інформації не порушуючи особисті свободи та міжнародну стабільність.

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 [16,с.9].

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.М. 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 [20].

Відповідно до дослідження Є.А. Макаренко «Міжнародна інформаційна безпека: Сучасні виклики та загрози» 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 [44].

Основні міжнародні нормативно-правові норми для розуміння забезпечення міжнародної інформаційної безпеки закріпленні у Статуті ООН, а також в ряді інших нормативно-правових актах. Саме вони формують правову базу для розв'язання збройних конфліктів, вивчають засади міжнародного гуманітарного права. Також, ці нормативно-правові акти регулюють процес упередження та боротьби з міжнародним тероризмом.

Серед основних правових принципів щодо забезпечення інформаційної безпеки виділяють наступні:

- Суверенна рівність держав в інформаційній сфері, щодо використання ресурсів, забезпечення інформаційного суверенітету, а також рівна участь в процесах розробки міжнародних правових документів в інформаційній сфері;

- «принцип невтручання у внутрішні справи інших держав, неприпустимість інформаційної інтервенції з метою проведення спеціальних інформаційних кампаній, ворожої пропаганди та поширення деструктивної чи спеціально спрямованої інформації» [68, с. 111; 30, с. 18];
- Заборона застосування сили, тобто заборона використання інструментами інформації впливів проти держав, їх територіальної цілісності або незалежності;
- «принцип мирного врегулювання міжнародних спорів, який зобов'язує держави до превентивної дипломатії або переведення збройного конфлікту на переговорний рівень за допомогою інструментів інформаційного впливу» [68, с. 111; 30, с. 18];
- «принцип територіальної цілісності та непорушності кордонів, який стосується визначення меж національного інформаційного простору та заходів захисту від несанкціонованого втручання ззовні» [68, с. 111; 30, с. 18];
- «принцип дотримання фундаментальних прав і свобод людини, який визначає конституційні та спеціальні норми, а також норми міжнародних договорів щодо свободи слова та вільного обігу інформації, незалежності і плюралізму міжнародних мас-медіа, свободи вираження, заборони цензури та захисту конфіденційності інформаційних ресурсів» [68, с. 111; 30, с. 18];
- «принцип самовизначення народів і націй, який встановлює права національних меншин на культурну самобутність та інформаційну діяльність; принцип міжнародного співробітництва, який зобов'язує держави співпрацювати задля зміцнення миру та міжнародного взаєморозуміння, розвитку глобальної інфраструктури з метою досягнення інтересів людства» [68, с. 111; 30, с. 18]

Таким чином, існує комплекс політико-економічних та соціокультурних принципів необхідних для міжнародних відносин.

Для більшого розуміння зарубіжного досвіду забезпечення інформаційної безпеки слід розглянути досвід на рівні Північноатлантичного альянсу та Європейського Союзу, враховуючи зовнішньополітичний курс України. Так, одним із пріоритетів національних інтересів України відповідно до Закону України «Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України» від 8 червня 2017 року визначено напрям інтеграції у безпековий простів НАТО відповідно до цілі вступу в Альянс [19].

На сьогоднішній день співпраця з НАТО вийшла на значно новий рівень, враховуючи відкриту війну Росії проти України, однак зміни в законодавстві від 2017 року свідчать про поглиблення співпраці Україна – НАТО задля подальшого членства. Однак, якщо фокусуватись на чіткому питанні політики інформаційної безпеки НАТО в сучасному світі, необхідно зрозуміти суть інформаційної політики і забезпечення безпеки інформації у системі організації.

На сьогоднішній день регуляція інформаційної сфери НАТО відбувається за наступними напрямками:

- Конкурентне середовище, боротьба з монополією засобів масової інформації;
- Можливості, в тому числі технічні, й права доступу до інформації та ресурсів у всього населення;
- Свобода слова, її дотримання;
- Захист інтересів національних меншин, культурної спадщини, мови, протистояння культурній експансії;
- Охорона інтелектуальної власності та боротьба з піратством;
- Протидія кіберзлочинності;

- Правове регулювання мережі Інтернет;
- Забезпечення інформаційної безпеки [39, с. 22-23].

Контроль військово-політичної сфери НАТО розглядає в тому числі питання інформаційної політики Основним органом щодо інформаційної політики в організації виступає Атлантична рада, яка виконує функції офіційного «рупору» альянсу, яка оприлюднює свої рішення й заяви для широкого загалу.

Забезпечення інформаційної безпеки НАТО було на порядку денному ще при створенні організації, і основні засади були розроблені достатньо давно. Так, засади політики НАТО щодо забезпечення безпеки інформації прописані у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)» [73]. 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. Представники цього органу беруть участь у нарадах Комітету безпеки НАТО, де безпосередньо розробляються політики й інституції у безпековій сфері. Функції відповідального органу залежать від розміру, кількості населення країни, географічні фактори і самого розподілу між органами у сфері національної безпеки. Тобто, це означає, що в окремих країнах це орган може входити до структури міністерства закордонних справ, оборони та юстиції (мова йдеться про країни НАТО); в інших країнах керівниками стають прем’єр-міністр або міністр внутрішніх справ. В рамках Ради євроатлантичного партнерства та «Партнерство заради миру», зокрема з Україною, партнерство передбачає обов’язки партнерів щодо питання інформаційного обміну й забезпечення безпеки [51].

Проблематика інформаційної безпеки НАТО здебільшого полягає в політичному вимірі, незважаючи на питання технічного забезпечення й стратегічного планування. Мається на увазі застосування статті 5 Вашингтонського договору по відношенню саме до інформаційних атак. Деякі члени Альянсу рішуче виступають проти розширення дії колективної відповідальності у сфері інформаційної безпеки НАТО. Правда, слід підкреслити що питання протидії інформаційним загрозам відноситься до «м'якої безпеки», в той час як головною задачею організації є протидія конвенційним викликам безпеки – тобто «жорсткої безпеки» [56, с. 252] Таким чином, відбувається розподіл між країнами, внаслідок чого, одні спеціалізуються на «м'якої безпеці» інші на «жорсткій», з застосуванням військових місій.

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 [75, с. 35].

Втім зауважимо, що переважна більшість європейських країн є членами Організації Північноатлантичного договору та Європейського Союзу одночасно. Тобто на них поширюються стандарти цих організацій щодо інформаційної політики та безпеки.

В рамках Європейського Союзу інформаційна відкритість державної влади країн учасниць є важливим елементом правового забезпечення безпеки. Так, в резолюції Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» від 18 грудня 2013 року [75] було зазначено про глобальність й відкритість мережі Інтернет, його інтенсивний розвиток у сфері

інформаційних та комунікаційних технологій. Відповідно до резолюції «ті ж права, що люди мають в оффлайн-режимі, мають також бути захищені онлайн, у тому числі право на приватність» [75].

Якщо розглядати нормативно-правові документи країн ЄС, то можна зробити висновок того, що:

- пріоритетність права людини розпоряджатись своїми персональними даними;
- використання персональних даних без дозволу особистості – відповідальність згідно з законодавством;
- той, хто користується персональними даними фізичних осіб з їхнього дозволу в разі умисного розголошення цих даних третім особам - встановлено відповідальність. [11, с. 5-6].

Основний документ ЄС про захист персональних даних «Директива 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних»» [13]. В якому говориться про бажання забезпечення вільного використання інформації, її переміщення, всередині країн ЄС.

Таким чином, роблячи висновки щодо інформаційної безпеки ЄС, то можна констатувати, що вони сформували злагоджену систему захисту інформації, але втім кожна держава має своє бачення, закони, інституції щодо врегулювання питань інформаційної безпеки.

Отже, роблячи висновки щодо зарубіжного досвіду, можна сказати що з метою набуття членства в НАТО та ЄС Україна активізує зусилля реформ, в безпековому та оборонному секторах зокрема. Розуміючи ситуацію в світі, інформаційна безпека стає одним із найважливіших аспектах забезпечення національної та міжнародної безпеки в цілому.

2.2. Проблематика воєнно-інформаційної безпеки в Україні: становище й потенціал

Україна унікальна держава, яка знаходиться в епіцентрі подій першої в світі війни, коли інформаційний простір стає полем боя. Інформація для України – зброя, броня та інструмент впливу. Інформаційний простір став потужним «фронтом» боротьби, як зі сторони громадянського суспільства, так і по відношенню до державних органів влади.

Збройний конфлікт якій відбувається з 2014 року, ескалація якого відбулась в 24 лютого 2024 року створив нову реальність. Коли інформаційні потоки настільки потужні, що складно сконцентруватись на дійсно важливий інформації. Війна Росії проти України – це один із небагатьох прикладів, коли військові зведення отримують через годину після події, коли Президент держави записує кожного дня відео-ролики, для мінімізації розповсюдження фейкової інформації. Інформаційна безпека зараз безперечно є популярною темою, яку експлуатують ЗМІ, політики тощо.

За останні роки в Україні майже усі процеси розвивались достатньо динамічна, тут інформаційна безпека не стала виключенням. Тож сьогодні вона є процесом якому здійснюються конкретні інформаційні впливи. Чинники ескалації загроз інформаційної безпеки мають комплексний характер, тобто охоплюють усі сфери життєдіяльності, людини, суспільства її жертви.

Загрози національним інтересам та безпеці в інформаційній сфері згідно Закону України «Про основи національної безпеки України» [49] можна віднести наступні прояви:

- Обмеження свободи слова та доступу громадян до інформації, розповсюдження ЗМІ культу насильства, жорстокості та порнографії;
- «Комп’ютерна злочинність та комп’ютерний тероризм» [49];

- Розповсюдження державної або іншої таємниці, конференційної інформації, яка є власністю держави «або спрямована на забезпечення потреб та національних інтересів суспільства і держави» [49];
- Маніпулювання свідомістю суспільства шляхом поширення інформації, яка є недостовірною, неповною або упередженою [49].

Загрозами інформаційній безпеці, згідно з актуальним законодавством, можна вважати неповну, невчасну й невірогідну інформацію, яка використовується задля негативного інформаційного впливу. До цього самі інформаційні технології, їх розвиток, стають загрозами безпеки, без надійного механізму протидії та забезпечення стабільного правового інструменту. Також, слід додати, нелегальне розповсюдження, використання та доступності інформації, як наслідок порушення конфіденційності та цілісності [9,с.102].

Постанова Кабінету Міністрів України „Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” [50] містить правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Згідно постанові, для захисту інформації необхідно створити комплексну систему від:

- По-перше, витоку даних технічними каналами під час функціонування засобів обробки інформації та комунікації;
- По-друге, неправомірних маніпуляцій з інформацією, включаючи використовування її для розповсюдження комп’ютерних вірусів;
- По-третє, впливу на обробку інформації, що в разі чого призводить до порушення цілісності та блокування [50].

Дослідники не мають спільної думки щодо класифікації загроз інформаційній безпеці. Наприклад, науковець В. Ліпкан класифікує загрози інформаційній безпеці таким же чином як і загальну щодо національної безпеки. А саме, розглядає за наступними класами як: джерело походження

(техногенне або антропогенне); гіпотетична шкода (небезпека або загроза); періодичність (повторюваність та продовжуваність); сфера походження (екзогенна або ендогенна); ймовірність реалізації (вірогідна, неможлива або випадкова); рівень детермінізму (закономірна або випадкова); значення (допустима, неприпустима); структура впливу (системна, структурна або елементна); характер реалізації (реальна, потенційна, здійснена або уявна); ставлення (об'єктивна або суб'єктивна); об'єкт впливу (особа, суспільства, держава) [34].

Втім науковці С. Гуцу [12] та О. Литвиненко [35] вважають, що загрози можна класифікувати наступним чином:

А) Розповсюдження неякісної інформація, в тому числі дезінформація, що транслюється на особистість, суспільства та державу;

Б) Реалізація впливу (зазвичай несанкціонованого) на інформацію та ресурси на різному етапі їх формування;

В) Створення загрози правам і свободам особистості в інформаційній сфері, а саме право на виробництво, пошук, поширення тощо інформації; в тому числи право на власність інформації.

М. Макарова виділяє наступні загрози в мережі:

– дані навмисно перехоплюються, зчитаються або змінюються;

– користувачі ідентифікують себе невірно, тобто отримує несанкціонований доступ [37].

Більш ширшу класифікацію пропонує А. Погребняк. Він підкреслює випадковість та навмисність інформаційних загроз:

Випадкові загрози:

1. помилки обслуговуючого персоналу і користувачів;
2. втрата інформації внаслідок неправильного її збереження;

3. випадкове знищення або заміна;
4. збій у роботі електроживлення або комплектуючих елементів мережі;
5. «некоректна робота програмного забезпечення, зокрема внаслідок зараження комп'ютерними вірусами тощо» [52,с.46-47].

До навмисних загроз відносяться:

1. несанкціонований доступ до інформації і мережевих ресурсів;
2. розкриття і модифікація даних і програм, їх копіювання;
3. розкриття, модифікація або підміна трафіка обчислювальної мережі;
4. розробка і поширення комп'ютерних вірусів;
5. крадіжка магнітних носіїв і розрахункових документів;
6. руйнування архівної інформації або навмисне її знищення;
7. фальсифікація інформації, маніпуляція фактором одержання чи не одержання інформації;
8. перехоплення інформації ворогом або [52,с.50].

Найбільша проблематика воєнно-інформаційної безпеки полягає в тому , що держава знаходиться в режимі відкритої війни, з постійним загрозами, викликами тощо, тобто це тимчасове припинення стратегічного планування. Адже виходить стратегічно реагувати.

Поняття «Гібридна війна» до 2014 року була майже невідома українським засобам масової комунікації, як і серед політиків і звичайних громадян. В міністерстві оборони США обговорюючи питання гібридної війни науковці і окреслювали її «як сукупність загроз з боку держав і недержавних організацій, що використовують комп'ютерні мережі та супутникові атаки; портативні ракети «поверхня-повітря»; саморобні вибухові пристрої; маніпулювання інформацією та засобами масової інформації; хімічну, біологічну, радіологічну, ядерну зброю» [76].

Науковець Є. Магда визначає гібридну війну «як прагнення однієї держави підпорядкувати собі іншу за допомогою політичних, економічних,

інформаційних інструментів» [36]. Тому в умовах гібридної війни бойові дії є другорядними, в той час як на перший план виходять інформаційні операції та інші важелі впливу. Війна полягає у прагненні однієї держави агресивно діяти на свідомість жителів іншого. Іншими словами – це прагнення не знищити мільйони людей, а залякати й деморалізувати їх. Завдяки швидкості поширення інформації світом вона перетворилася не лише на товар, а й на зброю [36].

Важливою умовою ведення гібридної війни є моніторинг ситуації і використання внутрішніх криз. Наприклад швидка анексія території півострова Криму відбулася через інформаційні інструменти ведення конфліктів. Зокрема, серед передумов, які сприяли можна виділити: послаблення влади – а відповідно контролю над територією, коли частковий безлад через зміну влади призвів до майже відсутності державного контролю; ріст суперечностей, поява нових й актуалізація вже існуючих розбіжностей між центральною владою та локальними структурами; стан українським безпекових структур – повністю знищена структура армії, від психологічного до матеріально-технічного аспекту, відповідно повна де-моралізація; пропагандистська робота РФ, яка особливо активно й продуктивна отримувала результати на півострові та Східних частинах України, які й постраждали від агресії Росії другими після Криму, ставши осередками інформаційного впливу, а навіть і самостійним інструментом в руках Кремля.

Внутрішньо політичний вплив значною мірою реалізується також через соціо-культурну та гуманітарну сфери. Серед них наприклад:

- Максимальна протидія українському народу в власному переосмисленні історичної спадщини: фактично українців змушували забути думати про власну історичну цінність, зневажити власний національний внесок в світову культурну спадщину. Як приклад, це маніпуляція колишніми правителями, яких Кремль вважає руськими, в реальності які правили на території сучасної України;

- Повне нівелювання українських культурних цінностей – одна із головних ідей Росії, цілей їх безперервної інформаційної кампанії це знищення української культурної ідентичності, створивши прообраз Малоросії, сільської мови тощо;
- За допомогою культурних інструментів дуже легко створити проросійські настрої в суспільстві: телебачення з російськими фільмами, російські медіа про Україну, мережа Інтернет – яка майже повністю російськомовна, відповідно більшість аудиторії споживання одного контенту росіяни і адаптація йде на Росію. Тобто коли весь інформаційний простір говорить тобі, що ти такий же як руський, ви говорити однією мовою, то межі затираються і формується настрій лояльності або прихилення до Росії;
- Наратив заперечення існування українців як нації, взагалі України як незалежної держави; відповідно риторика усіх медіа платформ, що не існує української мови (вона нібито є лише діалектом російської), зневажання культурою та повна відмова від думки про окрему історію України, про її незалежність (на думку президента РФ, Україну як державу створив Радянський Союз)

Таким чином, в Україні максимально актуальна проблематика воєнно-інформаційної безпеки. Становище на сьогоднішній день, є в режимі надзвичайної ситуації, коли складно повністю об’єктивно оцінити існуючи механізми, нормативно-правове забезпечення тощо. Однак, незважаючи на значні прогалини і не підготовку до активної гібридної війни перспективи подальшого забезпечення мають довготривалу й успішну підготовку та реалізацію беручі найкращі приклади сучасності, через призму вже існуючих загроз і досвіду протидії Російської загрози як в військовому, так й інформаційному просторі.

2.3. Ключова роль інформації в сучасній війни

Важко переоцінити роль інформації в сучасному інформаційному суспільстві коли вона є основним об’єктом. Інформація інтегрована в усі напрямки діяльності держави, суспільства й окремої людини. Так, з появою нових технологій, основою яких є впровадження засобів інформація стає постійним і необхідним атрибутом забезпечення діяльності держави. Інформаційний вплив на державу, суспільство, громадянина зараз є критичнішім за економіко-політичний або військовий вплив. Фактично сьогодні інформація стала реальною, майже фізично відчутною силою. Поняття «інформація» використовується в усіх галузях суспільних наук, зокрема у вивченні питання війни.

Спроби поняття «інформація», відомі ще з часів античності. Зокрема, родоначальником ідеї інформації вважають Платона – «безбарвна, безформна і невловима сутність, в суті своїй існуюча, зрима тільки для керманича душі – розуму». Згідно з Платоном, інформація присутня у світі об’єктивно, поза волею і бажанням людей [3, с. 32].

У наукові дослідження вперше термін «інформація» ввів у 1921 р. англійський вчений Р. Фішер – один із засновників математичної статистики. Під інформацією розуміється відомості, що передаються усним, письмовим або іншим способом. Таке трактування інформації вважається найпростішим або класичним [2].

Ведення інформаційної війни та роль яку відіграє інформація, у сучасних умовах є одним з вирішальних факторів перемоги в збройному конфлікті проти РФ. Особливо для України, яка веде асиметричну війну проти держави з переважаючим військовим потенціалом. Саме від того, як світове суспільство сприймає події в Україні, залежить і рівень політично-соціальної підтримки, і обсяги фінансової за озброєної допомоги України.

Роль інформації під час війни – критична, і зазвичай розглядається в контексті інформаційної війни або протиборства. Інформація є предметом дослідження багатьох сфер, однак розглядаючи саме історію розвитку інформаційних конфліктів роль перетворюється на системне використання інформаційно-комунікативних технологій при веденні війни.

Курбан О.В. в своєму навчальному посібнику «Сучасні інформаційні війни у мережевому онлайн просторі» розглядає розвиток інформаційно-комунікативних технологій у форматі ретроспективи історії міжнародних конфліктів. Починаючи з первісного суспільства Основними типовими прикладами первісних інформаційних війн можна вважати сакральну боротьбу (первісна магія) із силами природи та тваринами, а також на рівні внутрішньо-племінних та міжплемінних конфліктів. Останні супроводжувалися не тільки магічними обрядами, але й першими інформаційними атаками у вигляді залякування, дезінформації, приховування та інших типових для базового рівня інструментів [28, с.13]

Епохи Античності. З появою писемності в інформаційному процесі з’явилась конкретність, чіткість та змістовність. З’явилась можливість для надійного збереження та ефективного поширення інформації. Інформаційні протистояння ранніх держав носили різноманітний характер. Супроводжувались військові дії, політичні, економічні та релігійні процеси. Тобто саме в цей час людина вперше здійснює спроби системного застосування інформаційних технологій. Під час військових дій вожді та полководці того часу застосовували технології залякування, психологічного тиску, дезінформації спрямованих проти ворогів, а також як засіб мотивації для власної армії. Тобто фактично започатковані системи античної епохи зберегли основи і активно використовуються в протистояннях сьогодення [28, с.18].

Епоха Відродження. Середньовіччя заклало основу використання інформаційно-комунікативних технологій під безпосереднім контролем та за

участі церкви. Соціальний інститут церкви стає провідним споживачем та розробником інформації, а також одним із головних учасників інформаційних війн того часу. Засобами масової комунікації того часу базуються на традиційних інструментах: мова, мистецтво, писемність, реклама, література. Саме в епоху Відродження з'являються такі поняття як пропаганда та психологічна війна. Доволі значний внесок у практику ведення інформаційних війн внесла Візантійська імперія. Зокрема ми знаємо багато історичних фактів, коли візантійські імператори перемагали свої ворогів не силою зброї, а шляхом дезінформації, психологічного тиску, підкупу. Особливо активно велися такі 25 війни у протистояннях з князями Київської Русі, ісламськими державами, кочовими племенами давніх тюрків та ін. [28, с 24-26].

Епоха раннього капіталізму. Під час формування ринкових капіталістичних відносин інформація та інформаційні війни виконували допоміжну функцію. У своїй боротьбі суспільства того часу використовували товариства того часу, стереотипи та лозунги («Воля або смерть») Активно застосовувалось акції, демонстрації, медіа та маніпуляцію. Усі провідні світові конфлікти XIX ст. обов'язково супроводжувалися інформаційними протистояннями із застосуванням такого інструменту, як преса, що стала другою глобальною мас-медіа технологією. Серед теоретиків та практиків інформаційних війн зазначеного періоду важливе значення мали розробки прусського генерала Карла Фон Клаузевіца, викладені в його книзі «Про війну» (1832 р.). [28, с 32].

Ми розглядаємо інформацію – як інформаційну зброю, яка поширює ідеї, погляди й ідеологію, стає засобом політики через Засоби масової комунікації. На думку Кобільника Б.Ю та Гізун А.І., в їх роботі «Роль інформаційно-психологічних впливів у інформаційній війні» вони розказують, що інформаційні впливи можуть з'являтися не відразу, а через деякий час. Таким чином, побудована концепція Effects-Based Operations, де розрізняють ефекти відповідно до порядків. Людина зазвичай сприймає лише найближчі

наслідки, а вони можуть бути довготривалими. Як приклад, регулярні покази совєтських фільмів на Новий Рік, що генерує підсвідомий культурний код. Так, пропагандистський вплив стає ледь помітним, адже розтягнутий по часу на десятиріччя маючи конкретні наслідки в майбутньому[29].

На думку Валюшко І.О. в її роботі «Еволюція інформаційний війн: минуле і сучасність» «інформація набуває містеріального і стратегічного значення. Повсюдна інформатизація та інформаційна революція не тільки змінили спосіб нашого соціального життя, економічних і фінансових відносин, а й методи і форми ведення війн, де втрати обчислюються не кількістю загиблих, а кількістю прихильників тієї чи іншої політичної партії, течії, процесу або просто події. Інформаційна війна тепер не є якимось абстрактним поняттям, а цілком реально існуючим фактом, який активно розробляють і вивчають» [5].

У Стародавньому Китаї кілька тисяч років тому було створенні спеціальні стратегії, що застосовувалися однаково у політиці та військовій діяльності. В сучасній літературі вони отримали назву «стратагеми». Так, кожна стратагема, що була виражена у висловлюванні - є схемою не прямого засобу впливу та маніпулювання чужою поведінкою. Отже застосовуючи такі технології можна було ввести противника в оману, дезінформувавши його відповідно власних мотивів, планів та дій. Так досягається перевага над опонентом і з’являлась можливість досягнення успіху з мінімальними втратами ресурсів.

Так Сунь-Цзи писав, що «Війна – це шлях омани; хоч ти й близько від нього, показуй, нібито ти далеко; хот ти й далеко від нього, показуй, що ти близько» Фактично, це формулювання мети дезінформаційних заходів того часу, яке як ніколи є актуальним сьогодні. Слова ніби накладаються на стан сьогоднішніх інформаційних протистоянь, що в свою чергу говорить про системність й глибину історичного контексту для вивчення ролі інформації під час військових дій.

Вступ людства в нову інформаційну сферу змінив розуміння війни. Інформаційні технології змінили правила гри, ставлячи перед акторами міжнародної арени нові засоби, інструменти ведення війни. Взагалі з'явилась нова тактика і стратегія війни. Інформаційна складова змінює не тільки систему озброєнь, а й систему цілей. Так, відбувся перехід до атак, спрямованих не на військові бази, а на спрямовані атаки на електронні системи противника[5].

Таким чином основні елементи й напрямки застосування інформації як важеля впливу, як засобу послаблення морального духу противника, інструмент мотивації свої військ.

Військові фахівці впевнені в тому, що в новітніх війнах інформація є зброєю, яка дозволяє виграти війну без застосування важкої артилерії. Тепер, без спеціальних засобів виробництва, складної військової інфраструктури саме інформація є зброєю масового ураження. Засоби інформаційної війни — це програмне забезпечення, апаратні засоби комп'ютерних вірусів, логічних бомб тощо. Нові засоби потребують меншу вартість виробництва, а втім високу ефективність що під час активних бойових дій, що й у мирний час. Це у свою чергу розширює діапазон можливих комбатантів у такій війні, які включають як окремі країни, так і їх спецслужби, терористичні організації, злочинні кола, фірми і навіть особи, що діють без злого наміру. Унікальність інформаційної зброї полягає в тому, що будь-яка країна, у той час як розбудовує свою інформаційну інфраструктуру, має на мені створити певну основу для військового використання інформації як засобу ведення війни. Це обумовлено в першу чергу тим, що чим розвиненішим є науково-технічний потенціал держави, тим більша ймовірність використання інформаційної атаки в разі існування конфлікту. Цілями в такому випадку можуть бути: телекомунікації, пункти командування або управління, мобільний зв'язок, комп'ютери, системи управління в різних сферах життєдіяльності від банківської до нафтопровідної і т. д. [15].

Таким чином, підсумовуючи питання ролі інформації під час війни, можна зробити висновок що інформація у сучасному світі є важливим елементом політичної і військової боротьби з використанням при цьому різної практики та тактики її використання. В природному розумінні війна перестає бути єдиним засобом завоювання, поширення впливу та ідеології. Актуальність подальшого дослідження в тому числі обумовлено активним впливом на свідомість людей за допомогою Засобів масової комунікації (ЗМК). Перехід на віртуалізацію усіх засобів сприяє ще більшої доступності, а втім поширенням маніпулятивних технологій, які набувають поширенню їх впливу в сучасному суспільстві. Однак найголовнішою проблемою є те, що система ще не сформувала чіткі механізми забезпечення інформаційної безпеки чи механізми регулювання, що не порушують права і свободи людей, щодо отримання доступу до інформації.

РОЗДІЛ 3. КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА УМОВ ВЕДЕННЯ ВІЙНИ

3.1. Державна політика щодо забезпечення воєнно-інформаційної безпеки

Державна політика, а саме правове забезпечення воєнно-інформаційної безпеки України є актуальною не на перспективу, а на сьогодення. Ми маємо розумітися на концептуальних засадах правового забезпечення інформаційної безпеки, особливо враховуючи євроінтеграцію і військовий час, який ми маємо момент листопада 2022 року.

Законодавство – основа, на яке має спиратись в тому числі державна політика. Таким чином систематизація інформаційного законодавства потребує створення комплексної галузі інформаційного права, формування положень, котрі забезпечать відповідні норми законів та підзаконних нормативно-правових актів. Розробка та вдосконалення українського законодавства з безпекових питань інформаційної сфери мають відбуватись на готовому теоретичному підгрунті.

Зазначимо, що на сьогоднішній день рівень захищеності прав і інтересів людини, суспільства і держави в воєнно-інформаційній сфері недостатній для правового регулювання й забезпечення інформаційної безпеки. Так є випадки порушення чи обмеження прав та інтересів. В той час як в нормах існує багато суперечностей, лакун і колізій, а деякі відносини взагалі не врегульовані. Можна спостерігати розбіжності між системами права і законотворчості, усунення якої потребує системного підходу до відповідної законотворчості. Тільки такий підхід може бути головним методологічним інструментом забезпечення інформаційної безпеки. Тобто таким чином ми бачимо значні прогалини з теперішньому законодавстві, де не вистачає самого базового, як

терміни «інформаційна безпека», хоча само сполучення вживається в деяких законах.

Однією із складових інформаційної безпеки є комплексний захист прав і інтересів від непередбачуваного й шкідливого впливу. Іншими словами, головною ознакою стану захищеності в інформаційній сфері є оптимальне співвідношення інтересів людини, суспільства й держави.

Хорошими показниками забезпечення воєнно-інформаційної безпеки держави є гарантування:

1. Безпека інформації загального доступу, мереж зв'язку, інформаційно-телекомунікаційних систем; доступу до інформації. В останні місяці Україна як ніколи постраждала саме в сферах критичної інфраструктури, і держава, працюючи на останній засобах успішно вистояла випробування на темряву. Однак, якщо дивитись на подібну ситуації через перспективу, то слід актуальний стан мереж зв'язку та інформаційно-телекомунікаційних систем, адже при черговому вимкненні світла людина втрачає можливість робити базову для нашого суспільства річ – дзвонити;
2. Конфіденційності інформації з обмеженим доступом;
3. Захищеність особи, суспільства й держави від шкідливого впливу певних видів інформації. Мається на увазі про види інформації котрі здатні зашкодили вказаним суб'єктам інформаційних відносин[65].

На протязі останніх восьми років РФ веде гібридну агресію багато покладаючись саме в інформаційну складову, вбачаючи, що таким чином вона зможе безболісно окупувати не лише Крим і Донбас, а й всю територію України. В таких умовах особливої актуальності набуває протидія розповсюдження шкідливої для людини інформації, просоченою ненавистю і злобою, яку впевнено можна вважати інформаційною зброєю. Друге – про що слід зауважити це розвиток відповідного законодавства. Негативний

інформаційно-психологічний вплив, а саме це вплив на особу чи групу, який здійснюється безпосередньо на їх психічне становище, чи всупереч їхній волі застосовуючи спеціальні засоби і методи.

Під негативним інформаційно-психологічним впливом ми розуміємо вплив, неважливо, на людину або групу людей, що відбувається на її психологічний стан зазвичай без згоди, за допомогою окремих засобі і методів. В свою чергу це призводить до наслідків шкідливих не лише для особистості, а й суспільства та держави загалом.

Національна безпека України повною мірою відчула глибину постійних, цілеспрямованих впливів з боку РФ під час анексії Криму, воєнних дій на Сході і в подальшому на окупованих територіях після 24 лютого 2022 року. Фактично перше що роблять росіяни окуповуючи більш-менш ціле місце – вмикають своє телебачення, радіо, вішають пропагандистську рекламу по всьому місту. Роблять все, для того щось підсадити українців на наркотичну іглу їх ЗМІ.

Національний інформаційний простір – відкритий, що створює реальну загрозу інформаційного та психологічного впливу на суспільну свідомість населення. Таким чином, без дією ми створюємо соціальну небезпеку. Причому слід зауважити, що українське все ще різниться за ставленням до таких цінностей як демократія, незалежність, ринок землі тощо. Розбіжності можуть виступати джерелом внутрішніх загроз, коли існує низка міжрегіональних, міжетнічних, міжконфесійних суперечностей. Поки що рано говорити про повну єдність інформаційного простору та про спільні цінності, однак саме повномасштабне вторгнення Росії, 24 лютого, внесло свої корективи і за дуже короткий проміжок часу змінило ставлення українців до росіян, і навпаки [59, с. 96].

Досліджуючи державну політику у безпековій сфері, варто розглянути наступні аспекти:

- розробка й реалізація комплексних заходів щодо запобіганню, нейтралізації й попередження негативних впливів на суспільство й державу;
- підготовка суспільства до активної інформаційної протидії;
- масштабування інформаційного поля, розширення національного на світовий;
- вдосконалення системи масової комунікації;
- планування й формування системи щодо підготовки кадрів протидії в інформаційно-психологічній сфері;
- консолідація суспільства й пошук і усвідомлення усіма верствами населення нової соціальної ідентичності [65].

На сучасному етапі розвитку інформаційна політика має вирішувати завдання щодо збалансованого забезпечення інформаційної безпеки «тиради» з миттєвим визначенням нагальних пріоритетів. А саме: створення основних позицій захисту національної безпеки (в інформаційній сфері), формування ефективної інформаційної безпеки держави, виявлення інформаційних викликів, усунення загроз із визначенням можливих наслідків.

Підґрунтям державної інформаційної політики виступають:

1) Гарантія права людина на отримання достовірної, повної та своєчасної інформації, забезпечення свободи слова. Забезпечення діяльності інформації, гарантія не втручання у внутрішню організацію інформаційних процесів, окрім передбачених у законодавстві;
2) підтримка та вдосконалення національного інформаційного продукту. Підтримка Українських технологій, культурних проєктів, а тобто забезпечення підтримкою культурних цінностей, їх поширення і захист;
3) забезпечення інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі;
4) державна підтримка та розвиток ресурсів науково-технічної продукції та інформаційних технологій [4, с. 30].

Таким чином, державна політика має спрямовуватись на реалізацію системних запобігаючих заходів із наданням певних гарантій захисту життєво важливих інтересах «тріади» та по можливості унеможливлювати внутрішні та зовнішні, потенційні та реальні загрози національної безпеки України [68, с. 68].

У сфері забезпечення інформаційної безпеки державна політика виступає як:

1. В першу чергу як захист життєво важливих інтересів від внутрішніх і зовнішніх загроз. Враховуючи ситуацію, це напрям концентрується на протидії загрозам у військово-політичних цілях.
2. Захист суверенітету, політично-соціальна підтримка стабільності, територіальної цілісності України. Забезпечення постійного вдосконалення існуючої системи інформаційної безпеки Збройних Сил, військових формувань та інших інститутів, що включають в себе й сили інформаційного протиборства.
3. Захист критичної інформаційної інфраструктури. Підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування.
4. Постійний розвиток інформаційно-комунікаційних технологій. Підтримка сучасного та швидкого розвитку системи забезпечення інформаційної безпеки, а саме галузі інформаційних технологій;
5. Забезпечення участі України в міжнародній системі безпеки. Роль держави у формуванні міжнародної системи інформаційної безпеки на різних рівнях: від двостороннього до глобального.

3.2. Механізми воєнно-інформаційної безпеки в умовах війни

На початку XXI ст. Україна стала об'єктом гібридної війни зі сторони Росії, яка анексувала полу-острів Крим і частину Донецької та Луганської області перетворила на «бананові республіки» фінансуючи їх існування на протязі останніх восьми років.

Насправді, незважаючи на численні дослідження щодо інформаційної безпеки ситуація з інформацією, а скоріше з *інформуванням* на Сході майже в критичному стані. Однак при цьому Україна останній час зробила важливі кроки щодо регулювання.

24 лютого 2022 року Верховною радою України було введено воєнний стан через пряме повномасштабне вторгнення Росії на територію України. Президентом України було підписано Указ «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [67]. З закону було зрозуміло про створення «…в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації - цілодобовому інформаційному марафоні» [67].

За останні роки України зробила ряд важливих рішень щодо регулювання інформаційної безпеки на нормативно-правовому рівні. Зокрема, мова йдеться про Стратегію інформаційної безпеки, метою якої є посилення спроможності щодо забезпечення інформаційної безпеки держави, її інформаційного простору, інформаційними засобами підтримка задля соціал-політичної стабільності, оборони, захисту державного суверенітету тощо.

Сьогодні сучасна зброя – не обов'язково вогнева потужність, ефективність сучасної зброї все більше визначається ступенем інформаційної

забезпеченості. Сьогодні на полі боя все частіше почали використовувати сучасні технології, такі як дрони, адже переваги в ступені інформованості – неодмінна умова перемоги в повітряному, морському та сухопутному бою. Ми вже можемо це спостерігати своїми очима.

Однією із найважливіших функції держави – безпека, в тому числі інформаційна, яка повинна передбачати формування відповідними державними органами політики організаційно-правових механізмів в галузі інформаційної безпеки. Роль в даному напрямі належить державним органам, які відповідно до наданих повноважень в сферах своєї відповідальності повинні здійснювати організаційне, нормативно-правове, матеріально-технічне та фінансове забезпечення реалізації державної політики інформаційної безпеки [70].

Задля ефективного та контрольованого забезпечення військової безпеки необхідно функціонування за єдиним сценарієм системи військової безпеки, що виражається в ефективній діяльності трьох компонентів: управлінського, силового та забезпечувального. Система забезпечення безпеки має реагувати на загрози та виклики, але при цьому повинна розумітися на передбаченні можливих загроз. Чинником вимог до системи забезпечення військової безпеки є поєднання централізованого та децентралізованого управління засобами забезпечення інформаційної безпеки.

Механізм забезпечення інформаційної безпеки є невід'ємною складовою в процесі реалізації національної безпеки. Ключові напрямки, які має виконувати механізм забезпечення інформаційної безпеки варто відзначити наступні:

- виявлення внутрішніх та зовнішніх загроз інформаційній безпеці держави;
- визначення індикаторів інформаційної безпеки та їх порівняння нормативними показниками;

- формування та реалізація системи моніторингу, яка включає: спостереження, збір, обробку, збереження та аналіз інформації щодо стану інформаційної безпеки держави;
- розробка заходів, спрямованих на забезпечення стабільності інформаційної безпеки держави [9].

Механізм забезпечення інформаційної безпеки складається з:

1. Мета забезпечення інформаційно безпеки;
2. Відповідно до мети складаються завдання (розробка, формування, відновлення тощо);
3. Інструменти (правові, організаційно-технічні, економічні);
4. Заходи (виявлення, нейтралізація, запобігання);
5. Внутрішні та зовнішні загрози.

В умовах озброєного конфлікту або війни, коли країни стає об’єктом агресії і підпадає під значний удар, зокрема під низку інформаційних загроз. В свою чергу, ліквідація подібних викликів вимагає вжити певних організаційно-правових заходів. Стратегічна ціль у забезпеченні воєнно-інформаційної безпеки як частини національної безпеки обумовлена національними інтересами України до яких можна віднести збереження конституційного устрою, підтримка національної злагоді та єдність правового простору.

Напрямки вдосконалення системи забезпечення інформаційної безпеки:

- стратегічне стримування та ліквідація військових конфліктів, що можуть виникнути в результаті застосування інформаційних технологій;
- вдосконалення системи забезпечення інформаційної безпеки, включаючи в себе сили та засоби інформаційної протидії;
- прогнозування, виявлення та оцінка інформаційних загроз, включаючи загрози Збройним Силам України в інформаційній сфері.

Досліджуючи тему забезпечення інформаційної безпеки можна сказати з впевненістю, що державі і Збройним Силам України не слід ігнорувати існуючу загрозу не тільки ядерної бомб, а й інформаційного удару, в найбільш неочікуване місце. Тобто сьогодні інформаційна зброя є достатньо потужним засобом ведення війни, оскільки її технічна інноваційність, спроможність наприклад залишити велике місто без світла або тепла. Фактично, вони вже застосовують сучасні носії ракет, які здатні змінювати направлення, через інформаційні механізми. Незважаючи на високі показники ЗСУ по кількості збитих ракет ми маємо усвідомлювати, що їх технічна потужність є дуже небезпечною для нас. Отже, враховуючи це інформаційна безпека України має ґрунтуватись на скоординованих діях державних інститутах та структур громадянського суспільства.

Інформаційна війна між Росією та Україною триває вже більше 8 років, а можливо значно більше. Визначити точну дату початку інформаційно-пропагандистських наративів по відношенню до України доволі складно. Однак враховуючи довгі стосунки з російськими пропагандистами Україна вже розробила певні механізми реагування на інформаційні потоки з федеральних каналів.

Українське суспільство зацікавлене в самостійному створенні державних захисних механізмів, які б сприяли формуванню об’єктивного погляду для іноземців на події в Україні.

Аналізуючи механізми протидії інформаційному впливу до 24 лютого можна сказати що ми були занадто слабкі, в нас не було таких ресурсів як у Росії, але втім офіційні лиця, медіа намагались побудувати позитивний бренд про Україну. Після 24 світ побачив нову реальність, коли події виходять за рамки людяності. Українська риторика значно змінилась, Президент України Володимир Зеленський став справжнім світовим лідером, після промов якого зал аплодує стоячи.

Першочергове завдання держави – забезпечити її безпеку, в тому числі забезпечення захисту інформації, яка є гарантією національної безпеки. Цивілізація вже набула такого розвитку, коли інформація стала повноцінним ресурсом. Забезпечення інформаційної політики сьогодні, це час це не менш важливо ніж напрямок державної політики [6].

Незважаючи на активність бойових дій, на певну невизначеність в суспільстві, держава як інститут має постійно оновлювати, аналізувати та спостерігати за реалізацією та захистом національних інтересів в інформаційній сфері. Основними напрямками діяльності можуть виступами:

- розробка та прийняття довгострокової програми із забезпечення виходу на рівень провідних країн світу в галузі створення систем інформатизації та управління, що ґрунтуються на новітніх інформаційних технологіях;
- забезпечення свободи отримання та розповсюдження інформації громадянами, іншими суб’єктами суспільних відносин;
- забезпечення надійного захисту інформаційного потенціалу України від неправомірного його використання;
- організація ефективної системи підготовки та перепідготовки кадрів в галузі забезпечення інформаційної безпеки;
- розвиток взаємодії державних та комерційних систем інформаційного забезпечення з метою більш ефективного використання інформаційних ресурсів держави. [66].

3.3. Стратегія та перспективи в забезпеченні воєнно-інформаційної безпеки під час активних бойових дій та післявоєнного врегулювання.

На протязі усього дослідження ми розглядали інформаційну безпеку як складову частину національної безпеки, як окрему одиницю тощо. Захищаючи свої національні інтереси, кожна держава має дбати про свою інформаційну

безпеку. Інформаційне суспільство мабуть одне із найбільш швидко розвиваючих сфер людської життєдіяльності на сьогоднішній день. То, що ще вчора було на передовій технологічного забезпечення – завтра вже не актуально. Швидка зміна орієнтирів, поява нових технологій, що загрожують як окремій особистості, так і державі створює умови постійного аналізу і переоцінки існуючих стратегій та перспектив.

Останній Указ Президента України Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"[66]. Стратегія комплексно описує план щодо інформаційної безпеки до 2025 року.

Згідно з Указом – «Стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних»[66].

Однак на нашу думку, слід звернути увагу на деякі визначення, які чітко прописані в стратегії і грають ключову роль в забезпечення інформаційної безпеки під час активних бойових дій:

1) «Інформаційні заходи оборони держави - сукупність скоординованих дій, які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України в мирний час, в особливий період, в умовах воєнного або надзвичайного стану щодо прогнозування та виявлення інформаційних загроз у воєнній сфері, запобігання, стримування та відсічі збройній агресії проти України, протидії інформаційним загрозам з боку держави-агресора, а також здійснення інших необхідних дій в інформаційному протиборстві[66]»;
2) «Стратегічний наратив - спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію»[66];

3) «Урядові комунікації - комплекс заходів, що передбачають діалог уповноважених представників Кабінету Міністрів України з цільовою аудиторією з метою роз'яснення урядової позиції та/або політики з певних проблемних питань»[66].

Починаючи з термінів в стратегії відчувається підготовка к загостренню конфлікту і відповідне планування діалогу з громадянами і світовими лідерами. Додамо, що поняття інформаційні заходи оборони держави вже само говорить за себе, це відкрите натякання на неминуче загострення.

Згідно зі стратегією тривалий час спеціальні служби Росії проводять «спеціальні інформаційні операції, більшість із яких спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності» [66]. В свою чергу подібні інформаційні компанії призводять до панічних настроїв у суспільства, дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні.

У зв’язку з тимчасовою окупацією у 2014 році частини території Росія захопила розташовані на цій території об'єкти інформаційної інфраструктури, зокрема й об'єкти Концерну радіомовлення, радіозв'язку та телебачення. На окупованих територіях застосовуються методи тотального придушення свободи слова, контролю над редакційною політикою засобів масової інформації та інших інформаційних ресурсів.

Згідно з актуальною стратегією основними напрямками реалізації інформаційної безпеки є забезпечення стійкосте та взаємодії задля досягнення якої існують наступні стратегічні цілі та завдання.

Стратегічна ціль 1 пов’язана з протидією дезінформації та інформаційним операціям, а саме державі-агресору, зо спрямований на знищення Української незалежності, позбавленням конституції, порушення суверенітету та територіальної цілісності держави.

Стратегічна ціль 2. Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності.

Стратегічна ціль 3. Підвищення рівня медіакультури та медіаграмотності суспільства. Українське суспільство повинне бути захищене від деструктивного впливу дезінформації та маніпулятивної інформації, а медіасередовище - бути соціально відповідальним і функціонувати стабільно.

Стратегічна ціль 4. Дотримання прав на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації

Стратегічна ціль 5. Для перспективності стратегія передбачає роботу з тимчасово окупованими територіями, а саме інформаційна реінтеграція громадян України, що тимчасово окуповані Росією. Відповідно відновлення інформаційного простору України і забезпечення права на інформацію кожну особу.

Стратегічна ціль 6. Створення ефективної системи стратегічних комунікацій. Основною метою створення та розвитку системи стратегічних комунікацій є гарантування ефективної інформаційної взаємодії та діалогу між різними інститутами і групами громадянського суспільства з питань, що стосуються кризових ситуацій

Стратегічна ціль 7 передбачає загальний розвиток інформаційного суспільства та підвищення рівня культури діалогу.

Аналізуючи стратегічні цілі можна впевнено сказати, що вони розраховані в перспективному ключі і будуть тримати актуальності ще довго, бо мають комплексний характер і окреслюють майже всі найголовніші проблеми інформаційного характеру на сьогоднішній день.

Механізми реалізації відповідно до мети та завдань розподілені на зони відповідальності, що робить стратегії більш досяжними і візуальними адже

кожне профільне міністерство відповідає лише за свої функціональні завдання.

В стратегії неодноразово підкреслено щодо забезпечення громадянами України підтримки відновлення територіальної цілісності України, розуміння політики України щодо звільнення тимчасово окупованих територій. Таким чином, ми можемо прослідкувати, що стратегія має характер не лише реагування за загострення конфлікту, а й на післявоєнне відновлення, що в свою чергу вкотре доказує чітку позицію уряду щодо наших основних умов і прагнень – повне звільнення усіх тимчасово окупованих територій.

Відповідно до Стратегії є чітко сформовані результати:

1. Інформаційний простір України – захищений: розроблені усі основні механізми забезпечення від законодавчого до технологічного, в разі інформаційної атаки максимальна готовність реагування та стабільне функціонування усіх основних систем;
2. Система стратегічних комунікацій налагоджена та ефективно працює, кожна ланка в державі розуміється на процесах, миттєво реагує на інформування;
3. Протидія поширенню незаконного контенту. Прописаний нормативно-правовий механізм протидії розповсюдження нелегального контенту, освітньо-інформаційні заходи інформаційної гігієни поширені на широкі кола, суспільство діє інформаційно свідомо;
4. Процес реінтеграції громадян України на тимчасово окупованих територіях забезпечений, а саме налагодження мобільного зв’язку, відновлення вишок телекомунікації, відбудова електропостачання в постраждалі від бойових дій регіони. Постійна робота над психологічною реінтеграцією суспільства, що постраждало в наслідок тривалої окупації, а відповідно і тривалого інформаційно-пропагандистського впливу;

5. Покращений рівень медіакультури та медіаграмотності серед населення, поява ще більшої кількості незалежних ЗМІ, відсутність монополії на інформацію;
6. Забезпечення конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя;
7. Забезпечення захисту прав журналістів, відсутність переслідувань, покарань та обмежень на висловлювання думки незалежних журналістів. Створення міжнародної довіри до українських медіа-каналів;
8. Повноцінне формування української громадянської ідентичності. Незважаючи на тривалі інформаційні впливи саме на ідентичність українського народу, самоідентифікація, розуміння власного місця в світі, власної історії і прикладу. Захист ідентичності на усіх рівнях суспільних відносин.

Деякі з зазначених цінностей є доволі амбітними і складно досяжні, однак, якщо розглядати перспективу післявоєнного відновлення то стратегія не втратить свою актуальність, а навпаки тільки розкриє весь свій потенціал.

На сьогоднішній день інформаційна агресія і відчуття постійної загрози стали нашим повсякденням і жодна людина не почуває себе в безпеці в цьому відношенні. Про-активні громадяни, а особливо ті, хто перебуває на умовній «передовій» інформаційного протистояння повинні усвідомлювати можливі ризики, бути здатним протистояти інформаційним загрозам і впливам.

Інформаційні війни не менш руйнівні, порівняно з тими де застосовується танки чи артилерія. Насправді, інформаційний вплив може мати ще більш катастрофічні наслідки не тільки для окремої особистості, а й для всього суспільства. Повертаючись до стратегії – ми бачимо, як уряд виділяє роботу з людьми постраждалим від тривалої окупації, і відповідно від постійного інформаційного впливу. Бо відбувається руйнування суспільної

психології, викривлення інтелектуальних і ціннісних орієнтирів. Тому, коли мова йдеться про інтеграцію громадян з окупованих територій має бути продумана системна робота, розрахована на довгий і поступовий результат.

На сьогоднішній день, коли ми живемо в часі постійних змін, прогнозувати доволі важко. Однак головним показником успішності стратегії це її адаптивність до сучасних реалій. Адаптивність в сучасному світі – це засіб виживання, бо тільки таким чином можна досягнути зазначених цілей.

ВИСНОВКИ

Інформаційне суспільство поставило перед людством багато викликів, Україна стала вимушеним епіцентром ідеологічного протистояння, потерпаючи від збройної агресії РФ. Враховуючи це було прийняте рішення провести аналіз існуючого стану воєнно-інформаційної безпеки України, для розуміння системних недоліків в забезпечення інформаційної безпеки України під час кризисного реагування.

Головною метою магістерської роботи було дослідити вплив воєнно-інформаційної безпеки, її роль в забезпеченні миру та гарантій безпеки. Вплив воєнно-інформаційної безпеки складно недооцінити і переоцінити, адже Україна знаходиться в стані військового положення і до цього роками була готова до ескалації конфлікту на Сході України в будь-який момент.

Відповідно до поставлених завдань були досягнені наступні результати. *Теоретико-понятійний аналіз явища* інформаційна безпека як предмету дослідження пройшов успішно. Було проаналізовано відмінність в підходах вивчення інформаційної безпеки, відмінність в категоріях явища. Поняття «інформаційна безпека» є складною конструкцією, що зумовлюється комплексною соціально-правовою природою, завдяки різноманітті інформаційних відносин в суспільстві; відмінністю суб’єктів інформаційних відносин з власними інтересами, правами та обов’язками залежно від галузі використання термін може бути інтерпретований по різному, але з незначними відмінностями.

Були досліджені *методологічні засади* поняття інформаційної безпеки. Особливу увагу приділили дослідженню інформаційної безпеки через нормативно-правову призму, основні закони, їх стан і актуальність на сьогоднішній день. В цілому виявлено, що проблематика інформаційної безпеки тісно пов’язана з дослідженням феноменів інформаційного

суспільства, стану інформаційного простору, розумінні інформації як токової та в контексті національної безпеки держави.

Зарубіжний досвід забезпечення інформаційної безпеки був досліджений в контексті перспективи набуття Україною членства в Альянсі і Європейському Союзі. Таким чином, можна сказати що з метою набуття членства Україна активізує зусилля реформ, в безпековому та оборонному секторах зокрема. Розуміючи ситуацію в світі, інформаційна безпека стає одним із найважливіших аспектах забезпечення національної та міжнародної безпеки в цілому.

Проблематика воєнно-інформаційної безпеки в Україні полягає в розбіжності між системами права і законотворчості, усунення якої потребує системного підходу до відповідної законотворчості. Таким чином ми бачимо значні прогалини з теперішньому законодавстві, де не вистачає самого базового, як терміни «інформаційна безпека», хоча само сполучення вживається в деяких законах.

Роль інформації у сучасному світі є важливим елементом політичної і військової боротьби з застосуванням при цьому різної практики та тактики її використання. В природному розумінні війна перестає бути єдиним засобом завоювання, поширення впливу та ідеології.

Дослідження державної політики має спрямовуватись на реалізацію системних запобігаючих заходів із наданням певних гарантій захисту життєво важливих інтересах особистості, суспільства та держави по можливості унеможливлювати внутрішні та зовнішні, потенційні та реальні загрози національної безпеки України.

Механізми воєнно-інформаційної безпеки за умов війни є невід'ємною складовою в процесі реалізації національної безпеки. Першочергове завдання держави – забезпечити її безпеку, в тому числі забезпечення захисту інформації, яка є гарантією національної безпеки.

Вдалось проаналізувати стратегію та перспективи в забезпеченні воєнно-інформаційної безпеки. Згідно з актуальною стратегією основними напрямками забезпечення інформаційної безпеки України є стійкість та взаємодія.

Підсумовуючи магістерську роботу на тему «Воєнно-інформаційна безпека України за умов ескалації конфлікту на Сході України» можна зробити висновок, що незважаючи на складність теми, усі поставлені завдання бути реалізовані й покрити. Дослідження не втрачає своєї актуальності і тема може бути розкрита ще більше.

СПИСОК ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: дис. … канд. з державного управління: спец.: 25.00.02. Київ, 2017. 218 с.
2. Банах С. Поняття та особливості інформації як теоретичної категорії / С. Банах. Актуальні проблеми правознавства, 2019. №4, с. 226
3. Брижко В. М. До гносеології категорії «інформація». Інформація і право. 2011. № 2 (2). С. 13–20.
4. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. Актуальні проблеми післякризового відновлення економіки України: зб. матер. наук.-практ. конф. Львів. 2013. С.29-32
5. Валюшко І. О. Еволюція інформаційних війн: минуле і сучасність / І. О Валюшко [Електронний ресурс]. — Режим доступу: https://ir.kneu.edu.ua/bitstream/handle/2010/17471/127-134.pdf?sequence=1&isAllowed=y
6. Гбур З. В. Основи інформаційної безпеки держави в умовах війни / З. В. Гбур – Київ, с. 868 – 872.
7. Гізун А. І. Аналіз сучасних теорій інформаційно-психологічних впливів в аспекті інформаційного протиборства / А. І. Гізун, В. С. Гріга // Безпека інформації. - 2016. - 22, № 3. - С. 272-282. - Бібліогр.: 16 назв. - укр.
8. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення / Ю. О. Горбань // Вісн. Нац. акад. держ. упр. при Президентові України. - 2015. - № 1. - С. 136-141. - Бібліогр.: 17 назв. - укр.
9. Гончаренко О., Джангужин Р., Лисицин Е. Громадянський контроль і система національної безпеки. Національна без- пека України. 2003. № 1. С. 39–46.
10. Гурковський В. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дисертація на здобуття наукового ступеня кандидата юридичних наук

(спеціальність: 25.00.02 – механізми державного управління). Київ. 2004. 225 с.

11. Гнатюк С.Л. Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти: Аналітична доповідь. К. : Нац. ін-т стратегічних досліджень, 2013. 51 с.
12. Гуцу С. Ф. Правові основи інформаційної діяльності: Навч. посібник Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін. -т», 2009. 48 с
13. Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року. URL: http://zakon2.rada.gov.ua/laws/show/994_242 (дата звернення: 28.11.2022).
14. Деокупація і реінтеграція інформаційного простору Криму: міжнародноправові та медіакомунікативні інструменти: матеріали міжнародної науковопрактичної конференції. м. Київ: 18 квітня 2019 року. Київ. 2019. С. 17–22.
15. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. О.Д. Довгань. “Інформація і право” № 1(24)/2018
16. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: моногр. К.: НІСД, 2014. 328 с.
17. Закон України «Про інформацію» від 02 жовтня 1992 р..Відомості Верховної Ради України (ВВР). – 1992. – № 48. – С. 650
18. Закон України «Про Національну програму інформатизації» від 04.02.1998 р. № 74/ Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.181
19. Закон України «Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України» від 08.06.2017 року.
20. Забара І.М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. Теорія і практика правознавства. 2013. Вип. 2

21. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири. / К. В. Захаренко. Київ. 2021.с.423
22. Конституція України : Закон України від 08.06.1996 р. № 254к/96-ВР / Відомості Верховної Ради України. 1996. № 30. Ст. 141.
23. Кісілевич-Чорнойван О. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять // Юриспруденція: теорія і практика. 2009. № 8. С. 11–18.
24. Коваль З. Політико-правові механізми державного управління інформаційно-психологічною безпекою України: автореф. дис. ... канд. н. з держ. упр. (спеціальність: 25.00.02 – механізми державного управління). Одеса. 2011. 22 с.
25. Косогов О. М. Підхід до побудови державної системи протидії інформаційним загрозам в особливий період / О. М. Косогов // Зб. наук. пр. Харків. ун-ту Повітр. сил. - 2015. - Вип. 4. - С. 40-43. - Бібліогр.: 5 назв. - укр.
26. Косогов О. М. Методологічний підхід до аналізу загроз інформаційній безпеці держави у воєнній сфері та визначенню заходів протидії їм / О. М. Косогов // Наука і техніка Повітр. сил Збройн. сил України. - 2015. - № 3. - С. 51-53. - Бібліогр.: 4 назв. - укр.
27. Комаров В. С. Методичний підхід до обгрунтування раціонального складу органів військового управління / В. С. Комаров, О. М. Косогов, В. Ф. Курдюк // Зб. наук. пр. Харків. ун-ту Повітр. сил. - 2017. - Вип. 2. - С. 40-45. - Бібліогр.: 10 назв. - укр.
28. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. - 286 с.
29. Кобільник Б.Ю., Гізун А.І. Роль інформаційно-психологічних впливів у інформаційній війні / Кобільник Б.Ю., Гізун А.І. – Кропивницький: Матеріал Всеукраїнської науково-практичної конференції, 2016. – 28с.

30. Копійка М. Інституціональний концепт інформаційної безпеки України
31. 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. Вип. 3. С. 220-237
32. Левченко О. В. Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел / О. В. Левченко, О. М. Косогов // Системи оброб. інформації. - 2016. - Вип. 1. - С. 100-102. - Бібліогр.: 15 назв. - укр.
33. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навч. посібник. Київ: КНТ, 2006. 280 с.
34. Ліпкан В.А. Національна безпека України: навч. посіб. К.: КНТ, 2009. 576 с
35. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів.
36. Магда Є.В. Гібридна війна: вижити і перемогти. Х.: Віват, 2015. 304с
37. Макарова М.В. Електронна комерція : Посіб. К.: Видавничий центр “Академия”, 2002. 272 с.
38. Марунченко О. П. Інформаційна війна у сучасному політичному просторі : автореф. дис. ... канд. політ. наук : 23.00.02 / О. П. Марунченко; ДЗ "Південноукр. нац. пед. ун-т ім. К.Д. Ушинського". - О., 2013. - 17 с. - укр.
39. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. Збірник наукових праць: «Ефективність державного управління». Випуск 32. 2012. С.20-27
40. Медведєв В. К. Сучасна інформаційна війна та її обрис / В. К. Медведєв, Ю. Ф. Кучеренко, О. М. Гузько // Системи озброєння і військ. техніка. - 2008. - Вип. 1. - С. 52-54. - Бібліогр.: 2 назв. - укр.

41. Мельник С.В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. Інформаційні технології і засоби навчання. 2016. Т. 55. №5. С. 187–197.
42. Миронюк Д. І. Кримська війна (2014 р.): військова та інформаційна / Д. І. Миронюк // Держава та регіони. Сер. Соц. комунікації. - 2015. - Вип. 4. - С. 31-35. - Бібліогр.: 6 назв. - укр.
43. Мірошниченко П. В. Суспільна значущість лідера думок під час інформаційного протистояння / П. В. Мірошниченко, А. А. Нестеренко // Держава та регіони. Сер. Соц. комунікації. - 2015. - Вип. 4. - С. 36-41. - Бібліогр.: 18 назв. - укр.
44. Міжнародна інформаційна безпека: Сучасні виклики та загрози / Макаренко Є.А., Рижиков М.М. та ін. Київ: Центр вільної преси, 2006. 916 с.
45. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17-23.
46. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання. Київ: Видавничий дім «Гельветика», 2017. 168 с
47. Олійник О. Адміністративно-правові засади інформаційної безпеки // Європейські перспективи. 2012. № 4 (1). С. 65–68.
48. Олійник О. В. Державна політика інформаційної безпеки України. Юридичний вісник. 2012. №4(25). С.65-69
49. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9.01.2007 р. № 537–V. ВВР України. 2007. № 12. Ст. 102.
50. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.2006 р. № 373. Офіційний вісник України. 2006. № 13.

51. Партнерство заради миру: Рамковий документ, підписаний Україною 8 лютого 1994 року (набув чинності для України 8 лютого 1994 року). Офіційний вісник України. 2006. № 48. Ст. 3232

52. Погребняк А.В. Технології комп'ютерної безпеки: Моногр. Рівне: МЕГУ, 2011. 117 с.

53. Пояркова Т. К. Військове протистояння України з Росією (2014 - 2015) у світлі різних типологій сучасних війн / Т. К. Пояркова // Прикарпат. вісн. НТШ. Сер. Думка. - 2015. - № 3. - С. 9-17. - Бібліогр.: 12 назв. - укр.

54. Петров В. В. Воєнно-інформаційна безпека України за умов посилення загроз інформаційних війн : автореф. дис. ... канд. політ. наук : 21.01.01 / В. В. Петров; Рада нац. безпеки і оборони України, Нац. ін-т пробл. міжнар. безпеки. - К., 2010. - 19 с. - укр.

55. Пода Т. А. Інформаційна війна як стратегія формування політичної свідомості (соціально-філософський аналіз) / Т. А. Пода // Вісн. Нац. авіац. ун-ту. - 2014. - № 1. - С. 67-70. - Бібліогр.: 6 назв. - укр.

56. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 43, том 1. 2017. С.34- 39

57. Про основи національної безпеки України : Закон України : від 19.06.2003 р. № 964-IV. ВВР України. 2003. № 39.

58. Размєтаєва Ю.С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 37, том 1. 2016. С.43-46

59. Структура керівних документів державної політики в інформаційній сфері: нагальні проблеми та шляхи впорядкування. URL: http://www.niss.gov.ua/articles/572/ .

60. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро -

2012 / О. Саприкін // Вісн. Кн. палати. - 2013. - № 1. - С. 40-43. - Бібліогр.: 13 назв. - укр.

61. Сенченко М. Інформаційна війна: методи впливу інформаційної зброї / М. Сенченко // Вісн. Кн. палати. - 2006. - № 12. - С. 3-8. - укр.
62. Семен Н. Ф. Поняття "інформаційна війна" в контексті соціальних комунікацій / Н. Ф. Семен // Держава та регіони. Сер. Соц. комунікації. - 2016. - Вип. 1. - С. 22-25. - Бібліогр.: 20 назв. - укр.
63. Трач О. Р. Визначення показника стійкості віртуальної спільноти щодо інформаційних атак / О. Р. Трач, С. С. Федушко // Безпека інформації. - 2016. - 22, № 1. - С. 84-87. - Бібліогр.: 19 назв. - укр.
64. Триняк В. Інформаційна безпека як соціокультурний феномен (соціальнофілософський аналіз): автореф. дис. ...канд. філос. н. (спеціальність: 09.00.03 – соціальна філософія та філософія історії). Дніпропетровськ. 2009. 24 с.
65. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України / Т.Ю. Ткачук – ДВНЗ «Ужгородський національний університет», Ужгород, 2019.
66. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"» - 2021. – № 685/2021.
67. Указ Президента «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» від 24 лютого 2022. №64/2022
68. Фань Ч. Правове забезпечення інформаційної безпеки в системі сучасної міжнародної співпраці // Наукові праці МАУП. 2012. Вип. 4 (35). С. 110–115.
69. Цимбалюк В. С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. Адміністративне право і процес. 2014. № 2 (8).

70. Шипілова Л. М. Порівняльний аналіз ключових понять і категорій основ національної безпеки України: автореф. дис. … к. політ. н.: 21.01.01. Київ, 2007. 20 с.
71. Штанько В. І. Проблеми адаптації особистості в умовах створення інформаційного суспільства : [монографія] / В. І. Штанько, Л. А. Тіхонова, Н. В. Чорна, Т. Г. Авксентьєва, Я. М. Кунденко, В. В. Омельченко, Н. М. Дашенкова, О. О. Українська, І. С. Красинська; Харк. нац. ун-т радіоелектрон. - Х. : Компанія СМІТ, 2013. - 171 с. - Бібліогр.: с. 163-169 - укр.
72. Ярош С. П. Теоретичні основи побудови та застосування розвідувально-управляючих інформаційних систем протиповітряної оборони : монографія / С. П. Ярош; ред.: І. О. Кириченко; Харк. ун-т повітр. сил ім. І. Кожедуба. - Х. : ХУПС, 2012. - 511 с. - Бібліогр.: с. 500-511 - укр.
73. Document C-V(2002)49: Security within tne North Atlantic Treaty Organization (NATO).
74. Digital 2022: Global Overview Report URL: Digital 2022: Global Overview Report — DataReportal – Global Digital Insights
75. General Assembly Resolution «The right to privacy in the digital age»
76. Hybrid Warfare URL: http://www.gao.gov/assets/100/97053.pdf