МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»
Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра міжнародних економічних відносин та туризму
Спеціальність 292 – Міжнародні економічні відносини
Очна форма навчання, 2 курс

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

«Роль міжнародних організацій у системі забезпечення міжнародної інформаційної безпеки»

2ФМ 10748280 КМР

Розробив студент гр. 601-ФМ
__.__2023 р. _____М.А. Козир
Керівник кваліфікаційної роботи
__.__.2023 р._____А.А.Буряк
Консультанти:
із глобальної економіки
__.__.2023 р._____ І.Б. Чичкало-Кондрацька
із міжнародного менеджменту
__.__.2023 р._____ Н.В. Безрукова
із міжнародних стратегій економічного розвитку
__.__.2023 р._____ А.А.Буряк

Робота допущена до захисту:

Завідувачка кафедри міжнародних економічних відносин та туризму
І.Б. Чичкало-Кондрацька (П.І.Б.)
__.__.2023 р. _____ (підпис)

Полтава 2024

РЕФЕРАТ

Козир М.А. Роль міжнародних організацій у системі забезпечення міжнародної інформаційної безпеки. Рукопис. Кваліфікаційна магістерська робота на здобуття кваліфікації магістра зі спеціальності 292 «Міжнародні економічні відносини». Національний університет «Полтавська політехніка Юрія Кондратюка», Полтава, 2024.

Кваліфікаційна магістерська робота містить 108 сторінок, 5 рисунків, список літератури з 103 найменувань, 1 додаток.

Ключові слова: міжнародні економічні відносини, міжнародна інформаційна безпека, міжнародні організації, безпекоорієнтоване інформаційне середовище, інформаційний суверенітет України.

Предметом дослідження є концепція інформаційної безпеки у сучасних міжнародних економічних відносинах.

Об’єктом дослідження виступає сфера міжнародних економічних відносин в умовах трансформації глобальної парадигми інформаційної безпеки.

Мета кваліфікаційної магістерської роботи полягає у визначенні ролі міжнародних організацій у системі забезпечення міжнародної інформаційної безпеки.

Завданнями роботи є: розглянути наукові підходи до змісту категорії «міжнародна інформаційна безпека»; систематизувати сучасні теорії міжнародної інформаційної безпеки; визначити методологічні основи дослідження безпеки інформаційного середовища у міжнародних економічних відносинах; з’ясувати роль міжнародних організацій у формуванні та реалізації стратегій міжнародної інформаційної безпеки; охарактеризувати основні напрями діяльності провідних європейських країн у сфері інформаційної безпеки; дослідити стратегічні напрями забезпечення інформаційної безпеки у США; визначити основні засади інституціонального співробітництва України у сфері інформаційної безпеки; здійснити дослідження інструментів забезпечення безпекоорієнтованого інформаційного середовища в Україні; обґрунтувати основні напрями діяльності держави у сфері забезпечення інформаційного суверенітету України.

За результатами дослідження сформульовані рекомендації щодо активізації ролі міжнародних організацій у системі забезпечення міжнародної інформаційної безпеки.

Рік виконання кваліфікаційної магістерської роботи – 2024.

ABSTRACT

Kozyr M.A. The role of international organizations in the system of ensuring international information security. Manuscript. Qualifying master's thesis for obtaining a master's qualification in specialty 292 «International Economic Relations». National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, 2024.

The qualification master's work contains 108 pages, 5 figures, a list of literature with 103 items, 1 appendix.

Keywords: international economic relations, international information security, international organizations, security-oriented information environment, information sovereignty of Ukraine.

The subject of the study is the concept of information security in modern international economic relations.

The object of the study is the sphere of international economic relations in the context of the transformation of the global paradigm of information security.

The purpose of the qualifying master's work is to determine the role of international organizations in the system of ensuring international information security.

The tasks of the work are: to consider scientific approaches to the content of the category «international information security»; systematize modern theories of international information security; to determine the methodological bases of the study of the security of the information environment in the IER; find out the role of international organizations in the formation and implementation of international information security strategies; describe the main directions of activity of the leading European countries in the field of information security; to investigate the strategic directions of ensuring information security in the USA; to determine the main principles of institutional cooperation of Ukraine in the field of information security; to carry out a study of tools for ensuring a security-oriented information environment in Ukraine; justify the main directions of the state's activity in the sphere of ensuring Ukraine's information sovereignty.

According to the results of the research, recommendations were formulated regarding the activation of the role of international organizations in the system of ensuring international information security.

The year of completion of the qualifying master's thesis is 2024.

ЗМІСТ

No table of contents entries found.

ВСТУП

Актуальність обраної теми. Обрана тема про роль міжнародних організацій у системі забезпечення міжнародної інформаційної безпеки є актуальною та важливою. Глобалізація інформаційного простору підвищує використання цифрових технологій, зосереджує увагу на важливості міжнародної співпраці у сфері інформаційної безпеки. Міжнародні організації виступають ключовими учасниками у координації зусиль країн щодо боротьби з кіберзагрозами, кібератаками та іншими формами кіберзлочинності. Міжнародні організації можуть встановлювати та сприяти у впровадженні міжнародних стандартів безпеки в інформаційній сфері, що сприяє забезпеченню більшої узгодженості між країнами. Міжнародні організації створюють механізми для обміну інформацією та досвідом у сфері кібербезпеки, що сприяє покращенню здатності країн відповідати на загрози та захищати себе. У разі кібератак або інших загроз міжнародні організації можуть виконувати роль координаторів та сприяти спільним діям країн для реагування на кризові ситуації. Таким чином, дослідження ролі міжнародних організацій у забезпеченні міжнародної інформаційної безпеки є важливим для розуміння взаємодії між державами, спільних зусиль у боротьбі з загрозами, а також для визначення найкращих практик та створення механізмів співпраці.

Актуальність дослідження інформаційної безпеки в сучасних міжнародних економічних відносинах підтримується підвищеним інтересом відомих зарубіжних та вітчизняних науковців та експертів, зокрема К.Волкера, Дж.Гарстки, Р.Кеохейна У.Кертіса,, М.Лібіцкі, Е.Міллера, Дж.Ная, О.Андрєєвої, А.Баровської, Н.Бєлоусової, С.Даниленка, Д.Дубова, С.Гнатюка, О.Гребініченка, О.Запорожець, М.Капітоненка, В.Ліпкана, О.Литвиненка,

Є.Макаренко, М.Ожевана, Г.Почепцова та ін. Постановка проблеми відображає важливість цілісного аналізу в галузі інформаційної безпеки в міжнародних економічних відносинах, особливо у контексті сучасних викликів та гібридних загроз. Трансформація парадигми глобальної інформаційної безпеки дійсно викликає значні зміни у чинниках, що впливають на формування політики інформаційної безпеки країни. Ця трансформація вимагає перегляду та оновлення інструментів забезпечення інформаційного суверенітету та захисту національних інтересів. Для України, яка переживає широкомасштабне вторгнення РФ, складні геополітичні виклики та активно долучається до міжнародних відносин, особливо важливою є адаптація та ефективне використання інформаційних інструментів для захисту своєї національної безпеки.

Мета роботи. Метою дослідження є визначення ролі міжнародних організацій у системі забезпечення міжнародної інформаційної безпеки.

Досягнення поставленої мети зумовило необхідність розв’язання таких **завдань:**

- розглянути наукові підходи до змісту категорії «міжнародна інформаційна безпека»;

- систематизувати сучасні теорії міжнародної інформаційної безпеки;

- визначити методологічні основи дослідження безпеки інформаційного середовища у міжнародних економічних відносинах;

- з’ясувати роль міжнародних організацій у формуванні та реалізації стратегій міжнародної інформаційної безпеки;

- охарактеризувати основні напрями діяльності провідних європейських країн у сфері інформаційної безпеки;

- дослідити стратегічні напрями забезпечення інформаційної безпеки у США;

- визначити основні засади інституціонального співробітництва України у сфері інформаційної безпеки;

- здійснити дослідження інструментів забезпечення безпекоорієнтованого інформаційного середовища в Україні;

- обґрунтувати основні напрями діяльності держави у сфері забезпечення інформаційного суверенітету України.

Об'єктом дослідження є сфера міжнародних економічних відносин в умовах трансформації глобальної парадигми інформаційної безпеки.

Предметом дослідження є концепція інформаційної безпеки у сучасних міжнародних економічних відносинах.

Наукова новизна дослідження полягає в узагальненні та систематизації теоретико-методологічних підходів до концепту інформаційної безпеки у міжнародному вимірі, визначенні ролі міжнародних організацій у системі забезпечення міжнародної інформаційної безпеки.

Методи дослідження. Для вирішення завдань, поставлених у роботі, були використані загальнонаукові та спеціальні методи дослідження. Зокрема, системний метод був використаний з метою дослідження теоретико-методологічних основ міжнародної інформаційної безпеки; структурно-функціональний метод – при дослідженні стратегічних засад забезпечення інформаційної безпеки учасників міжнародних економічних відносин; компаративний метод – для аналізу стратегічних напрямів забезпечення інформаційної безпеки в Україні в умовах функціонування глобального інформаційного простору.

Інформаційна база дослідження. Джерелами дослідження стали навчальні посібники, підручники, монографії, науккові статті, а також документи з інформаційної безпеки міжнародних організацій, стратегії та нормативні акти з інформаційної безпеки США, країн ЄС та України, Інтернет-ресурси.

Структура роботи. Робота складається із вступу, трьох розділів, висновків і пропозицій по темі, списку використаних джерел інформації та додатків.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Наукові підходи до змісту категорії «міжнародна інформаційна безпека»

Американські науково-дослідницькі центри та видатні економісти США є важливими учасниками у формуванні поглядів на поняття та явища в галузі інформаційної безпеки. Вони внесли значний вклад у розуміння цієї сфери та виявили потребу у детальному визначенні понять, що стосуються міжнародної інформаційної безпеки.

Трансформація парадигми міжнародної безпеки та модернізація інформаційних озброєнь супроводжуються активізацією гібридних конфліктів, що робить це поле ще більш важливим для аналізу та розуміння. Американські дослідники у цій галузі ретельно аналізують ці процеси та їх вплив на сучасну міжнародну безпеку, їхні дослідження визначають нові підходи до типології понять і категорій інформаційної безпеки, що є важливим для розвитку та вдосконалення стратегій у цій сфері. Наукові роботи [1–2] можуть бути корисними для глибшого розуміння сучасних викликів та явищ у галузі інформаційної безпеки, допомагаючи у виробленні більш адаптивних стратегій в безпековій області.

Так, в Європі були розроблені та прийняті загальні «Європейські критерії безпеки інформаційних технологій» [3]. Цей документ вперше ввів поняття «адекватності засобів захисту» і значно розширив сферу його застосування. Ці критерії враховують не лише захист інформації від несанкціонованого доступу, а й забезпечення конфіденційності та цілісності інформації, захищеність від несанкціонованої модифікації або знищення, а також підтримку працездатності систем і протидію потенційним загрозам. Ці

критерії допомагають стандартизувати та систематизувати підходи до захисту інформаційних технологій в Європі, що є важливим для забезпечення безпеки та захисту інформації на різних рівнях, включаючи захист на рівні систем та мереж.

Розвиток типології понятєвих категорій інформаційної безпеки враховував внесок як відомих зарубіжних експертів, які пропонували визначення основних понять та складових інформаційної безпеки, так і внесок вітчизняних науковців [4], які досліджували сутнісні характеристики інформаційної безпеки та інструментарій інформаційного протиборства.

Поява сучасних засобів інформаційного впливу потребує постійної систематизації та тлумачення новітніх понятєвих категорій інформаційної безпеки з урахуванням їх еволюції та інноваційності. Сьогодні у науковому дискурсі присутні як ретроспективні, що описують минуле, так і проспективні дослідження щодо визначення як власне інформаційної безпеки, так і всіх її суміжних понять. Цей підхід дозволяє враховувати зміни в сучасному інформаційному середовищі та динаміку розвитку технологій інформаційного впливу.

Так, практика міжнародного співробітництва у сфері інформаційної безпеки дійсно сприяла використанню відповідної термінології та тлумаченню основних понять, які були зафіксовані в міжнародних документах ООН та її спеціалізованих установ, регіональних організацій і в стратегіях національної безпеки провідних країн світу.

Наприклад, у Документі A/54/213 Генеральної Асамблеї ООН «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» було запропоновано для обговорення визначення поняття «інформаційна безпека». Це поняття трактувалося як «стан захищеності основних інтересів індивідуума, суспільства і держави в інформаційному просторі, включаючи інформаційно-телекомунікаційну інфраструктуру і саму інформацію щодо таких властивостей, як цілісність, об’єктивність доступності і конфіденційність». Також в цьому документі

використовувалися та обговорювалися суміжні поняття, такі як «інформаційна війна», «інформаційна зброя», «інформаційні загрози», «інформаційний тероризм», «інформаційна злочинність», «несанкціоноване втручання», «критично важлива інфраструктура», «міжнародна інформаційна безпека» та інші.

Так, поняття «міжнародна інформаційна безпека» визначалося як «стан міжнародних відносин, що виключає порушення світової стабільності і створення загрози для безпеки держав і міжнародного співтовариства в інформаційному просторі». Це визначення визначало зміст та область застосування поняття «міжнародна інформаційна безпека» в міжнародному співробітництві і при формулюванні стратегій національної та міжнародної безпеки в контексті інформаційного простору.

Протягом ряду сесій Генеральної Асамблеї ООН у період з 2007 р. по 2019 р. держави-члени висловлювали свої погляди та позиції щодо питань інформаційної безпеки. Ці сесії стали майданчиками для обговорення та обміну думками про стратегії зміцнення безпеки інформаційних та телекомунікаційних мереж як на національному, так і на міжнародному рівнях.

Зазначені сесії та дебати свідчать про те, що базові поняття міжнародної інформаційної безпеки, включаючи його визначення та способи реалізації національних та міжнародних стратегій, стали об’єктом уваги та обговорень через колізії та неоднозначності у міжнародних відносинах. Це спонукало держави-учасниці до активного обговорення питань стандартизації понять і методології у роботі з інформаційною безпекою для досягнення універсальності та єдності в розумінні цих понять і заходів безпеки.

Поняття «міжнародна кібербезпека» дійсно часто акцентується на технічних аспектах забезпечення цілісності, доступності та конфіденційності інформації, інформаційно-комунікаційних технологій, а також захисту глобальних мереж та критично важливої інфраструктури. Деякі науковці обмежують своє дослідження саме цими аспектами, оскільки у сфері

кібербезпеки технічні аспекти мають величезне значення через швидкість зміни технологій і постійно зростаючу загрозу кібератак.

Проте, важливо зауважити, що сучасні підходи до кібербезпеки все більше включають інші аспекти, такі як правові, етичні, політичні та соціальні питання. Міжнародна кібербезпека не обмежується лише технічними вимірами, але також охоплює питання законодавства, нормативного регулювання, міжнародних відносин, людської поведінки в кіберпросторі, кіберполітики та ін. Цей більш широкий підхід вимагає врахування складних взаємозв'язків технічних, правових, соціальних та політичних аспектів для досягнення повного рівня захисту в кіберпросторі на міжнародному рівні.

Виступ Б. Обами в Університеті Перд'ю у 2008 р. [5] виявився важливим у контексті підкреслення важливості кібербезпеки як ключової складової національної безпеки США. Після терористичних подій 11 вересня 2001 р. кібербезпека отримала додаткове значення через загрози кібератак та зловживання в інформаційному просторі. Б. Обама, підкреслюючи важливість кібербезпеки, спрямував увагу на необхідність співпраці державних структур, академічних установ та приватних секторів для захисту інформаційних мереж та інфраструктури. Його підходи включали як запобіжні заходи, так і наступальні стратегії в кіберпросторі.

Ці зусилля також передбачали залучення військових структур, таких як Національна агенція безпеки, для захисту національної безпеки США. Приватні компанії, такі як Lockheed, Martin, Boeing, Raytheon, Symantec і Mcafee, стали ключовими партнерами Пентагону у наданні ресурсів для цієї діяльності. Фінансування дослідницьких проектів та розробки нових технологій і засобів інформаційної безпеки зазнайомило США з новими напрямками захисту національної безпеки. Однак ці заходи також викликали обговорення та певне занепокоєння через військову мілітаризацію сфери інформаційної безпеки та залучення військових структур до цих цілей.

Розуміння міжнародної інформаційної безпеки дотримується більш широкого підходу до безпеки в інформаційному просторі, включаючи

психологічний вплив і поширення негативного контенту в міжнародному масштабі. Такий підхід розглядає не лише технічні аспекти захисту інформації, але і способи використання інформаційних ресурсів для впливу на міжнародні відносини, суспільну свідомість і динаміку світового співтовариства. Ця концепція міжнародної інформаційної безпеки ставить акцент на взаємодію міжнародних акторів та їх спільні зусилля для запобігання потенційним загрозам у формі інформаційно-психологічних і кібернетичних впливів. Вона орієнтована на підтримання міжнародної стабільності та захист інформаційного середовища у глобальному масштабі. Це розуміння міжнародної інформаційної безпеки враховує широкий спектр можливих загроз інформаційній безпеці, включаючи не лише технічні аспекти, а й соціальні та психологічні аспекти.

Концепція «м'якої сили», яку розвинули Дж. Най [6] та інші дослідники, відображає ідею використання не лише військової потужності, а й політичних, економічних, культурних, інформаційних і технологічних засобів для досягнення стратегічних цілей держави. Інформаційно-технологічна потужність тут грає важливу роль, оскільки дозволяє впливати на суспільство, політику та міжнародні відносини через інформаційний простір.

Концепція «інформаційної парасолі» відображає ідею того, що країни можуть використовувати свою інформаційну потужність для стримування агресії та захисту від потенційних загроз. США, як країна зі значними інформаційними можливостями та впливом у світі, грають ключову роль у розробці та використанні стратегічних інструментів комунікації та інформаційних технологій. Ці інструменти використовуються для політики стримування й нейтралізації традиційних воєнних загроз і нових видів озброєнь, підтримки національних інтересів та зміцнення впливу в міжнародному масштабі через інформаційну стратегію.

Поняття «інформаційні загрози» відображає можливість існування ризиків для інтересів міжнародних акторів у глобальному інформаційному

просторі. Ці загрози можуть бути технологічного, комунікаційного та психологічного характеру (рис. 1.1).

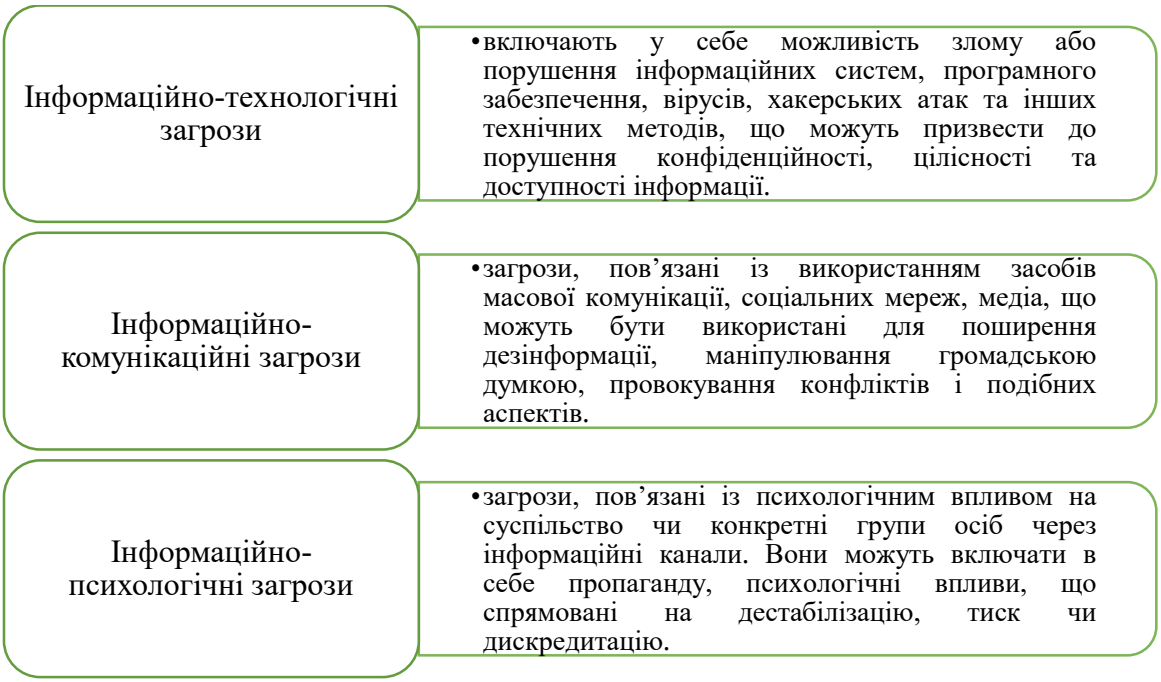

Рис. 1.1. Поняття «інформаційні загрози» у контексті ризиків для інтересів міжнародних акторів у глобальному інформаційному просторі

Джерело: складено автором

Отже, «інформаційні загрози» охоплюють різні аспекти, пов'язані із можливими ризиками, що можуть виникнути у сфері інформаційної безпеки для різних міжнародних акторів та взаємодії між ними у світовому інформаційному просторі.

Цитований погляд дослідників міжнародної інформаційної безпеки відображає комплексність і глибину загроз, які існують у глобальному інформаційному просторі. Вони розглядаються як загрози, які охоплюють не лише окремі країни, але й увесь світ в цілому. Основні підходи та висновки цих досліджень можна узагальнити наступним чином:

1. Глобальний характер загроз – інформаційні загрози розглядаються як потенційні проблеми для всього світу, що можуть виникнути у будь-якому регіоні, країні чи спільноті. Це підкреслює важливість глобальної співпраці для вирішення таких проблем.

2. Необхідність міжнародного співробітництва – політика протидії інформаційним загрозам потребує спільних зусиль усіх країн та міжнародних організацій для створення ефективної стратегії забезпечення безпеки в глобальному інформаційному просторі.

3. Критично важливі сфери – виділення загроз для критично важливих сфер життєдіяльності держави та суспільства (військово-політичні, економічні, культурні, технологічні, терористичні, злочинні) підкреслює те, що ці загрози можуть спричинити серйозні наслідки для стабільності суспільства та держави.

4. Цільове спрямування інформаційних загроз – визначення мети цих загроз – знищення інфраструктури, дестабілізація систем управління, деморалізація суспільства та порушення прав людини, свідчить про їх потенційно негативний вплив на соціальний, політичний і економічний розвиток.

Поняття «інформаційна зброя» відіграє ключову роль у сучасній міжнародній інформаційній безпеці. Це поняття охоплює широкий спектр заходів, методів і технологій, що мають на меті впливати на інформаційну інфраструктуру противника та викликати вплив на його системи управління та громадську думку. Основні аспекти інформаційної зброї включають аспекти, що зображені на рис. 1.2.

Термін «інформаційна зброя» застосовується для опису інструментів, які використовуються для маніпулювання інформацією з метою досягнення стратегічних цілей або ведення інформаційних операцій для зміни суспільного мислення, орієнтації або дій в конфліктних ситуаціях.

Поняття «гібридна війна» відіграє ключову роль у сучасній концепції міжнародної інформаційної безреки. Цей термін, введений Ф. Хоффманом [8], описує сучасні конфлікти, де ведеться поєднання різних видів військових, політичних, економічних, інформаційних, та гібридних методів для досягнення стратегічних цілей. Основні риси гібридної війни включають [9]:

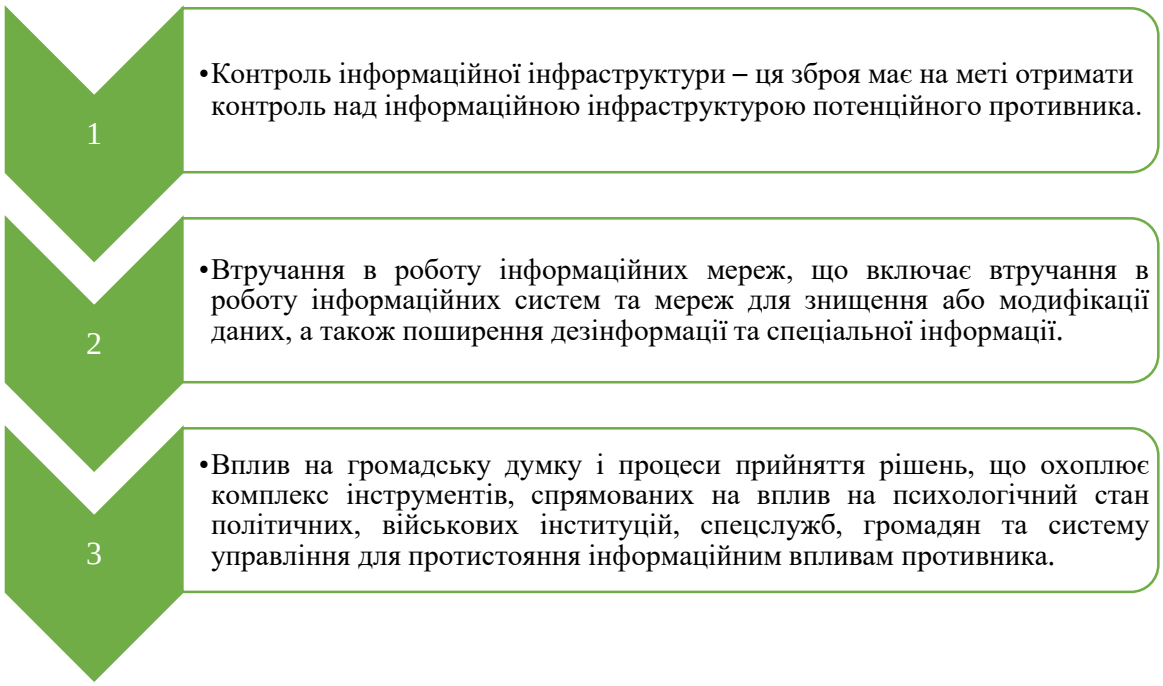

Рис. 1.2. Основні аспекти інформаційної зброї у глобальному інформаційному просторі

Джерело: складено автором за даними [7].

1. Гібридна війна використовує не лише військові засоби та технології, але й елементи неконвенційної, інформаційної та економічної війни для досягнення своїх цілей.

2. Гібридні війни можуть включати в себе співпрацю та координацію різних державних та недержавних груп для проведення військових дій та досягнення стратегічних цілей.

3. Інформаційна компонента гібридної війни є ключовою, оскільки ці конфлікти розраховані на маніпулювання інформацією, використання медіа та пропаганди для впливу на громадську думку та створення певного образу конфлікту.

4. Гібридна війна базується на метанаративах, що використовуються для приховування справжніх намірів та дій у конфлікті.

На нашу думку, ці концепції й поняття використовуються для аналізу та розуміння сучасних конфліктів, де складність та різноманіття методів ведення війни стають нормою. Гібридна війна наголошує на необхідності управління

не лише фізичними аспектами конфлікту, але й на інформаційних та психологічних аспектах для досягнення стратегічних цілей.

Поняття «міжнародний інформаційний тероризм» описує використання терористичними угрупованнями інформаційних систем та ресурсів з метою спричинення терористичних дій [10]. Це включає в себе широкий спектр заходів і методів, які впливають на міжнародний інформаційний простір з метою тероризму. Терористичні групи використовують різноманітні технології та медіа-ресурси для активної інформаційно-пропагандистської діяльності. Способи їхньої роботи включають:

1. Поширення інформації та дезінформація – вони використовують глобальні і національні медіа-ресурси для збільшення обсягу інформації, яка може бути як правдивою, так і змішаною з дезінформацією. Це може стосуватися негативних наслідків терористичних дій, загроз подальшого тероризму та спроби залякування населення.

2. Цілеспрямована пропаганда і деморалізація – така інформаційна кампанія може бути спрямована на деморалізацію правоохоронних органів, політиків, чи інших цільових груп.

3. Психологічний тиск через загрози терористичних акцій – вони можуть намагатися вплинути на громадську думку, залякувати населення, дискредитувати владу, або спонукати до певних дій через психологічний тиск.

Протидія інформаційному тероризму вимагає розробки та впровадження ефективних стратегій та методів для виявлення, припинення і зменшення впливу терористичної пропаганди. Це може включати в себе кібербезпеку, аналітику даних, контрпропаганду, та інші заходи для запобігання інформаційному впливу терористів.

«Мова ворожнечі» відноситься до практики агресивних висловлювань, які спрямовані на приниження, дискредитацію чи засудження представників суспільства за їхніми політичними, расовими, релігійними, гендерними, соціальними чи культурними ознаками [11]. Це може включати у себе образи,

ненависть, загрози та інші форми негативного впливу, які мають на меті налякати, дискредитувати чи вразити чиюсь гідність.

Кліктивізм, хактивізм та тролінг вказують на різноманітні активності в мережі Інтернет, що включають акції інтернет-активістів (хакерів, тролів) з метою залучення уваги до певних питань, впливу на громадську думку або протесту.

Бот-мережі та ботоферми описують групи або системи автоматизованих акаунтів у соціальних мережах, які використовуються для розповсюдження інформації, здійснення впливу або маніпулювання громадською думкою.

«Квантум-безпека» стосується застосування квантових технологій у сфері інформаційної безпеки з метою захисту конфіденційності даних від потенційних кіберзагроз.

«Covid-безпека» – це поняття, яке може відноситися до заходів і стратегій, спрямованих на захист інформації щодо пандемії COVID-19, включаючи відстеження інформаційних загроз, боротьбу з дезінформацією та вплив на громадську свідомість та публічні настрої щодо пандемії.

Варто констатувати, що Facebook, Twitter, YouTube і Microsoft узгодили кодекс поведінки [12], який зобов’язує їх діяти проти поширення «мови ворожнечі» та виявлення висловлювань, які розпалюють ненависть у соціальних мережах. Це означає, що ці компанії взяли на себе зобов’язання видаляти висловлювання, що містять ненависть або провокують конфлікти, упевнюючись, що це відбувається протягом короткого проміжку часу, зазвичай протягом 24 годин. Такий підхід націлений на зменшення поширення негативних повідомлень, які можуть призвести до напруги та конфліктів у соціальних мережах.

На нашу думку, актуальним у цьому контексті в умовах повномасштабного вторгнення РФ в Україну є розгляд проблеми поширення «мови ворожнечі» через проросійські медіаресурси, зокрема в Криму і на Донбасі. За допомогою цієї мови ворожнечі, спрямованої проти української нації, кримських татар, мусульман, мігрантів і проєвропейських активістів

[13], створюється конфліктне середовище та розпалюється ненависть між різними етнічними та соціальними групами. Збільшення української присутності в інформаційно-комунікативному середовищі Криму може стати частиною стратегії по зміцненню національної ідентичності й підвищенню взаєморозуміння між населенням Криму, Сходу України та українською державою. Це може сприяти сприйняттю інформації більш широким колом людей та допомогти зменшити негативний вплив «мови ворожнечі» на сприйняття національних та етнічних ідентичностей. Протистояння цій негативній тенденції потребує комплексного підходу, який міг би включати політичні, соціально-економічні та інформаційні заходи з метою сприяння співіснуванню різних культур і забезпечення рівних умов для усіх громадян.

У свою чергу, термін «кліктивізм» визначається як використання соціальних медіа та інших інструментів Інтернету для просування або реклами будь-якої діяльності, процесу, кандидатів або партій під час передвиборчої агітації чи програм громадських організацій [14]. Це визначення стосується передусім використання медіа-платформ для підтримки політичних або громадських ініціатив у період перед виборами або в рамках роботи громадських організацій. Кліктивізм спирається на масове використання мережі Інтернет, особливо соціальних мереж, для мобілізації громадської підтримки або зацікавленості в певних цілях або проектах. Цей підхід часто використовується для залучення уваги до певних поглядів, проблем або кандидатів, використовуючи різноманітні стратегії цифрового маркетингу та комунікації для залучення та мобілізації аудиторії [15].

Е. Говард влучно відзначає значущість «кліктивізму» у сучасному політичному та соціальному ландшафті [16], де Інтернет та соціальні медіа стали потужними інструментами для організації масових протестів та громадських рухів. Під час арабської весни соціальні мережі дійсно використовувалися для координації та мобілізації протестувальників. Це був потужний механізм для організації масових акцій протесту та звернення до світу, який призвів до великих змін у владі в арабських країнах. Проте, також

важливо відзначити, що влада в цих країнах спробувала обмежити цей вплив, перекриваючи доступ до соціальних мереж та Інтернету.

Загальною тенденцією стало те, що влади збільшували свій контроль над Інтернетом і соціальними мережами в намаганні запобігти масовим протестам і організації громадських рухів, які могли би загрожувати стабільності їх режимів.

У цілому, «кліктивізм» став важливим інструментом для висловлення громадянської позиції та мобілізації широких мас населення для підтримки певних політичних чи соціальних змін.

Так, підходи дослідників до поняттєвих категорій міжнародної інформаційної безпеки справді відображають зміну інформаційної парадигми в сучасному світі. Це відображення нових закономірностей у формуванні міжнародної безпекової політики загалом.

Сучасні інформаційні технології та їх вплив на суспільство привели до необхідності оновлення та переосмислення типології понять у сфері міжнародної інформаційної безпеки. Це оновлення включає в себе такі аспекти, як боротьба з кіберзагрозами, використання соціальних мереж для масової мобілізації та впливу на громадську думку, протидія дезінформації та маніпуляціям інформацією.

Дослідження та систематизація цих аспектів допомагають спеціалістам та міжнародним спільнотам краще розуміти та ефективніше протистояти викликам, що стоять перед інформаційною безпекою у сучасному світі.

Отже, переосмислення та систематизація понять у сфері інформаційної безпеки відображає нові реалії та виклики, з якими суспільство стикається у цифрову епоху, та є ключовим елементом реагування на ці виклики для забезпечення міжнародної безпеки.

1.2. Сучасні теорії міжнародної інформаційної безпеки

Сучасні міжнародні відносини включають в себе широкий спектр концепцій та підходів до інформаційної безпеки. Низка зазначених концепцій відображає сучасні тенденції у галузі захисту інформації та впливу на міжнародні відносини:

Концепція «м'якої» та «гострої» сили – визнає, що у сучасному світі інформаційна влада і вплив можуть бути реалізовані як шляхом суворої дії (гострої сили), так і за допомогою м'яких інструментів впливу (м'якої/розумної сили).

Теорія міжнародної інформаційної безпеки – фокусується на заходах щодо захисту інформації та даних від загроз, включаючи кіберзлочинність, кібершпигунство та кібератаки.

Інформаційне домінування – концепція, яка описує прагнення домінувати в інформаційному просторі шляхом контролю або маніпуляції інформацією.

Інформаційне протиборство та інформаційні озброєння. Ці поняття вказують на конкурентне або конфліктне використання інформації для досягнення політичних, економічних або військових цілей.

Гібридні, мережево-центричні та кібернетичні війни. Ці поняття відображають сучасні форми конфліктів, де кібератаки, маніпуляція інформацією, гібридні загрози поєднуються для досягнення воєнних або політичних цілей.

Організаційні підходи підтримки інформаційної безпеки – описують структурні та управлінські аспекти захисту інформації в організаціях та міжнародних установах.

Теорія «чорного лебедя» стверджує, що непередбачувані події можуть мати значний вплив на безпекові умови у міжнародних відносинах, що може призвести до змін у стратегіях безпеки та політиці інформаційної безпеки.

У сучасних міжнародних економічних відносинах інформаційна безпека стає все більш важливою з погляду захисту суспільства та економіки від загроз в інформаційному просторі. Такий широкий спектр концепцій відображає різноманітність загроз та підходів до їх вирішення у світі, який все більше залежить від цифрових технологій та інформаційного обміну.

Концепції інформаційної безпеки враховують широкий спектр аспектів, що включають не лише технічні та стратегічні підходи до захисту інформації, а й філософсько-політичні принципи, національні цінності та соціокультурні стандарти. Ці концепції покладаються на базові ініціативи, спрямовані на забезпечення стабільності та розвитку суб'єктів міжнародних економічних відносин та світового співтовариства.

Основні компоненти міжнародної інформаційної безпеки узагальнено автором на рис. 1.3 (рис. 1.3). Ці аспекти взаємодіють і еволюціонують у контексті змін у міжнародному розвитку, науково-технологічній модернізації та інтегрованих процесів у сучасному світі. Інноваційні загрози, такі як нові види кіберзагроз та зміна способів маніпулювання інформацією, впливають на пріоритети та стратегії забезпечення міжнародної безпеки і вимагають постійного вдосконалення і адаптації заходів захисту.

Вищевикладене свідчить про важливість наукових досліджень у сфері інформаційної безпеки та її міжнародного виміру. Останні дослідження у цій галузі акцентують увагу на дослідженні трансформацій глобальної безпекової парадигми, а також розглядають нові аспекти, пов'язані з інформаційною безпекою в міжнародних відносинах (рис. 1.4).

Ключові напрямки досліджень включають:

1. Концепції інформаційної безпеки у новому геополітичному середовищі. Аналіз змін у світовій політиці та геополітичному ландшафті, що впливають на концепції інформаційної безпеки на міжнародній арені.

2. Інформаційне протиборство та нові види загроз. Розгляд сутності та характеристик інформаційного протиборства, а також аналіз нових загроз і гібридних впливів, зокрема інформаційно-психологічних.

1. Політичний аспект:

- Включає в себе стратегії, політику та правила, які регулюють використання, доступ та контроль над інформацією в контексті міжнародних відносин.

2. Економічний аспект:

- Включає важливість захисту економічних інтересів, фінансових систем та електронної комерції в умовах глобалізації та цифрової економіки.

3. Інформаційний аспект:

- Сфера захисту інформації, даних та обміну інформацією, включаючи заходи протидії кіберзлочинності та кіберзагрозам.

4. Військовий аспект:

- Аспект, пов'язаний із використанням технологій та інформації у військовій сфері, включаючи кібервійни та кібероборону.

5. Енергетичний аспект:

- Враховує важливість забезпечення інформаційної безпеки в енергетичному секторі, особливо в контексті критично важливої інфраструктури.

6. Антитерористичний аспект:

- Охоплює заходи протидії терористичним групам, які можуть використовувати інформаційні технології для своїх цілей.

Рис. 1.3. Основні компоненти міжнародної інформаційної безпеки

Джерело: складено автором

3. Стратегії протидії використанню інформаційних озброєнь у кризових ситуаціях. Дослідження можливих стратегій і методів протидії використанню інформаційних озброєнь у сучасних кризових та непередбачуваних ситуаціях.

4. Аналіз поведінки міжнародних акторів у сфері інформаційної безпеки. Розгляд стратегій та дій ключових міжнародних гравців у плані захисту своєї інформаційної безпеки та взаємодії в цьому контексті.

Ці дослідження відіграють важливу роль у визначенні стратегій захисту інформаційної безпеки на міжнародній арені та формуванні ефективних

політичних та стратегічних відповідей на сучасні виклики та загрози у цій сфері.

Рис. 1.4. Трансформація глобальної безпекової парадигми

Джерело: складено автором

Політика інформаційної безпеки значно впливає на міжнародні відносини, стратегії зовнішньої та безпекової діяльності міжнародних акторів, інституцій та безпекові доктрини. Дійсно, вона спричиняє трансформацію концепції міжнародної безпеки у постбіполярному світі та впливає на способи використання інформаційних озброєнь та інтервенцій у регіональних та локальних конфліктах. Ось деякі ключові аспекти цього впливу:

Трансформація концепції міжнародної безпеки. Політика інформаційної безпеки змінює уявлення про безпеку в міжнародних відносинах, ураховуючи важливість захисту інформації та даних у новому геополітичному середовищі.

Зміна мотивацій міжнародних акторів. Використання інформаційних озброєнь та інформаційно-психологічних втручань у конфліктні ситуації стає активнішим з урахуванням їх потенційного впливу на сучасні міжнародні конфлікти.

Перегляд повноважень міжнародних інститутів з підтримання безпеки. Міжнародні організації, що відповідають за підтримання міжнародної безпеки, поступово включають інформаційну складову до своїх завдань та стратегій.

Включення інформаційної складової у безпекові доктрини. Сучасні безпекові доктрини країн та міжнародних організацій враховують інформаційний аспект у визначенні стратегій захисту національної та міжнародної безпеки.

Отже, політика інформаційної безпеки відіграє значну роль у формуванні стратегій та підходів до забезпечення міжнародної стабільності, впливає на мотивації та дії міжнародних акторів у конфліктних ситуаціях, а також змінює перспективи міжнародних організацій у сфері забезпечення безпеки.

Еволюція концепцій сил у міжнародних економічних відносинах відбувалася відповідно до змін у системі міжнародної безпеки та змін у стратегіях воєнних конфліктів. Теоретики виокремлюють дві основні стратегії сили: «м’яка сила» та «жорстка сила».

Стратегія «жорсткої сили» у міжнародних економічних відносинах пояснюється як здатність держав досягати переваг над іншими міжнародними акторами шляхом застосування примусу та нав’язування своїх інтересів. Ця стратегія базується на використанні економічної та військової сили для досягнення своїх цілей. Вона включає в себе військовий, економічний та фінансовий тиск і розглядається як засіб впливу на інших учасників міжнародної арени.

«Жорстка сила» може бути спрямована на застосування військових операцій, економічних санкцій, торговельних обмежень або інших форм тиску з метою досягнення певних політичних, економічних чи стратегічних цілей.

Важливо зазначити, що у сучасному світі концепція сили у міжнародних відносинах поступово еволюціонує. На додачу до «жорсткої сили», дедалі більше уваги приділяється концепції «м’якої сили», яка ґрунтується на

здатності країн до впливу на інших за допомогою культурного, інформаційного та гуманітарного впливу, дипломатії, міжнародних співтовариств та інших невійськових засобів впливу. «М’яка сила» спрямована на отримання впливу через переконання, а не через примус.

Таким чином, у сучасних міжнародних економічних відносинах спостерігається ширший спектр стратегій сили, що включає як «жорстку», так і «м’яку» силу, а вибір стратегії залежить від конкретної ситуації та мети, яку держава прагне досягти.

Ідея глобального домінування США не лише за показниками військової сили та економічної потужності, а й за можливостями несилового впливу на міжнародні відносини була адресована як президентській адміністрації Дж.Буша-старшого, так і теоретикам наукової школи «політичного реалізму», яким «…слід було б відмовитися від абсолютизації ролі «жорсткої сили» в світовій політиці в умовах завершення біполярної конфронтації і досягати переваг через механізми узгодження зовнішньополітичних акцій і залучення до співпраці інших акторів з урахуванням спільних цінностей». Загалом концепція «м’якої сили», до якої було віднесено й інформаційно-технологічну потугу, вперше була сформульована на науково-теоретичному рівні Дж. Наєм для підтримки національних інтересів США на міжнародній арені і просування важливих здобутків американської соціальної і культурної політики [17].

Дж. Най в своїй науковій роботі «М’яка сила. Складові успіху у світовій політиці» звертає увагу на проблеми та особливості оцінки ефективності використання «м'якої сили» у зовнішній та безпековій політиці Сполучених Штатів Америки. Він визначає деякі концептуальні проблеми у розумінні міжнародної інформаційної безпеки, які ускладнюють оцінку впливу «м’якої сили»:

1. Психологічний стереотип. Відзначається, що традиційні фактори, такі як військовий потенціал, ВНП, чисельність населення, енергетичні ресурси,

досі мають переважаючу роль у теоріях балансу сил, інколи перекриваючи роль інформації як потужного чинника впливу.

2. Нерозуміння природи інформації та її системних зв'язків. Інформація часто розглядається відокремлено від інших складових, таких як політичні, економічні, соціальні аспекти. Недостатнє усвідомлення того, як інформаційна складова пов'язана з іншими аспектами, що формують міць держави та суспільства.

3. Неусвідомлення стратегічної ролі міжнародної інформаційної безпеки. В США та інших розвинених країнах не завжди повністю розуміють стратегічне значення міжнародної інформаційної безпеки та можливі наслідки використання інформаційних озброєнь для забезпечення миру.

На нашу думку, ці проблеми визначають ключові аспекти, які необхідно враховувати при аналізі використання «м'якої сили» у зовнішній та безпековій політиці країн, оскільки вони можуть вплинути на ефективність стратегій економічного розвитку в міжнародному контексті.

Варто зазначити, що існує широкий спектр теорій та досліджень щодо інформаційної безпеки у міжнародних економічних відносинах, які були представлені в працях таких авторів, як М. Лібіцкі, Б. Берковіц, Р. Банкер Ф. Хоффман, А. Себровскі, Дж. Гарстка, Дж. Стейн, У. Лінн, Д. Арквілль, Д. Ронфельдт та багатьох інших дослідників. Ці дослідження виявили наявність різноманітних нових загроз у сфері інформаційної безпеки, які походять з-за меж національних кордонів та виявляються в деяких випадках як переважаючі за можливостями захисту суверенних держав. Ці загрози можуть включати кібератаки, кібершпигунство, масштабні розповсюдження дезінформації та інші форми кіберзагроз.

У зв'язку з цими викликами та загрозами, виникає необхідність розробки та впровадження стратегій, спрямованих на протидію новим інформаційним загрозам. Ці стратегії мають охоплювати широкий спектр заходів, таких як кібербезпека, захист даних, підвищення інформаційної готовності та виявлення загроз, інтернаціональне співробітництво у сфері

кібербезпеки та інші ініціативи, що спрямовані на підвищення інформаційної безпеки у міжнародних відносинах.

Так, М. Лібіцкі є відомим дослідником, який розробив концепцію інформаційного домінування. Він визначив потенційний вплив інформаційних озброєнь у завоюванні інших держав без руйнівних наслідків. Концепція інформаційного домінування передбачає використання інформаційних засобів та технологій для здійснення впливу на інші країни, зокрема, шляхом використання інформаційних озброєнь. Це може включати такі методи, як кібератаки, психологічні операції, дезінформацію, вплив на громадську думку через медіа та інші канали [18].

М. Лібіцкі аргументує, що використання інформаційних озброєнь може забезпечити завоювання інших держав без необхідності відкритої війни або руйнівних наслідків, які часто супроводжують традиційні військові конфлікти [19]. Таким чином, він робить акцент на важливості інформаційних технологій та їх потенціалу в сучасному світі для досягнення політичних та стратегічних цілей без відкритого використання фізичної сили.

Проте слід відзначити, що використання інформаційних озброєнь має свої ризики, оскільки це може викликати напруження у міжнародних відносинах, порушувати кібербезпеку, спричиняти дезінформацію та інші негативні наслідки для безпеки та стабільності світового співтовариства.

У. Лінн вніс значний внесок у розвиток теорії глобальної кібервійни та інформаційної безпеки у сучасних міжнародних відносинах. Його дослідження визначають деякі ключові характеристики цієї сфери [20]:

1. Кіберпростір як самостійне поле діяльності. У. Лінн визначає кіберпростір як окремий вид операцій, де відбувається віртуальна боротьба, кібератаки та захист інформаційних систем.

2. Тактика «активного захисту» та координація дій. У. Лінн вказує на необхідність прийняття тактики активного захисту, спрямованої на виявлення потенційних кіберзагроз. Також він підкреслює важливість координації дій

між структурами внутрішньої безпеки для захисту стратегічно важливих мереж та інфраструктури.

3. Співпраця із партнерами та союзниками. У. Лінн визначає необхідність співпраці та обміну інформацією із іншими країнами, партнерами для ефективної протидії кіберзагрозам.

4. Протидія кібератакам. У. Лінн акцентує увагу на необхідності розробки та впровадження стратегій протидії кібератакам для забезпечення кібербезпеки.

Крім того, У. Лінн підкреслює важливість розуміння та врахування сучасних реалій ведення війн та нових типів інформаційних та кіберзагроз при формуванні політики забезпечення безпеки в сучасних державах. Його дослідження стали важливим внеском у розуміння та протидію кіберзагрозам у міжнародних економічних відносинах.

Річард Кларк Банкер є визнаним американським теоретиком з питань національної безпеки та передових концепцій щодо модернізації способів ведення війни у сучасній епохі. У своїх роботах Р. Банкер [21] аналізує еволюцію сучасних конфліктів, зокрема ураховує роль технологій, інформаційних засобів та кіберпростору у веденні сучасних військових дій. Він звертає увагу на поняття гібридної війни, кібервійни та інших аспектів нових типів конфліктів, де використання інформаційних технологій та кіберзасобів грає значну роль.

Р. Банкер досліджує можливі наслідки та виклики, які виникають у зв’язку з розвитком технологій та їх вплив на сучасні військові стратегії та тактики. Він також вивчає роль інформаційної безпеки та кібербезпеки у контексті захисту національних інтересів у сучасних умовах.

Дослідження Р. Банкера важливі для розвитку теорій інформаційної безпеки через їх фокус на аналізі сучасних конфліктів та визначенні стратегій та заходів для захисту національної безпеки в умовах нових загроз.

Теорія «чорного лебедя», запропонована Нассімом Ніколасом Талебом, стала важливим аспектом розуміння ризиків і непередбачуваних подій у

сучасному світі. Н. Талеб [22] у своїй теорії зосереджується на «чорних лебедях» – подіях, які є вкрай рідкісними, непередбачуваними та мають суттєвий вплив. Ці «чорні лебеді» відрізняються від стандартних або передбачуваних подій, оскільки їх важко передбачити на основі існуючих моделей або даних. Такі непередбачені події можуть мати значний вплив на різні сфери життя – від економіки до політики, від технологій до культури. Вони можуть спричиняти значні зміни в системах та структурах, змушуючи нас переосмислити наші уявлення про світ та реагувати на нові виклики.

Ця теорія важлива для розуміння міжнародної інформаційної безпеки через свій акцент на ризиках і подіях, які не можуть бути передбачені традиційними методами прогнозування. Розгляд «чорних лебедів» дозволяє краще розуміти природу непередбачуваних загроз і ризиків у контексті міжнародної інформаційної безпеки та розвитку стратегій для їх управління.

Аналіз концептуальних підходів та теоретичних досліджень у сфері міжнародної інформаційної безпеки підтверджує, що вони враховують значні трансформації в інформаційній парадигмі глобального розвитку. Ці зміни відображають сучасні особливості розвитку системи міжнародних економічних відносин. Ця трансформація відбувається під впливом швидкої зміни технологій, нововведень у цифровій сфері, зростаючої кількості кіберзагроз, а також зміни пріоритетів та методів захисту від цих загроз. Спричинені цими трансформаціями нові виклики потребують постійних інновацій у сфері захисту інформаційної безпеки для забезпечення стабільності та безпеки на міжнародній арені.

Отже, розвиток системи міжнародних економічних відносин на сучасному етапі вимагає постійного перегляду та удосконалення стратегій інформаційної безпеки для адаптації до нових викликів, що виникають у цифровому світі. Це включає в себе не лише захист інформаційних систем, а й адекватну реакцію на кіберзагрози та вироблення нових методів міжнародної інформаційної безпеки, що враховують сучасні реалії та потреби.

1.3. Методологічні основи дослідження безпеки інформаційного середовища у міжнародних економічних відносинах

Вітчизняна школа досліджень безпеки інформаційного середовища у міжнародних відносинах є значущою та має численні наукові роботи, які висвітлюють ключові аспекти цієї проблематики. Вони включають аналіз трансформаційних процесів у системі міжнародної безпеки, параметри і особливості сучасного інформаційного протиборства, вивчення практики гібридних воєн, а також дослідження інформаційної безпеки держави.

У наукових працях висвітлюються тенденції у розвитку міжнародних економічних відносин, пов’язані із використанням інформаційних технологій, кіберзагрозами, питаннями кібербезпеки, інформаційного впливу на політичні процеси тощо. Дослідження розглядають також вплив інформаційної безпеки на національну безпеку, стратегії захисту інформаційних ресурсів, а також інструменти та методи боротьби з інформаційними загрозами.

Наукові праці грають важливу роль у формуванні національної стратегії інформаційної безпеки та в розробці ефективних заходів для захисту від сучасних загроз і викликів, що постають у сфері інформаційної безпеки. Їх аналіз і рекомендації відіграють важливу роль у формуванні політики безпеки країни в умовах сучасного цифрового середовища та змін у міжнародних економічних відносинах.

Можна стверджувати, що в Україні сформувалися потужні наукові школи, присвячені дослідженню інформаційної та кібербезпеки, які активно вивчають ключові аспекти цієї сфери. Дослідження, проведені в рамках цих шкіл, охоплюють широкий спектр питань, пов’язаних із інформаційною безпекою та кіберзахистом.

Наукові, експертно-аналітичні та фахові розвідки відомих українських науковців та експертів, таких як В.Горбулін, О.Литвиненко, М.Ожеван, Д.Дубов, А.Баровська, С.Гнатюк, Г.Яворська, Т.Ісакова та інших, мають

значний внесок у розвиток інформаційної політики, кібербезпеки та вивчення викликів, що пов’язані з гібридною війною та іншими аспектами цієї сфери.

Дослідження цих науковців охоплюють широкий спектр тем, таких як інформаційно-психологічні аспекти гібридної війни, використання стратегічних комунікаційних технологій, кібербезпекові тренди, захист виборчих процесів від деструктивних інформаційних впливів, нормативно-правове регулювання у сфері інформаційної безпеки, дотримання інформаційних прав і свобод в Україні та багато іншого. Ці дослідження важливі для формування національної стратегії у сфері інформаційної та кібербезпеки та вирішення актуальних питань у цій галузі як на національному, так і на міжнародному рівнях.

«Світова гібридна війна: український фронт» під редакцією В.Горбуліна [23] є значущим дослідженням, присвяченим аналізу гібридної війни та російської агресії проти України у контексті світової безпеки. Це колективне дослідження у своїй сутності охоплює різні аспекти цього явища та відображає його вплив на різні сфери життя. У праці розглядаються не лише воєнні, а й політичні, економічні, соціальні, гуманітарні та інформаційні аспекти гібридної війни. Дослідження виокремлює причини та передумови російської агресії проти України, її стратегічні цілі та методи впливу. Важливою є також оцінка спроможності України з відстоювання свого державного суверенітету в умовах гібридної агресії.

Це колективне дослідження має значний внесок у розуміння сутності гібридних конфліктів та їх впливу на сучасну міжнародну систему безпеки. Інсайти, що надані цим дослідженням, можуть бути корисними як для України, так і для інших країн, які стикаються із подібними викликами та загрозами у сучасному світі.

Наукові праці О. Литвиненка [24] щодо теоретико-методологічних аспектів спеціальних інформаційних операцій та пропагандистських кампаній у сучасному світі мають велике значення для розуміння принципів управління впливом у складних системах.

О. Литвиненко досліджував класичні підходи до управління складними системами впливів і розглядав їх застосування в сфері інформаційної безпеки. Його роботи стосовно інформаційних операцій у контексті концепції «м'якої сили» підкреслюють важливість стратегій непрямих дій і використання синергетичних підходів для досягнення цілей інформаційної безпеки.

М. Ожеван [25–26] зробив значний внесок у вивчення проблем інформаційної безпеки, спеціалізуючись на дослідженні пріоритетних напрямків діяльності США у цій сфері за президентства Б. Обами. Одним із ключових акцентів його досліджень була «інформаційна парадигма», яка характеризувала стратегію безпекової політики провідної країни світу. Він висвітлив, як в контексті інформаційної безпеки, стратегія безпеки США підкреслювала поєднання різних ідеологічних підходів, таких як ліберально-демократична та консервативно-республіканська ідеології. М. Ожеван вивчав, як це поєднання ідеологій впливало на підходи до вирішення проблем інформаційної безпеки та формулювання стратегій у цій сфері під час президентства Б. Обами. Його роботи мали велике значення для розуміння того, як різні політичні уявлення впливають на міжнародну інформаційну безпеку.

Д. Дубов [27–28] зробив значний внесок у вивчення основних принципів та аспектів інформаційної безпеки, проводячи дослідження, що охоплюють різні аспекти розвитку інформаційного суспільства та його вплив на геополітичне протистояння. Він аналізував стратегічні аспекти кібербезпеки в контексті України та вирішення питань державної інформаційної політики в умовах гібридного миру та війни. Його дослідження були спрямовані на розуміння сутності та розвитку інформаційного простору, а також вивчення та аналіз стратегій, необхідних для забезпечення кібербезпеки національних систем у сучасному світі. Ці роботи стали важливим джерелом для формулювання стратегій та політики в галузі інформаційної безпеки, зокрема в контексті України, у часи гібридної війни та геополітичного напруження.

Дослідження, проведені науковцями Національного інституту стратегічних досліджень [29] щодо державно-приватного партнерства в галузі кібербезпеки, мають важливе значення для формування практичних стратегій у цій сфері. Акцентуючи увагу на теоретичних аспектах цього партнерства та використанні світового досвіду, особливо у таких країнах, як США, ЄС, ФРН, Велика Британія, Польща та Україна, дослідники проаналізували та визначили ключові аспекти у формуванні довірчих відносин між державним та приватним сектором у питаннях кібербезпеки.

Ці роботи можуть бути корисними для урядів, спеціалістів з кібербезпеки, а також для приватних компаній, оскільки вони можуть надати рекомендації та моделі, які сприятимуть покращенню співпраці між державними установами та приватними підприємствами для ефективного захисту кіберпростору. Такий підхід може сприяти покращенню загального рівня кібербезпеки в країні та зниженню загроз в цьому важливому сегменті сучасного суспільства.

Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка відіграє значну роль у дослідженні проблем політики інформаційної безпеки. Його наукові праці та дослідження розглядають широкий спектр аспектів теорії та практики міжнародної інформаційної безпеки, що стали важливим внеском у розвиток цієї галузі.

Спеціалісти Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка зосереджують увагу на темах, пов’язаних із теорією інформаційних війн, психологічного впливу через інформацію, виявленні та характеристиці сучасних інформаційних загроз, методах протидії дезінформації та використанні маніпулятивних технологій у медіа-впливі.

Ці дослідження та публікації відображають актуальні тенденції у галузі інформаційної безпеки, сприяючи розвитку стратегій захисту від нових викликів, що виникають у світі інформаційних технологій та комунікацій.

Г. Почепцов є видатним представником наукової школи, який активно досліджував проблеми інформаційної безпеки [30] та її вплив на сучасне

геополітичне середовище. Він зосередився на розумінні взаємозв'язків між різними теоріями та практиками, такими як теорія комунікації, пропаганди, розвідки, теорії прийняття рішень, концепція «м'якої сили», а також на аналізі сучасних явищ, таких як мережево-центричні війни, інформаційні озброєння, гібридні та смислові війни.

У своїх дослідженнях Г. Почепцов визначав вплив зовнішніх та внутрішніх інформаційних інтервенцій на національну безпеку, розкрив сутність гібридних війн. Також він приділяв увагу ролі мас-медіа як важливих ресурсів, що мають значний вплив на поширення фейкових повідомлень і маніпуляцій з новинним контентом. Його внесок є важливим для розвитку міжнародних економічних відносин та розуміння сучасних динамік у світі інформаційних технологій та їх впливу на глобальну безпеку.

Є. Макаренко у своїх дослідженнях [31–32] розглядає питання міжнародної інформаційної безпеки в контексті формування нової структури міжнародних відносин, що відбувається в умовах стрімкого розвитку високих технологій. Вона акцентує увагу на нових підходах та параметрах сучасної системи міжнародної безпеки, які виникають внаслідок широкого використання інформаційно-комунікаційних технологій у політичних, економічних, соціальних та культурних сферах.

У своїх працях Є. Макаренко зазначає, що руйнівний вплив сучасного озброєння та різноманітність використання інформаційних технологій змусили ООН та інші міжнародні організації включити проблему інформаційної безпеки до свого глобального порядку денного. Також вона відзначає необхідність суворого дотримання принципів незастосування сили, невтручання внутрішніх справ держав, захисту прав і свобод, а також недопущення використання сучасних технологій з протиправною метою.

У зв'язку з цим, Є. Макаренко проводить аналіз існуючого міжнародно-правового регулювання інформаційної безпеки та пропонує розробку регуляторних положень для міжнародного контролю за інформаційним

озброєнням. Її робота спрямована на забезпечення міжнародної стабільності та безпеки у контексті сучасних технологічних викликів.

Науковці О. Андрєєва, Н. Бєлоусова, І. Валевська, С. Даниленко, О. Запорожець, М. Капітоненко, О. Кучмій, І. Мінгазутдінов, Н. Піпченко, М. Рижков, Ю. Романенко, а також О.Фролова [33–43] у своїх дослідженнях розглянули різноманітні аспекти, пов’язані із інформаційною безпекою та міжнародними економічними відносинами. Основні теми досліджень цих науковців включають:

1. Концепцію інформаційної безпеки України. Аналіз концепції інформаційної безпеки, що включає у себе визначення загальних принципів, цілей і завдань, а також розгляд поточного стану інформаційної безпеки в країні.

2. Інформаційний тероризм. Розуміння сучасних форм і методів інформаційного тероризму, включаючи аналіз стратегій, тактик і наслідків інформаційних атак.

3. Кризові комунікації. Дослідження специфіки і проблем кризової комунікації в сучасному інформаційному середовищі, їх вплив на стабільність та безпеку.

4. Трансформація інформаційної парадигми глобального розвитку. Аналіз змін у сучасному світі, пов’язаних із інформаційними технологіями, розвитком медіа та їх вплив на міжнародні економічні відносини.

Ці дослідження є важливими для розуміння і побудови стратегій у сфері міжнародних економічних відносин, а також для розробки засад інформаційної безпеки національних держав в умовах зростаючих інформаційних викликів.

Наукові дослідження в галузі міжнародної інформаційної безпеки в Україні відбуваються не лише у столичних університетах, але й у інших вищих навчальних закладах країни, таких як Східноєвропейський національний університет імені Лесі Українки. Дослідження науковців А. Шуляк, Є. Тихомирової та Н. Карпчук [44] є важливими для розуміння сучасних

викликів і загроз у галузі інформаційної безпеки. Вони розглядають різноманітні аспекти, такі як інформаційний тероризм, стратегічні комунікації, дезінформація, медіальне ведення війни та вплив медіатехнологій на конфлікти. Ці дослідження виявляються актуальними в контексті глобальних та регіональних інформаційних тенденцій, що впливають на міжнародні економічні відносини, зокрема у контексті сучасних гібридних загроз та інформаційних воєн. Вони надають новий погляд на роль і важливість інформаційної безпеки в сучасному світі, де інформація стає однією із основних видів зброї у суспільному, політичному та культурному просторі.

У науковій роботі «Медіа як невоєнний метод упливу в гібридній війні» дослідниця Н. Карпчук [45] зазначає, що останнім часом досить часто використовуються технології, які спрямовані на створення псевдореальності задля формування певної «картини дійсності» у масовій свідомості спільноти в контексті гібридної війни. Ці технології можуть включати різноманітні методи та засоби, такі як:

1. Фейкові новини та дезінформація. Розповсюдження маніпулятивної інформації або фейкових новин для сприйняття бажаного образу подій або ситуацій.

2. Цифрова обробка зображень та відео. Використання редакційних програм для створення фальшивих або змінених зображень та відеоматеріалів, що може призвести до створення неіснуючих подій чи маніпуляції фактами.

3. Соціальні мережі та інтернет. Використання платформ соціальних мереж для поширення пропаганди, спрямованої на маніпулювання думкою громадськості через демонстрацію вигідних для агресора перекручених або вигаданих подій.

4. Інформаційні атаки. Намагання завдати шкоди шляхом перешкоджання роботі інформаційних систем або поширення шкідливих програм.

Ці методи використовуються для формування псевдореальності, яка може бути спрямована на маніпулювання громадською думкою, сприйняттям подій або політичними переконаннями. Це є важливим аспектом гібридної війни, оскільки вплив на масову свідомість може мати значний вплив на ставлення громадськості до конфлікту або до окремих політичних подій.

Наукова школа з інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича фокусується на різноманітних аспектах інформаційної безпеки. Дослідження в рамках цієї школи охоплюють як теоретичні основи цієї сфери, так і практичні застосування зокрема у сферах масової та соціальної комунікації (рис. 1.5).

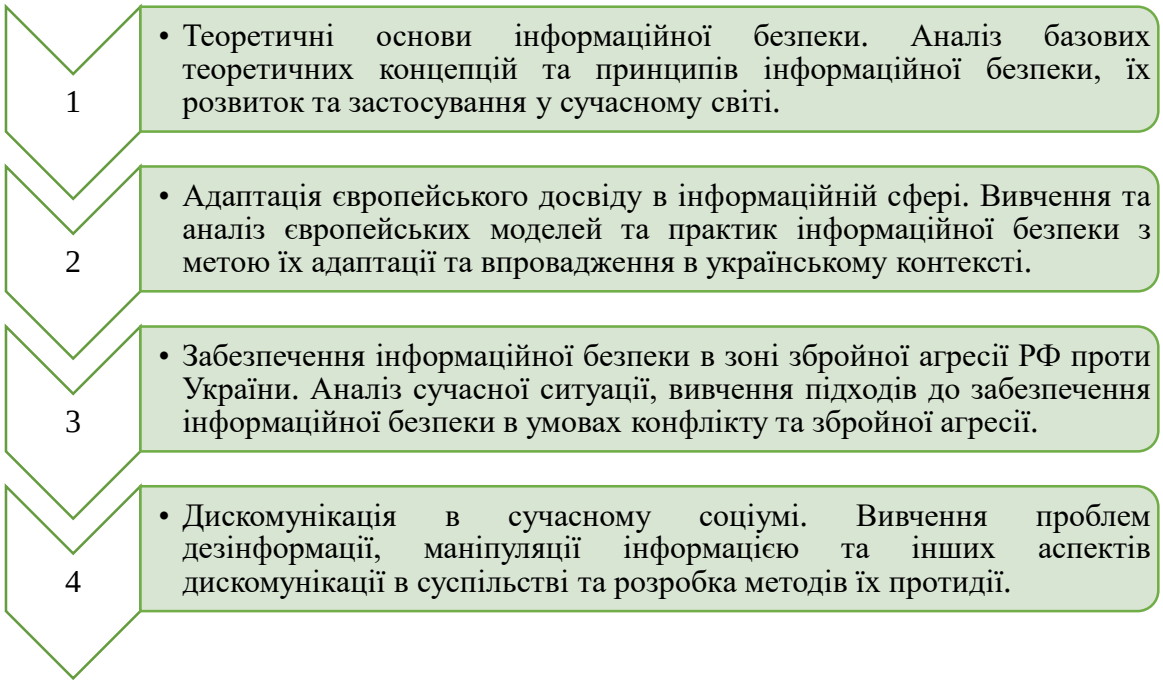

Рис. 1.5. Ключові напрямки досліджень наукової школи з міжнародної інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича

Джерело: складено автором

Ці дослідження спрямовані на розуміння суті інформаційної безпеки в різних контекстах, а також на розвиток практичних методів інформаційної безпеки, які відповідають сучасним викликам і загрозам.

Як висновок, варто зазначити, що дискурс стосовно міжнародної інформаційної безпеки дійсно свідчить про наявність сформованої методологічні основи дослідження безпеки інформаційного середовища у міжнародних відносинах. Ця наукова традиція вимагає подальших комплексних наукових досліджень, більш деталізованого та конкретизованого погляду на окремі аспекти і наслідки впливу інформаційних впливів на міжнародне економічне співробітництво. Теоретичні розвідки українських науковців є важливим ресурсом для вдосконалення стратегії інформаційної безпеки України. Вони можуть бути використані для визначення ролі як України, так і міжнародних організацій у захисті інформаційної незалежності країни та безпеки інформаційного середовища загалом. Аналіз цих досліджень може також сприяти прогнозуванню перспектив розвитку інформаційних інструментів на майбутнє та визначенню стратегій для подальшого розвитку інформаційної безпеки.

Висновки до розділу 1

Підходи до політики інформаційної безпеки у міжнародному вимірі відображають необхідність балансування між захистом національних інтересів та співпрацею на міжнародному рівні для ефективної боротьби з сучасними загрозами інформаційної безпеки. Це поєднання стратегій та пріоритетів дозволяє країнам ефективніше відповідати на нові виклики і загрози у цифровому віці.

Зміни у міжнародних відносинах під впливом інформаційної парадигми глобального розвитку відображаються у розвитку наукових теорій та стратегій. Постійно зростаюча важливість цифрових технологій, засобів комунікації та інформаційної взаємодії відкриває нові можливості, але й приносить нові загрози, такі як кібератаки, дезінформація та інші форми кіберзлочинності.

Саме тому країни виявляють зацікавленість у зміцненні співпраці на міжнародному рівні для спільного протистояння цим загрозам. Спільні зусилля у сфері інформаційної безпеки стають надзвичайно важливими для забезпечення стабільності та захисту від новітніх викликів, що стали не відокремленою частиною сучасного міжнародного середовища.

Оцінка результатів напрацювань в галузі міжнародної інформаційної безпеки визначається рядом ключових аспектів:

1. Чіткість концепції інформаційної безпеки. Оцінка залежить від того, наскільки чітко визначено та осмислено поняття інформаційної безпеки, її сутність, складові елементи та цілі.

2. Перетин концепцій. Розуміння та аналіз взаємодії концепцій міжнародного розвитку та політики інформаційної безпеки є важливими. Це включає визначення спільних точок, де ці концепції перетинаються, виявлення спільних детермінант і підтримку стратегій міжнародного співробітництва в цій сфері.

3. Типологія понять інформаційної безпеки. Розроблення чіткої системи понять інформаційної безпеки, включаючи їх класифікацію, взаємозв’язки та диференціацію, що допомагає краще розуміти цю область.

4. Інституціональне забезпечення. Ефективність інституційного забезпечення міжнародної інформаційної безпеки визначає чи існують відповідні установи, процедури та механізми для реалізації та координації цих стратегій.

5. Протидія гібридним інформаційним впливам. Розробка ефективних стратегій протистояння сучасним гібридним загрозам в інформаційній сфері, включаючи кіберзлочинність, дезінформацію та інші форми інформаційної війни.

Успішність досліджень та напрацювань у цих напрямках може визначати ефективність стратегій інформаційної безпеки на міжнародному рівні та їх здатність до адаптації до умов сучасного світу.

Так, сучасні процеси трансформації системи міжнародної безпеки та зміни інформаційної парадигми безпекової політики відображають важливі аспекти, які впливають на поняттєві категорії інформаційної безпеки. Деякі ключові підходи, які враховуються в цьому контексті:

1. Гібридні конфлікти та інформаційний вплив – застосування нових інноваційних інструментів інформаційного впливу у гібридних конфліктах стає значущим фактором. Це включає маніпулятивні технології, розповсюдження дезінформації, оновлення інформаційних ресурсів та створення викривленої реальності.

2. Руйнування інформаційно-психологічного середовища – постійна еволюція цих процесів може призвести до руйнування стійкості та стабільності міжнародного та національного інформаційно-психологічного середовища, відхилень в цінностях суспільства та порушень основних прав і свобод.

3. Трансформація ціннісних орієнтацій – викривлення інформації та маніпуляції можуть призвести до зміни ціннісних орієнтацій суспільства, що може мати серйозний вплив на внутрішню стабільність країн і міжнародну співпрацю.

4. Охорона прав і свобод – порушення прав та свобод, які є частиною інформаційної безпеки у міжнародному контексті, вимагає більш ефективних стратегій інформаційного контролю та захисту.

Усі ці аспекти відображають нові виклики, які необхідно враховувати при розробці інформаційної безпеки, щоб забезпечити відповідний захист інформаційних ресурсів та збереження основних цінностей та свобод у міжнародному вимірі.

У результаті дослідження нами виявлено появу нових понятєвих категорій міжнародної інформаційної безпеки, що з’являються у контексті сучасних реалій. Серед них:

Кліктивізм – це поняття, що описує використання соціальних мереж та інших інтернет-інструментів для просування будь-якої діяльності чи процесу, зокрема для політичної агітації.

Хактивізм – це активна участь осіб у соціальних мережах та в Інтернеті задля впливу на політичні процеси або громадські справи, часто пов’язана із хакерською діяльністю.

Тролінг – це діяльність людей, які свідомо створюють конфлікти у соціальних мережах через провокаційні коментарі чи повідомлення.

Ботоферми та бот-мережі – терміни, що вказують на масштабне використання ботів у соціальних мережах для підвищення впливу, ретельного контролю дискусій або розповсюдження дезінформації.

Квантум-безпека – застосування квантових технологій для захисту інформації від кіберзагроз.

Covid-безпека – категорія, що виникла під час пандемії COVID-19 і стосується заходів безпеки в інформаційному просторі щодо поширення дезінформації та впливу на громадську думку під час пандемії.

Обґрунтування цих новітніх категорій має важливе значення для формулювання міжнародних стратегій захисту інформаційної безпеки в умовах сучасного інформаційного середовища.

РОЗДІЛ 2
СТРАТЕГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЧАСНИКІВ МІЖНАРОДНИХ ЕКОНОМІЧНИХ ВІДНОСИН

2.1. Роль міжнародних організацій у формуванні та реалізації стратегій міжнародної інформаційної безпеки

У сучасному світі міжнародні організації переглядають свою політику та підходи до забезпечення міжнародної інформаційної безпеки. Зміна вектору безпекових загроз, зокрема інформаційних загроз, вимагає переосмислення традиційних стратегій та розробки нових підходів до забезпечення стабільності та захисту.

Зокрема, на сьогоднішній день, міжнародні організації активно співпрацюють для боротьби з інформаційними ризиками. Вони спільно виробляють стратегії та політику, оскільки інформаційна безпека стає ключовим аспектом міжнародних відносин. Розвиток інформаційних технологій і поширення цифрового простору підвищили необхідність координації зусиль міжнародної спільноти у цій сфері.

Зростання потенційних загроз, пов’язаних із використанням інформаційних технологій подвійного призначення, стимулює необхідність узгодженого міжнародного підходу до їх контролю та регулювання. Країни та міжнародні організації зосереджують увагу на розробці спільних стратегій, які сприятимуть попередженню негативних наслідків використання таких технологій для воєнних цілей та інших загроз.

Міжнародне співробітництво у сфері інформаційної безпеки вимагає не лише реактивних заходів, а й активного планування, співпраці та розробки стратегій, які б враховували швидкоплинний розвиток технологій та варіативність загроз.

Так, сучасна діджиталізація економіки та розвиток інноваційних технологій значно змінюють парадигму міжнародних відносин і вимагають від урядових і неурядових міжнародних організацій адаптації до нових умов. Ця модернізація включає реагування на виклики, пов’язані із цифровою трансформацією економіки та державного управління, а також зі змінами в міжнародній безпеці, включаючи гібридні конфлікти з використанням інформаційних технологій і психологічного впливу.

Організації, які займаються міжнародними відносинами та безпекою, активно працюють над адаптацією до цих нових реалій. Вони розробляють стратегії та механізми реагування на загрози, вдосконалюють методи захисту інформації, сприяють регулюванню та розвитку стандартів у кіберпросторі.

Зростання кількості гібридних конфліктів, в яких інформаційні технології грають значну роль, також змушує ці організації працювати над вдосконаленням методів виявлення, аналізу та відповіді на такі загрози. Тому сучасні міжнародні урядові та неурядові організації активно розвивають свою стратегію, щоб ефективно протидіяти новим викликам у сфері інформаційної безпеки [46].

Так, багато визначних зарубіжних експертів та дослідників звертали увагу на проблеми інформаційної безпеки у міжнародному контексті [47–51]. Вони розробляли концепції сили у міжнародних відносинах, теорії інформаційних вій нового покоління та проводили аналіз практики використання інформаційних озброєнь у міжнародних конфліктах. Ці дослідники активно вивчали характеристики інформаційної безпеки, розробляли визначення цього поняття, а також проводили аналіз трендів міжнародного співробітництва у сфері інформаційної безпеки на рівні міжнародних організацій та в провідних державах світу. Зазначені вчені також зосереджували увагу на інституційних засадах міжнародної інформаційної безпеки, розглядали міжнародні механізми протидії інформаційним викликам для системи міжнародної безпеки та вивчали способи захисту від таких загроз. Їх дослідження та аналіз стали важливим доповненням до загального

розуміння інформаційної безпеки в контексті міжнародних відносин та глобальної безпеки.

Справді, сучасні виклики у сфері інформаційної безпеки вимагають інтегрованих підходів та спільних зусиль від міжнародного співтовариства. Міжнародні організації, такі як ООН, НАТО, ОБСЄ та інші, грають ключову роль у формуванні інформаційної безпеки і співпраці в цій області.

На рівні міжнародних безпекових організацій приймаються рішення, спрямовані на забезпечення безпеки та стабільності в умовах постійно зростаючих інформаційних загроз. Ці рішення базуються на принципах міжнародного права та спільних цілях усіх учасників. Вони визначають стратегії, спільні ініціативи та механізми відповіді на сучасні загрози і виклики, пов’язані із інформаційною безпекою.

Шляхом широкого представництва та урахування позицій та інтересів різних міжнародних акторів, ці організації працюють над створенням механізмів, спрямованих на спільні дії для забезпечення інформаційної безпеки у всесвітньому масштабі. Такий підхід сприяє вирішенню проблем у сфері інформаційної безпеки та сприяє підтриманню миру й стабільності в міжнародному співтоваристві.

Варто зазначити, що експертами було визначено важливі питання та напрямки у сфері міжнародної інформаційної безпеки через обговорення на сесіях Генеральної Асамблеї ООН. Резолюції «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» і «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки» створили основу для обговорення важливих аспектів, які визначають сучасну політику інформаційної безпеки. Ці резолюції містили положення про подвійне використання інформаційно-комунікаційних технологій у цивільній і воєнній сферах, використання досягнень науки і техніки у модернізації сучасних озброєнь, а також важливість протидії деструктивним впливам. Це свідчить про усвідомлення необхідності розвитку міжнародних стандартів інформаційної безпеки та застосування сучасних технологій з метою

забезпечення стабільності та безпеки. Такі документи [52] відображають визнання важливості спільних зусиль держав, приватного сектору, наукових установ і громадянського суспільства для досягнення мети підвищення ефективності міжнародного співробітництва в сфері інформаційної безпеки. ООН, через обговорення таких питань, узагальнює спільні підходи та стратегії, які можуть служити основою для подальших дій у цій області.

Обговорення проекту Конвенції про міжнародну інформаційну безпеку на сесії Генеральної Асамблеї ООН відобразило різні погляди держав на визначення понять, оцінку потенційних інформаційних загроз та організаційне забезпечення міжнародного співробітництва у цій сфері.

Для досягнення консенсусу стосовно формулювання Конвенції була створена Група урядових експертів. Її завданням було проведення компетентного аналізу проблем інформаційної безпеки, розроблення міжнародних принципів регулювання комунікаційних мереж, зокрема врахування того, що інноваційні технології можуть бути використані для атак на базові системи держав і громад.

Проте, конкуренція між підходами різних країн до базових принципів конвенції стала причиною її несхвалення та перенесення дискусії на подальше майбутнє. Різні погляди на те, яким чином повинна регулюватися міжнародна інформаційна безпека, ускладнили процес узгодження тексту конвенції [53].

Резолюція «Заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки» [54], ухвалена на сесії Генеральної Асамблеї ООН за підтримки більшості держав-членів, відображає необхідність створення безпечного, стабільного та мирного інформаційно-комунікаційного середовища в кіберпросторі. Ця резолюція визначає, що установлення довірчих відносин між державами в кіберпросторі є важливою умовою для забезпечення міжнародної безпеки. Також акцентується на потребі розширення можливостей держав для співпраці та використання високих технологій для зменшення ризику виникнення конфліктів у кіберсфері.

Ця резолюція також визначає, що хоча відповідальність за забезпечення безпеки в кіберпросторі лежить на державах, участь приватного сектору, наукових установ та громадянського суспільства може сприяти ефективнішому міжнародному співробітництву.

У контексті цієї резолюції на рівні ООН було створено новий формат Групи урядових експертів, з урахуванням географічного представництва держав [55]. Ця група може внести значний внесок у зміцнення міжнародної інформаційної безпеки через розробку рекомендацій та встановлення механізмів для заохочення відповідальної поведінки держав у кіберпросторі.

Так, НАТО визначила кіберпростір як ключове середовище для інформаційного протиборства і надає великий пріоритет інформаційній безпеці. Організація створила передові центри НАТО у своїх країнах-членах, що є багатонаціональними інститутами для розробки стратегій інформаційної безпеки та сприяння міждержавній взаємодії у цій сфері.

Центр інформаційної безпеки НАТО, заснований в Естонії, виник за ініціативою естонських влад і перших країн-спонсорів. Він не входить до складу військового командування або структури збройних сил НАТО. Замість цього, його персонал і фінансування забезпечуються державами-спонсорами та державами-членами організації. Цей Центр має важливе значення для обміну досвідом інформаційного захисту, розробки та впровадження стратегій протидії інформаційним загрозам, а також співпраці з іншими організаціями, такими як Європейська оборонна агенція та Дослідницький центр кібербезпеки в Німеччині [56].

Так, експерти Центру спільно з Організацією Червоного Хреста та кібернетичним командуванням США представили документи «Керівні принципи міжнародного права, що можуть застосовуватись під час кібервійни» і «Талліннські керівні принципи 2.0». Ці документи є базовими засадами щодо ведення інформаційної війни і відповідають положенням сучасного міжнародного права, що регулює операції у інформаційному просторі.

Документи визначають, що країни, що здійснюють інформаційні атаки, несуть відповідальність за свої дії проти інших держав. Вони закликають до заборони застосування сили в інформаційному просторі, оскільки інформаційні атаки можуть призвести до руйнування інфраструктури, цифрових даних та систем життєзабезпечення держав і впливати на цивільне населення, що може бути визнано військовими злочинами.

Така класифікація інформаційної війни як «збройних конфліктів» визнає застосування контрзаходів у відповідь на кібератаки як законні. Проте варто підкреслити, що доповідь експертів є незалежною думкою авторів і, на відміну від офіційних документів НАТО, має рекомендаційний характер [57].

Аналіз політики інформаційної безпеки НАТО свідчить про ініціативу Естонії як держави-члена НАТО у співпраці з країнами-учасницями Програми Східного партнерства, зокрема з Україною та Грузією, у сфері інформаційної безпеки. Спільні заходи, які були запроваджені, охоплювали підготовку персоналу, технічні консультації та постачання обладнання для боротьби з інформаційними загрозами.

В умовах повномасштабного вторгнення РФ в Україну, а також під час конфлікту на Сході України та незаконної окупації Криму, міністр оборони Естонії закликав партнерів по НАТО надавати фінансову допомогу Україні у контексті агресивних кібератак РФ щодо України. Естонія також передала 100 тис. євро у трастовий фонд НАТО для підтримки інформаційної безпеки України та організувала навчання українських фахівців з кіберзахисту.

Важливо відзначити, що Україна може стати важливим партнером у співпраці із Центром через свій досвід протидії російським кіберзагрозам і негативному інформаційному впливу, що становить загрозу не лише для демократичних процесів у європейському регіоні, але й на міжнародному рівні.

Приєднання України до ініціативи «Партнерства розширених можливостей НАТО» є важливим кроком, спрямованим на розширення взаємодії з НАТО у сфері інформаційної безпеки. Це може виявитися

корисним під час вирішення кризових ситуацій і здійснення миротворчих місій.

В рамках програми розширеного партнерства Україна матиме можливість забезпечувати оперативне планування на ранніх стадіях конфліктів, розширити діалог у сфері обміну розвідувальною інформацією, у тому числі й щодо попередження кібератак. Також Україна зможе брати участь у навчаннях з кібероборони, передбачених для учасників програми, а також отримувати посади у Міжнародному військовому штабі НАТО та інших командних структурах альянсу для набуття досвіду управління у сфері інформаційної безпеки [58].

Співпраця України з НАТО в рамках Комплексного пакету допомоги є важливим кроком для покращення стандартів військово-політичної організації в країні. Цей пакет допомоги включає підтримку через трастові фонди та реалізацію Річної національної програми, яка є інструментом для впровадження реформ.

У рамках цього практичного співробітництва було прийнято Указ про затвердження Річної національної програми під егідою Комісії Україна – НАТО на 2022 рік. Крім цього, був ухвалений План заходів щодо реалізації Концепції вдосконалення інформування громадськості з питань євроатлантичної інтеграції України. Ці ініціативи включають роботу спільних робочих груп Україна-НАТО з питань воєнної реформи, оборонно-технічного співробітництва та інформаційної безпеки, а також співпрацю з питань науки і довкілля [59].

ОБСЄ (Організація з безпеки та співробітництва в Європі) є важливим форумом для обговорення сучасних проблем безпеки в Європі, Північній Америці та незалежних державах, що виникли після розпаду СРСР. Початково ця організація була створена для підтримки безпеки, прав людини, демократії та розвитку медіа в зонах збройних конфліктів, а також для спостереження за розвитком кризових ситуацій.

З появою гібридних конфліктів, де спеціальні інформаційні операції та деструктивні інформаційно-психологічні впливи стали невід'ємною частиною, модернізація політики ОБСЄ стала нагальною. Організація розглядає пропозиції щодо корекції своїх пріоритетів у сфері міжнародної інформаційної безпеки, серед яких визначення понять у цій галузі, створення ефективних механізмів попередження загроз, дотримання міжнародного права у сфері інформаційних загроз, системи виявлення джерел таких загроз, а також координація міжнародних зусиль для захисту Інтернет-мережі та підвищення довіри до глобальної інформаційної інфраструктури.

Організація ОБСЄ підкреслює важливість інформаційних загроз у сучасному світі. Вона закликала всіх зацікавлених сторін до пошуку рішень у сфері інформаційної безпеки та досягнення загального та ефективного регулювання кіберпростору на основі міжнародного права [60].

Конференція «Загальний підхід до кібербезпеки: визначення майбутньої ролі ОБСЄ» [61], стала важливим кроком у визначенні стратегії ОБСЄ щодо інформаційної безпеки. На цій конференції обговорювалися проблеми протиправного використання кіберпростору, а також аналізувалися відповідні контрзаходи міжнародних та регіональних організацій, зокрема їх вплив на безпеку в регіоні ОБСЄ. Основні теми конференції включали в себе потенціал ОБСЄ у розробці всеосяжного підходу до інформаційної безпеки, обмін досвідом між країнами регіону, створення норм і правил для регулювання поведінки держав у кіберпросторі, а також прийняття рішень для зміцнення інформаційної безпеки в регіоні.

В результаті роботи конференції були прийняті інноваційні рекомендації щодо заходів щодо зміцнення довіри у сфері інформаційної безпеки. Ці рекомендації передбачали взаємодію ОБСЄ з приватним сектором та провайдерами ключової інфраструктури, спільні підходи до управління інформаційною безпекою, спрямовані на підвищення прозорості та забезпечення інформаційної безпеки в ОБСЄ.

Зусилля ОБСЄ у проведенні інтерактивних дискусій виявилися ключовими для розгляду питань, які стосуються багатосторонньої кібердипломатії, розвитку регіональної інформаційної безпеки як стимулюючої сили глобального прогресу, впливу штучного інтелекту на безпеку інформаційно-комунікаційних технологій та захисту критичної інфраструктури. Конференція акцентувала увагу на тому, що інформаційно-комунікаційні технології стали визначальним фактором економічного та соціального прогресу в сучасному світі, відкривши нові можливості у міжнародних відносинах. Однак, загрози у кіберпросторі спричинили потенційне наростання напруженості між державами через неправомірне використання мереж, кібератаки і порушення конфіденційності.

Члени ОБСЄ акцентували увагу на потребі розроблення довіри між державами-учасницями для зменшення ризиків конфліктів, пов’язаних із використанням інформаційно-комунікаційних технологій [62]. Проактивний підхід організації міг би включати дослідницькі проекти, аналітичні експертні оцінки та спеціалізовані програми, що мали б на меті конкретизувати проблематику політики інформаційної безпеки на платформі ОБСЄ.

Підсумовуючи аналіз діяльності міжнародних організацій у сфері інформаційної безпеки, важливо відзначити, що їхні можливості полягають у спроможності сприяти багатосторонньому діалогу між міжнародними учасниками, ураховувати різноманітні позиції різних суб’єктів глобального управління та діяти як універсальні міжнародні платформи для узгодження поглядів у вирішенні актуальних питань безпеки.

Основною проблемою є забезпечення інформаційної безпеки на різних рівнях – міжнародному, субрегіональному, трансатлантичному та регіональному. Це стосується прагнень окремих світових акторів контролювати політичні процеси на значних територіях за допомогою спеціальних інформаційних операцій. Такий підхід управління створює проблеми інформаційного дисбалансу сил і може призвести до порушень

національного інформаційного суверенітету, що спостерігається в Україні в умовах повномасштабного вторгнення РФ.

Розуміння цих проблем і їх розв'язання вимагає спільних зусиль і співпраці на міжнародному рівні, з метою розробки норм та стратегій, спрямованих на забезпечення безпеки у цифровому середовищі та захисту національного суверенітету в цьому новому інформаційному ландшафті.

Так, змішання глобальних та регіональних проблем значно впливає на роль і можливості міжнародних інститутів у визначенні напрямків змін на глобальному рівні. Це спонукає ці організації залучати потужні механізми для вирішення проблем, що стосуються світового розвитку.

Одночасно гібридний характер інформаційних впливів призвів до зміни підходів міжнародних організацій до політики в сфері інформаційної безпеки. Це вимагає формування нових структур і стратегій для ефективного протистояння сучасним викликам, спрямованим на забезпечення безпеки та стабільності. Такі організації повинні адаптуватися до мінливого інформаційного середовища та виробляти інноваційні стратегії, спрямовані на захист від нових загроз, що виникають у цифровому просторі.

2.2. Основні напрями діяльності провідних європейських країн у сфері інформаційної безпеки

Політика інформаційної безпеки в Європейському союзі (ЄС) відображається через використання передових технологій, таких як цифрові та квантові технології, системи штучного інтелекту, а також вдосконалення інформаційного озброєння. Ця політика також ставить перед собою завдання використовувати комунікативний інструментарій та протидіяти деструктивним інформаційно-психологічним впливам у геополітичному протистоянні міжнародних акторів.

Експертні розвідки зазначають [63], що політика інформаційної безпеки в Європі визначається рішеннями та програмними документами інтеграційного об’єднання, а також національними стратегіями країн Європи з великим економічним, науковим і технічним потенціалом і геополітичним впливом, такими як Франція та Німеччина. Особливо важливою стає реакція на нові виклики у сфері інформаційної безпеки, що виникають у зв’язку зі зміною тенденцій у регіональній безпеці.

Сучасні стратегії інформаційної безпеки ЄС та провідних країн Європи мають на меті захист інформаційного суверенітету держав та протидію новим інформаційним загрозам. Реформування національних стратегій забезпечення інформаційної безпеки стає необхідним у зв’язку зі зростаючою турбулентністю міжнародного інформаційного середовища та широким впровадженням інноваційних технологій у сфери захисту критичної інфраструктури.

Політика інформаційної безпеки в провідних європейських країнах, таких як Велика Британія, Франція та Федеративна Республіка Німеччина, ставить перед собою завдання захисту критично важливих секторів життєзабезпечення та протидії зовнішнім інформаційним загрозам, таким як інформаційно-психологічні операції, інформаційний тероризм, кіберзлочинність та деструктивні інформаційні впливи.

Вирішення таких проблем потребує покращення координації між наднаціональними інститутами ЄС та країн-членів, а також розроблення спільних стратегій для боротьби з кіберзлочинністю та ворожою пропагандою. Ці заходи повинні сприйматися європейською громадськістю як стратегічний інтерес у зміцненні оборонного потенціалу та реформуванні механізмів європейської колективної безпеки, з урахуванням національних пріоритетів.

Ця політика інформаційної безпеки вважається стратегічною парадигмою, що стосується всіх сегментів суспільства. Вона сприяє забезпеченню інформаційної незалежності, надійності національної інформаційної інфраструктури, конфіденційності інформаційних даних і

приватності. Ця модель може стати прикладом для інших міжнародних акторів у розвитку системи інформаційної безпеки. Наприклад, Україна може врахувати цей досвід, оскільки країна в умовах повномасштабного воєнного вторгнення стикається із загрозами інформаційної безпеки.

Дійсно, сучасні дослідження в області інформаційної безпеки європейських країн зосереджені на аналізі доктрин та практики, що застосовуються у цій сфері. Особлива увага приділяється захисту конфіденційності інформаційних ресурсів, а також проблемам, які виникають у контексті державно-приватного партнерства у сфері інформаційної безпеки.

Дослідження підкреслюють [64], що знайдені закономірності та проблеми підтверджують наявність суперечностей у політиці інформаційної безпеки в сучасних міжнародних відносинах. Експерти роблять акцент на тому, що національні стратегії інформаційної безпеки повинні враховувати динамічні зміни у політичній реальності, розвиток концепцій сили у міжнародних відносинах, а також впровадження механізмів для забезпечення національної інформаційної безпеки як складової зовнішньої та безпекової політики.

Аналіз інформаційної безпеки, представлений дослідниками RAND Corporation [65], вказує на загальні тенденції у сфері безпеки, які можуть мати вплив на міжнародну взаємодію і виникнення інформаційних загроз нового типу. Оскільки такі дослідження розглядаються як важливі для політичних лідерів та експертів різних країн, уряди європейських країн роблять певні зміни у національних стратегіях з інформаційної безпеки для адаптації до цих тенденцій.

В рамках цього дослідження головною проблемою інформаційної безпеки у міжнародному контексті визнано потенційні порушення конфіденційності інформаційних ресурсів державного, корпоративного та приватного характеру. Ці порушення можуть призвести до значного впливу на функціонування критичної інфраструктури, порушень стандартів правового

захисту інформаційної безпеки, пониження захищеності урядової інформації, яка використовується для прийняття керівних рішень.

Такі тенденції відображають зміну підходів Європейського союзу до формування політики інформаційної безпеки на регіональному та національному рівнях. Ці зміни охоплюють переосмислення та оновлення практичних механізмів безпекової політики з метою протидії поширенню інформаційних загроз. Особлива увага приділяється визначенню пріоритетів у сфері регіональної та національної інформаційної безпеки.

Наприклад, Європейська стратегія зовнішньої та безпекової політики [66], включала положення щодо принципів взаємодії у секторі спільної безпеки і оборони. Водночас, конкретні цілі та заходи у сфері інформаційної безпеки визначаються у програмах та робочих планах наднаціональних інститутів ЄС. Ці програми передбачають формулювання спільних рішень між Європейським союзом та європейськими країнами щодо забезпечення європейської інформаційної безпеки.

Крім того, була укладена Угода ЄС з промисловою індустрією щодо інформаційної безпеки та активізації зусиль для протидії інформаційним загрозам [67], а також запроваджено План дій в галузі інформаційної безпеки для інтенсифікації протидії інформаційним загрозам у рамках програми державно-приватного партнерства.

Дослідження глобального стану інформаційної безпеки [68] відзначало, що інформаційна безпека, конфіденційність даних та етика є більш взаємопов’язаними аспектами, що потребують ефективного управління інформаційними ризиками. У цьому контексті компанія Pricewaterhouse Coopers розробила нову платформу для інформаційної безпеки та конфіденційності, спрямовану на захист від загроз, реалізацію трансформаційних процесів та досягнення зростання. Ця нова платформа має спрямовуватися на поєднання заходів з інформаційної безпеки та засобів захисту конфіденційності даних. Це може включати застосування передових технологій шифрування, захист від кібератак, контроль доступу до даних та

інші ініціативи з метою запобігання порушенням конфіденційності та забезпечення безпеки даних. Такі інструменти та платформи [69] важливі для бізнесу та організацій, оскільки допомагають управляти та зменшувати ризики в сфері інформаційної безпеки, яка постійно стає складнішою через швидкі зміни технологій та виклики цифрового світу.

Європейське агентство з мережевої та інформаційної безпеки (ENISA) відіграє ключову роль у координації безпекового співробітництва між Європейським Союзом та країнами Європи на рівні мережевої та інформаційної безпеки [70]. Це агентство було створене з метою забезпечення ефективного захисту інформаційного суверенітету та інформаційної інфраструктури країн Європи, а також для сприяння розвитку відносин між ЄС та представниками інформаційної індустрії та приватного сектору.

Низка країн, таких як Німеччина, Франція та Велика Британія, співпрацюють з ENISA, зосереджуючи увагу на національних стратегіях інформаційної безпеки. Наприклад, уряд ФРН ухвалив «Національний план захисту інформаційної інфраструктури», співпрацюючи з ENISA, щоб забезпечити відкритість кіберпростору та захист інформаційних ресурсів в мережевому середовищі як на національному, так і на міжнародному рівнях. Франція також спрямовує свою практику інформаційної безпеки на застосування технічних засобів захисту інформації від кіберзлочинності та інформаційного тероризму, відповідно до принципів ENISA.

Співпраця з ENISA також стимулює розвиток інформаційної безпеки у Великій Британії, допомагаючи у впровадженні інновацій, залученні інвестицій та покращенні якості сервісів у сфері інформаційно-комунікаційних технологій. Ці зусилля спрямовані на запобігання кібератакам злочинних і терористичних угруповань та створення більш безпечного інформаційного простору.

Агентство ENISA вирішило підтримати співпрацю країн Європи у боротьбі з універсальними загрозами інформаційної безпеки. Для цього був розроблений спеціальний практикум [71], спрямований на формування

національної політики інформаційної безпеки для країн Європи. Цей практикум включає короткий аналіз поточного стану стратегій, які використовуються європейськими країнами в сфері інформаційної безпеки. Такий аналіз спрямований на ідентифікацію загальних рис і відмінностей між національними стратегіями, що допомагає у зрозумінні найкращих практик та недоліків. Крім того, у цьому практикумі висунуто рекомендації стосовно впровадження стратегій інформаційної безпеки у країнах Європи. Ці рекомендації можуть містити конкретні заходи, які країни можуть прийняти для підвищення ефективності своїх заходів і захисту від загроз у сфері інформаційної безпеки. Окрім цього, вони можуть включати стратегічні підходи до превентивних заходів та реагування на потенційні загрози, що сприяє покращенню загального рівня безпеки.

Загальний регламент про захист персональних даних ЄС, відомий як GDPR, став чинним з 2018 р. Це важливий законодавчий акт, який уніфікує та регулює захист всіх персональних даних в Європейському Союзі. Він розроблений з метою забезпечення більш високого рівня захисту приватності та контролю над власними даними громадянами. Згідно з опитуваннями, проведеними Європейським комісаріатом [72], виявлено, що після прийняття GDPR більше двох третин опитаних (67%) були інформовані про існування цього регламенту. Проте лише 36% з цих осіб знали про його зміст, тоді як 31% знавали про документ, але не були ознайомлені з конкретними його положеннями чи вмістом. Ці дані свідчать про те, що, хоча рівень обізнаності щодо існування GDPR серед опитаних є досить високим, знання про конкретний зміст цього регламенту залишається меншим, що може потребувати додаткової освіти.

Останнім часом деструктивна пропаганда авторитарних держав, вірусні фейки та спрямована дезінформація стали серйозними загрозами для інформаційної безпеки Європейського Союзу та європейських країн. У зв’язку з цим на рівні ЄС було ухвалено рішення щодо посилення протидії агресивній пропаганді [73], зокрема російській, а також на рівні окремих європейських

країн були створені спеціальні установи й підрозділи для боротьби з цими загрозами.

Наприклад, у Великій Британії заходи з протидії ворожим пропагандистським впливам віднесено до повноважень Національного підрозділу Ради національної безпеки; у Франції такі заходи здійснюють спеціальні державні та законодавчі інституції; у ФРН запроваджено програми для боротьби з фейковою інформацією. Координація дій ЄС і європейських країн у боротьбі з ворожою пропагандою розглядається як стратегічний інтерес організації, оскільки це підтверджує її статус як міжнародного актора на рівні європейської інформаційної безпеки.

Європейські стандарти інформаційної безпеки підтримуються всіма державами-членами ЄС, що свідчить про спільні підходи до критеріїв оцінки інформаційних загроз. Однак, варто відзначити, що диференціація у підходах провідних європейських країн виявляється через їхні власні національні пріоритети в сфері безпекової політики.

Стратегія інформаційної безпеки Великої Британії враховує як міжнародні, так і національні інтереси держави у формуванні системи захисту від сучасних інформаційних загроз. У програмному документі «Стратегія національної безпеки» [74] визначено, що серед критичних викликів для безпеки Великої Британії виділяються кібератаки з боку інших держав, злочинних та екстремістських угруповань, кібершпигунство і хакерство щодо критично важливої інфраструктури, що розглядаються як найбільші загрози для безпеки країни в цілому.

Стратегія інформаційної безпеки, оголошена британським урядом, передбачала реалізацію таких проектів, як створення громадських/приватних «хабів» з інформаційної безпеки, що дозволяють урядовому і приватному секторам обмінюватися інформацією про інформаційні загрози і протидіяти кібератакам. Основні принципи Стратегії також передбачали створення підрозділу кіберфахівців для протидії інформаційній злочинності та використання чинних санкцій у відношенні до інформаційних злочинів.

Для Франції поняття «цифровий суверенітет» є ключовим у пріоритетах інформаційної безпеки. Це означає здатність держави самостійно приймати рішення з охорони національної безпеки, інформаційної інфраструктури та інформаційного середовища країни [75]. Відмітимо, що наявність постійного впливу проросійської пропаганди та зовнішнього маніпулювання масовою свідомістю громадськості Франції створює загрозу для інформаційної безпеки урядових інститутів та суспільства.

Серед інших важливих впливів особливу увагу приділяють кіберзагрозам. Кіберзлочинність, інтернет-шпигунство та хакерські атаки на інфраструктурні об’єкти розглядаються як напади на критично важливі сфери життєдіяльності країни, які потребують правового оформлення в рамках національного законодавства.

Франція реалізувала кардинальні зміни в безпеці та оборонній політиці в рамках безпекової доктрини. У стратегічних документах інформаційна безпека була визначена як один із головних пріоритетів національної безпеки країни, що підтверджує її постійну модернізацію і зосередженість на цій проблемі.

Агентство ANSSI (Agence nationale de la sécurité des systèmes d'information) [76], створене у 2009 р., перетворилося на важливе загальнонаціональне відомство Франції щодо захисту інформаційних систем та критичної інфраструктури. У Міністерстві оборони було сформовано Генеральний директорат з інформаційного захисту, який ініціював ухвалення стратегії інформаційної безпеки країни. Ця стратегія підтверджувала використання досвіду інших європейських країн у створенні національної системи інформаційного захисту, зокрема на основі резервних мереж. Документ також визначав підтримку проектів державно-приватного партнерства у сфері інформаційної безпеки, які залучали державні органи, великі промислові корпорації, приватний сектор, науково-дослідницькі та освітні установи.

Основні сектори інформаційної сфери, що потребують державного захисту, визнавалися системами інформації обмеженого користування, інформаційними ресурсами державної таємниці та спеціальними урядовими і військовими телекомунікаціями. Аналіз оцінок фахівців вказував на сприйняття загрози інформаційної або глобальної інформаційної війни в експертному середовищі як на реальну. Однак, такі висновки були нівельовані інерційністю системи військових витрат і недостатнім усвідомленням політичними чиновниками всіх можливостей інформаційних озброєнь, які виходять за рамки традиційних засобів захисту інформаційних ресурсів.

Розвиток доктрини і практики інформаційної безпеки у Франції був спрямований на впровадження французької національної цифрової стратегії [77]. В цій стратегії визначалися ключові цілі, які включали безпеку національних інформаційних систем та критично важливої інфраструктури, захист конфіденційності приватного життя та персональних даних громадян у мережі Інтернет, підтримку французьких компаній, які працюють у секторі цифрових продуктів та послуг, а також зміцнення впливу Франції у міжнародних організаціях через програми інформаційної безпеки для найменш захищених країн та загальну підтримку стабілізації кіберпростору.

Для забезпечення інформаційного захисту Франції планувалося збільшити чисельність співробітників французького Агентства з мережевої та інформаційної безпеки, а також Міністерств оборони і внутрішніх справ. Також планувалося зміцнити безпеку суспільно важливих недержавних інформаційних систем, підтримати французькі організації, що розробляють системи виявлення і захисту від кібератак для малих і середніх компаній. Це свідчить про спрямованість Франції на посилення заходів у сфері інформаційної безпеки та підтримку власних інформаційних ресурсів у цифровому середовищі.

Так, кібертероризм виявляється серйозною загрозою для інформаційної безпеки Франції. Злочинні організації та терористичні групи активно

використовують веб-сайти для поширення пропаганди, вербування нових членів, фінансування та планування терористичних акцій.

Ця пропаганда може включати в себе різноманітні методи, які спрямовані на вплив на громадськість Франції. Такі організації використовують мас-медіа для висвітлення терактів, захоплення заручників та реакції влади на заяви терористичних угруповань. Це може призвести до поширення негативної інформації та збільшення впливу терористичних груп у медіа-середовищі країни.

Державні структури Франції повинні активно співпрацювати з медіа та іншими відповідальними органами для моніторингу та контролю цих процесів. Важливо вживати заходи для запобігання розповсюдженню та реагування на такі випадки, щоб зменшити вплив терористичних організацій у цифровому інформаційному просторі Франції.

Так, експерти з інформаційної безпеки в Франції розглядають не лише зовнішні фактори, що впливають на інформаційну інфраструктуру країни, а й внутрішні загрози, такі як деструктивна діяльність «фабрик тролів», «ботів» та гібридних воєн. Ці організації використовуються для поширення фейкових новин, маніпулювання громадською думкою та порушення інформаційної безпеки.

Фахівці в цій сфері рекомендують урядовим відомствам Франції створити централізований орган, який спеціалізуватиметься на боротьбі з фейковими новинами. Цей орган міг би здійснювати перевірку, спростування та недопущення поширення маніпулятивних повідомлень в інформаційне середовище країни. Він міг би використовувати інструменти та методи для виявлення та розкриття дезінформації та фейкових новин, щоб зменшити їх вплив на суспільство та інформаційну безпеку країни. Аналогічний досвід варто, на нашу думку, імплементувати в Україні, в умовах повномасштабного вторгнення РФ.

На 10-тій конференції Федерального відомства з питань захисту Конституції у Берліні, тематика обговорення була спрямована на широкий

спектр питань, пов’язаних з інформаційною безпекою та інформаційним суверенітетом держави. Деякі з ключових тем, які були висвітлені на конференції, включали [78]:

1. Відповідальність урядових структур за інформаційний суверенітет держави. Обговорення того, як урядові органи повинні брати на себе відповідальність за захист інформаційного суверенітету країни, включаючи розробку політики, законодавства та стратегій захисту.

2. Захист інфраструктури від несанкціонованого втручання і інформаційних загроз. Обговорення методів та стратегій захисту важливої інфраструктури від кіберзагроз, хакерських атак та несанкціонованого доступу.

3. Поширення дезінформації для впливу на суспільство. Розгляд аспектів дезінформації та її впливу на суспільство через мас-медіа та інші канали.

4. Формування системи державно-приватного партнерства у сфері інформаційної безпеки. Обговорення необхідності та методів співпраці між урядовими структурами та приватним сектором для захисту інформаційної безпеки.

5. Захист конфіденційності персональної інформації. Розгляд аспектів захисту приватної інформації громадян від кіберзагроз та незаконного доступу.

6. Діяльність мас-медіа в умовах зовнішніх інформаційно-психологічних та кібервпливів. Обговорення ролі та відповідальності медіа у засвоєнні та розповсюдженні інформації в умовах, коли існують зовнішні впливи, такі як інформаційно-психологічні та кібервпливи.

Ці теми відображають ключові аспекти, які стали предметом уваги на конференції, показуючи актуальні питання інформаційної безпеки та дискусії щодо заходів її забезпечення в Німеччині.

Обговорення в Німеччині підкреслювало важливість розробки та реалізації стратегій інформаційної безпеки, які мають на меті забезпечити інформаційний суверенітет країни в цифровому світі. Для цього урядові

інституції визначали потенційні кібератаки та їх можливий вплив на системи інформаційної безпеки, пропонуючи рішення для ухвалення керівних політичних рішень та їх втілення у концепції інформаційної безпеки.

Однією з ключових ідей було визначення цифрової стратегії як інструменту, що дозволяє максимально використовувати потенціал цифрових технологій для загального блага суспільства та одночасно запобігати ймовірним загрозам. Пріоритетними заходами в цій стратегії було забезпеченням ефективного використання сучасних інформаційних продуктів та стандартів безпеки, а також тісної співпраці та узгодженості дій щодо запобігання, виявлення та знешкодження кібератак.

Стратегія також передбачала формування цифрового та інформаційного середовища, яке було б стійким до загроз, спрямованих на дестабілізацію внутрішньої безпеки країни, з метою запобігання їхньому виникненню. Крім того, було відзначено, що всі відповідальні сектори суспільства, такі як держава, бізнес, наука та громадськість, мають спільну відповідальність за інформаційну безпеку країни.

Щодо міжнародної політики в сфері інформаційної безпеки, була підтверджена необхідність тісної співпраці з європейськими та міжнародними партнерами. Зазначимо, що відповідальність за забезпечення захисту кіберпростору Німеччини наразі лежить на Федеральному міністерстві оборони, Бундесвері та Федеральному міністерстві закордонних справ.

Моніторинг деструктивної інформаційної активності, особливо з Росії, відіграє важливу роль у забезпеченні інформаційної безпеки для європейських країн, зокрема для ФРН. Національний центр інформаційного захисту ФРН використовує такий моніторинг для виявлення потенційних загроз та запобіжних заходів урядових мереж та приватних компаній. Це дозволяє попереджати операторів критичної інфраструктури про можливість несанкціонованого втручання в їх функціонування.

Урядові документи ФРН свідчать про потребу у модернізації стратегії інформаційної безпеки, що відбиває реальні загрози та розвиток нових

спільних підходів. Ця модернізація визначає новий підхід до усвідомлення інформаційно-безпекових загроз, активно залучаючи державні та приватні структури, а також громадськість ФРН.

Один із головних аспектів цієї модернізації – це підвищення свідомості та ефективного менеджменту управління ризиками, що базується на аналізі та оцінці цих ризиків, з метою підвищення рівня безпеки інформаційних систем у всіх сферах діяльності, які піддаються інформаційним загрозам.

Діяльність, спрямована на використання фейкових новин та дезінформації, часто розглядається як один із інструментів гібридної війни, особливо в контексті протистояння російській пропаганді. Російські засоби масової інформації, намагаючись впливати на громадську думку, часто розповсюджують фейкові новини та спотворені факти, щоб формувати опозиційну громадськість або сприйняття фальшивої інформації як достовірної.

Ефективним засобом протидії такій пропаганді вважають створення якісних медіа для російськомовної меншини в Німеччині. Це може допомогти збалансувати інформацію, яку споживає ця частина суспільства, і запропонувати їм правдиві та об’єктивні джерела інформації.

Політика інформаційної безпеки стає ключовим елементом у боротьбі з такими загрозами, оскільки дезінформація може стати дуже небезпечним явищем для національної безпеки та психологічного стану суспільства. Агентства інформаційної безпеки, спільно з національними установами та відповідними державними та наддержавними організаціями за кордоном, повинні координувати дії щодо аналізу, спростування та контрпропаганди фейкових новин та дезінформації.

Інформаційна безпека стає все більш суттєвим викликом для багатьох країн, включаючи ФРН, через зростання використання цифрових технологій та їхній вплив на суспільство та політику. Відкритість інформаційного простору принесла багато позитивних аспектів, але вона також створила потенційні загрози та проблеми, зокрема в сфері інформаційної безпеки.

Сучасний світ, опираючись на інформаційні технології, відкриває шлях для впливу на економіку та суспільство. Це створює нові виклики для національної безпеки, оскільки інформаційні загрози та деструктивний вплив можуть швидко поширюватися та мати значний вплив на країну.

Німеччина, як і багато інших країн, змушена реагувати на ці виклики та розвивати ефективні стратегії інформаційної безпеки для захисту державних інтересів. Відкритість цифрового світу створює несприятливе середовище для можливих загроз, тому важливо реагувати на ці тенденції та підтримувати ініціативи, спрямовані на захист національної інформаційної безпеки.

2.3. Стратегічні напрями забезпечення інформаційної безпеки у США

Вплив та формування стратегій інформаційної безпеки Сполучених Штатів залежать від політичних та геополітичних позицій, які приймаються у кожній президентській адміністрації. Ці позиції відображаються в пріоритетах національних інтересів, положеннях зовнішньої політики та підходах до забезпечення безпеки країни.

Сполучені Штати зазвичай розвивають комплексні стратегії, які поєднують різні доктрини та стратегії безпекової політики відповідно до мети, яку слід досягти. Вони враховують такі аспекти, як міжнародна співпраця, дипломатичні зусилля, військові можливості та захист кіберпростору.

За останні роки зростає увага до інформаційної безпеки через поширення технологій та інтернету, тому стратегії безпеки тепер включають в себе значний компонент інформаційного захисту. США також активно співпрацюють з іншими країнами та міжнародними організаціями для забезпечення інформаційної безпеки в глобальному масштабі.

Останні події та виклики, такі як кібератаки, дезінформація та інформаційні втручання, стали стимулом для розвитку більш вдосконалених

стратегій інформаційної безпеки. Такі стратегії вимагають поєднання захисту критично важливої інфраструктури, попередження інформаційних загроз та розробки механізмів реагування на нові виклики у цифровому світі.

Так, інформаційна безпека – один із ключових аспектів у сучасному світі, що привертає увагу науковців, політологів та дослідників. Розвиток інформаційних технологій та їх вплив на різні аспекти життя суспільства, військовість і цивільні сфери, створює нові виклики та загрози, які необхідно ретельно аналізувати та прогнозувати.

Американські науковці та політологи [79–81], відіграють важливу роль у вивченні проблем інформаційної безпеки, розробці стратегій захисту, та аналізі наслідків використання інформаційних і комунікаційних технологій у сучасному світі. Вони вивчають еволюцію концепцій інформаційної безпеки, виокремлюють ключові підходи до використання різних форм впливу, розглядають зміни у безпеці як важливий фактор у формуванні міжнародних відносин та світового порядку. Ці дослідження сприяють розвитку стратегій та політик у галузі інформаційної безпеки, сприяють у формуванні більш обізнаного підходу до реагування на виклики, що виникають у сучасному інформаційному середовищі.

Справді, стратегії інформаційної безпеки в США еволюціонували протягом останніх десятиліть у контексті впливу на формування сучасної міжнародної системи. Застосування підходу «жорсткої сили» у міжнародних відносинах, тобто здатність держави впливати на політику інших країн через економічний та військовий тиск.

Нікколо Макіавеллі в своєму трактаті «Державець» та Гоббс у «Левіафані» розглядали «жорстку силу» як здатність впливати через військову та економічну силу. Моргентхау вважав «жорстку силу» певною формою політичної влади, а К. Грей розглядав її як здатність застосовувати військову силу у контексті політики XXI століття [82–83].

У сучасному світі інформаційна безпека стають ключовими складовими «жорсткої сили». Це включає в себе захист кіберпростору, використання

інформаційних засобів для досягнення впливу та забезпечення національних інтересів. Особливо у сфері кібербезпеки, військові загрози можуть відбуватися не лише у фізичному світі, а й у віртуальному просторі, через кібератаки та інші цифрові зловживання. Ці концепції важливі для розвитку стратегій безпеки США, оскільки зміни у світі вимагають адаптації політики інформаційної безпеки до нових викликів та загроз.

Так, в стратегії національної безпеки США [84], визначалися ключові напрямки адаптації американських військових сил до нових умов і викликів. Відбуваючись під час різкого розвитку технологій та змін у міжнародній ситуації, ця стратегія відображала потребу у відповіді на нові виклики та загрози. Зокрема, було визначено:

1. Розширення можливостей. Стратегія спрямовувалася на розширення військових можливостей за рамками звичайних стримувальних заходів, щоб відповідати новим ситуаціям та загрозам.

2. Національна спеціалізація. У цей період акцентувалася увага на розвитку оборонної сфери, включаючи ядерні, космічні та передові технології, які впливали на наступальні та оборонні програми.

3. Глобальна орієнтація. Стратегія передбачала перехід до меншого збройного складу, але більш глобально орієнтованого, що реагує на швидкоплинні зміни в інформаційних технологіях та враховує можливість непередбачуваних ситуацій.

Ці стратегічні кроки визначали напрямки для змін у військовій сфері з метою забезпечення адаптації до нових викликів, що стали актуальними в умовах стрімкого розвитку технологій та геополітичних змін.

Під час президентства Б. Обами було зосереджено увагу на посилення інформаційного фактору в стратегіях безпеки та оборони США. Інформаційні операції стали ключовим аспектом стратегічного впливу на міжнародні відносини, оскільки вони включали психологічні впливи, поширення дезінформації, кібератаки та електронні військові дії, спрямовані на знищення або нейтралізацію інформаційних систем супротивника [85]. В рамках цієї

стратегії, США вживали різні заходи проти країн, які були визнані агресивними у сфері інформаційної безпеки. Наприклад, були запроваджені санкції проти Росії та Північної Кореї, а також було засуджено хакерів з Китаю та Ірану. Домовленості між президентами США та Китаю про припинення комерційного хакерства також стали частиною цієї стратегії.

Крім того, було приділено значну увагу захисту критичної інфраструктури США, а також розроблено та вдосконалено системи захисту національних інформаційних мереж для запобігання та реагування на кібератаки та інші загрози цифрової безпеки.

Концепція «Більш розумна, більш безпечна Америка» [86–87], розроблена Центром американського прогресу, стала важливим визначенням стратегічних засад зовнішньої та безпекової політики президентської адміністрації Б. Обами. Ця концепція включала рекомендації, спрямовані на використання «розумної сили» в суперечці зі стратегією попередніх силових втручань. Вона акцентувала увагу на необхідності використання невійськових інструментів для захисту національних інтересів США на міжнародній арені.

Згідно з концепцією «розумної сили», Ф. Вонг-Діаз підкреслив, що ця стратегія не обмежувала дії США на міжнародній арені та не передбачала різкого скорочення військових витрат. Вона натомість стимулювала участь США у спільних діях для забезпечення міжнародної та національної безпеки, використовуючи високі технології для захисту держави і суспільства від потенційних інформаційних загроз.

В межах стратегії національної безпеки президента Б. Обами, проблема захисту кібермереж поруч із питаннями захисту від ядерних і біологічних загроз визнавалася як одна з ключових складових. Президент визначав кібернетичну безпеку як важливу складову національної безпеки та оборони США, підкреслюючи стратегічний характер інформаційної інфраструктури та цифрового простору як стратегічних національних активів, захист яких вважався пріоритетом національної безпеки.

Такий підхід визначав трансформацію інформаційної складової у стратегії національної безпеки США під час президентства Б. Обами, оновлюючи сприйняття кіберпростору як специфічної сфери захисту національних інтересів в умовах зростаючих міжнародних загроз.

Президент Б. Обама в своїй промові у військовій академії Вест-Пойнт ще у 2014 р. висловив необхідність нового підходу до принципів зовнішньої та безпекової політики США в контексті змін у світі. Ці зміни потребували нової моделі лідерства держави, яка враховувала актуальні геополітичні реалії та виклики.

У промові президента Б. Обами було підкреслено важливість реагування на агресію Росії проти України. Б. Обама та його адміністрація не згадували Будапештський меморандум, але підтримували Україну як ключового партнера для забезпечення безпеки в Європі та світі загалом. Вони висловили готовність надати Україні сильну політичну підтримку, а також допомогу у військовій та фінансовій сферах, спільно з Європейським Союзом, щоб підтримати реформи в Україні, боротьбу з корупцією та протистояти інформаційним загрозам.

Ця підтримка стала важливим кроком для України в її зусиллях зміцнення безпеки, а також у контексті захисту від інформаційних загроз. Президентство Б. Обами визначило участь США в підтримці України як частину стратегії зовнішньої політики, спрямованої на підтримку демократії та безпеки у регіоні.

Під час президентства Д. Трампа було прийнято Національну кіберстратегію Сполучених Штатів [88], яка визначила важливі пріоритети у сфері інформаційної безпеки. Одним із ключових аспектів стратегії стала охорона мереж, інформації та критичної інфраструктури від інформаційних загроз. Ця стратегія також передбачала боротьбу з кіберзлочинністю та реагування на кіберінциденти. США запровадили міжнародну ініціативу з кіберстримування, яка орієнтована на координацію і підтримку протидії серйозним кіберінцидентам у співпраці з іншими країнами-партнерами. Ця

ініціатива включала обмін розвідданими, підтвердження претензій стосовно кібератак, публічні заяви щодо підтримки проведених заходів і спільні дії для переслідування злочинців. У додаток до цього, стратегія визначала мету розширення американського впливу для забезпечення доступу до відкритого, надійного та безпечного Інтернету, а також нарощування міжнародного інформаційного потенціалу [89]. Ці кроки вказують на значимість інформаційної безпеки та важливість співпраці між державами для ефективного захисту інформаційного простору та боротьби з інформаційними загрозами.

Так, стратегії інформаційної безпеки США дійсно обумовлені спрямованістю інформаційних загроз на критично важливі структури функціонування держави. Розпізнання інформаційних технологій як нового виду глобальної зброї масового ураження стає важливим моментом у цьому контексті. Для забезпечення національної безпеки, США розвивають стратегії протидії та попередження інформаційної агресії, а також визнають необхідність підтримки механізмів для цього на рівні міжнародних та національних інституцій, які відповідають за питання безпеки і оборони.

Такі стратегії включають в себе розвиток імунітету від інформаційних загроз, зміцнення захисту критично важливої інфраструктури, вироблення ефективних механізмів реагування на кіберінциденти та протидії дезінформації. Розробка та впровадження таких стратегій є важливим елементом забезпечення стабільності та безпеки у державному, міжнародному та кібернетичному просторі.

Висновки до Розділу 2

Здійснений нами аналіз стратегій міжнародного співробітництва у сфері інформаційної безпеки підтверджує, що міжнародні організації перебувають у процесі модернізації своєї діяльності. Це визначається позиціями різних

міжнародних акторів, їх пріоритетами у забезпеченні інформаційної безпеки та рівнем розвитку їхньої інформаційної компетентності.

Гібридний характер інформаційних загроз спричинив потребу у створенні нових структур для більш ефективної протидії сучасним викликам. Міжнародні інститути, які відповідають за питання безпеки і оборони, реагують на ці виклики шляхом розробки і реалізації нових стратегій та механізмів співробітництва у сфері інформаційної безпеки. Вони розглядають інноваційний характер інформаційних загроз, а також працюють над забезпеченням відповідного рівня захисту та реагування на них.

Ця модернізація інституційного підходу до інформаційної безпеки у міжнародних рамках свідчить про постійне адаптування до нових викликів та загроз у цій сфері для забезпечення більш ефективного захисту інформаційних просторів та кіберінфраструктури.

Порівняльний аналіз політики інформаційної безпеки країн Європейського Союзу дійсно дозволяє виявити спільні та відмінні пріоритети в їх діяльності щодо захисту інформаційного суверенітету, критично важливої інфраструктури і суспільства загалом.

Спільними пріоритетами країн ЄС у сфері інформаційної безпеки є розробка та підтримка загальноєвропейських стратегій та підходів до захисту кіберпростору, використання стандартів та нормативно-правових актів, спрямованих на підвищення рівня інформаційної безпеки, а також співпраця та обмін інформацією між країнами для ефективного реагування на інформаційні загрози.

Проте, відмінності в політиці інформаційної безпеки ЄС визначаються пріоритетами окремих держав у забезпеченні національних інтересів. Деякі країни можуть акцентувати увагу на питаннях кібервійськової безпеки та реагування на інформаційні загрози з боку інших країн або неурядових суб’єктів, тоді як інші можуть більше зосереджуватися на захисті критичної інфраструктури чи боротьбі з кіберзлочинністю.

Отже, спільні пріоритети сприяють створенню загальноєвропейських стратегій, але відмінні характеристики враховують різні національні потреби та пріоритети держав в контексті захисту інформаційної безпеки.

Сучасні дослідження стратегій і практик інформаційної безпеки в США відображають складну концепцію зовнішньополітичного курсу країни та показують збіжність доктрин і стратегій безпеки з їх практичним використанням для досягнення цілей. Дослідження підтверджують поступальні зміни в сутності інформаційної безпеки як важливої складової національної безпеки. Під президентством Б. Обами була розроблена стратегія інформаційної безпеки, яка акцентувала увагу на політиці «розумної сили». Це означало використання науково-технологічних інновацій для ефективного впливу на міжнародний порядок та систему міжнародної безпеки. У свою чергу, національна стратегія Д. Трампа характеризувалася більш жорстким підходом і використанням «гострої сили».

Ці стратегії свідчать про різні підходи до досягнення національних цілей у сфері інформаційної безпеки та демонструють різноманітність інструментів, які використовує американська адміністрація для впливу на світову політику і безпеку.

РОЗДІЛ 3
СТРАТЕГІЧНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ В УМОВАХ ФУНКЦІОНУВАННЯ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

3.1. Засади інституціонального співробітництва України у сфері інформаційної безпеки

Удосконалення інституціональних засад політики інформаційної безпеки в Україні є критично важливим у контексті забезпечення захисту національних інтересів, суверенітету та національної безпеки. Низка заходів у цьому напрямку визначається наступними аспектами [90]:

1. Законодавство та нормативна база. Розвиток правового середовища є ключовим для створення ефективної системи інформаційної безпеки. Україна працює над створенням та удосконаленням законодавства, яке регулюватиме питання інформаційної безпеки, захисту персональних даних, боротьби з кіберзлочинністю та інші аспекти інформаційної безпеки.

2. Створення спеціалізованих органів. Формування спеціалізованих установ, агентств чи комітетів, відповідальних за здійснення політики інформаційної безпеки, які будуть відповідати за розробку стратегій, моніторинг, аналіз і реагування на інформаційні загрози.

3. Стандарти і практики безпеки. Розробка стандартів і практик безпеки для державних інституцій, бізнесу та громадян є важливою складовою створення безпечного інформаційного середовища.

4. Співпраця з міжнародними партнерами. Україна активно співпрацює з міжнародними організаціями та іншими державами для обміну досвідом і найкращими практиками в галузі інформаційної безпеки.

5. Освіта громадян. Важливим аспектом є підвищення рівня освіти щодо інформаційної безпеки серед населення, що допоможе усвідомити ризики та навчити заходам захисту.

Усі ці заходи спрямовані на створення системи інформаційної безпеки, яка не лише захищає державу від зовнішніх загроз, але й сприяє стабільності, економічному розвитку та забезпеченню прав громадян у цифровому світі.

У аналітичній розвідці А. Баровської «Структура керівних документів державної політики в інформаційній сфері: нагальні проблеми та шляхи впорядкування» [91] акцентується на важливості політико-правових документів, які регулюють інформаційну діяльність в Україні. Серед таких документів виокремлюються наступні:

1. Доктрини, концепції, стратегії та програми. Ці стратегічні документи спрямовані на систематизацію інформаційної сфери та створення цілісної системи документів, які регулюють цю галузь. Вони визначають стратегічні цілі, завдання та пріоритети розвитку інформаційної безпеки.

2. Ієрархія та механізми набуття чинності. Одним з ключових аспектів є обґрунтування ієрархії цих керівних документів. Важливо чітко визначити, які документи є стратегічними, а які – на допоміжному рівні, та передбачити механізми їх впровадження та реалізації.

3. Актуалізація та модернізація законодавства. Зокрема, аналізується необхідність внесення змін до чинних законодавчих актів, що стосуються інформаційної безпеки, а також створення нових законодавчих засад для відповідності сучасним реаліям цієї галузі.

Загальною метою є створення структурованої системи політико-правових документів, які не лише визначають стратегічні напрями розвитку інформаційної безпеки, а й створюють правові умови для їх реалізації та захисту національних інтересів у цій сфері.

Нами узагальнено принципи інформаційної безпеки, які у міжнародному вимірі відіграють важливу роль у забезпеченні стабільності, безпеки та використання інформаційних ресурсів, серед них:

1. Принцип суверенної рівності держав. Визнання права кожної держави на використання власних інформаційних ресурсів та захист їх від зовнішнього втручання. Цей принцип підкреслює важливість поваги до суверенітету кожної країни.

2. Принцип невтручання. Заборона деструктивної пропаганди та інформаційної інтервенції у внутрішні справи інших країн.

3. Принцип заборони силової агресії через інформаційний вплив. Запобігання використанню інформаційного впливу для силової агресії проти територіальної цілісності та політичної незалежності держав.

4. Принцип непорушності кордонів інформаційного простору. Захист національних меж в інформаційному просторі, що означає заборону незаконного перетину та втручання в інформаційні системи інших країн.

5. Дотримання основних прав і свобод людини. Забезпечення конституційних і спеціальних норм свободи слова, вільного обігу інформації, незалежності мас-медіа, свободи вираження думок та захисту конфіденційності інформаційних ресурсів.

6. Принцип міжнародного співробітництва. Запобігання конфліктам через взаємодію міжнародних суб’єктів для розвитку глобальної інформаційної інфраструктури та забезпечення політичних, економічних та соціокультурних прав світової спільноти.

Ці принципи створюють загальні рамки для етичного, правового та стабільного використання інформаційних ресурсів у міжнародному контексті.

Нами згруповано правові документи та законодавчі акти в Україні, які визначають основи інформаційної безпеки країни, надаючи органам влади необхідні нормативні засади для забезпечення цієї безпеки. Деякі з ключових документів, які утворюють основу інституційних норм інформаційної безпеки в Україні, включають:

1. Конституція України – основний правовий документ встановлює загальні принципи і права, включаючи права на свободу слова та інформації.

2. Закон України «Про інформацію» – нормативний акт, який встановлює основні правила та принципи роботи з інформацією в Україні.

3. Закон України «Про основи національної безпеки України» – визначає загальні принципи забезпечення національної безпеки, що включають інформаційну безпеку.

4. Стратегія розвитку інформаційного суспільства в Україні – встановлює стратегічні цілі та завдання для розвитку інформаційного суспільства в країні.

5. Доктрина інформаційної безпеки України – визначає загальні принципи, завдання та основні напрями політики інформаційної безпеки в країні.

6. Стратегія кібербезпеки України – визначає напрями і завдання у сфері кібербезпеки.

Ці документи створюють правову основу для формування і функціонування системи інформаційної безпеки в Україні, надаючи відповідним органам влади необхідні положення та керівні принципи для здійснення заходів забезпечення інформаційної безпеки.

Поняття «інформаційний суверенітет» в контексті правових норм України є досить важливим, оскільки визначає правові основи контролю держави за інформаційними ресурсами на своїй території та правила використання цих ресурсів в міжнародних відносинах [92].

У Законі України «Про інформацію» вказано, що інформаційний суверенітет ґрунтується на національних інформаційних ресурсах. Це означає, що Україна має виключне право контролювати та вільно розпоряджатися інформацією, яка створюється на її території. Цей закон визначає, що інформаційний суверенітет України відповідає правам власності на інформаційні ресурси, створені за рахунок державних коштів.

Також, важливою частиною цього поняття є контроль за доступом інших держав до інформаційних ресурсів України. Це право є виключним, і

використання інформаційних ресурсів відбувається за умови рівноправного співробітництва з іншими державами.

Отже, інформаційний суверенітет, як визначено в законодавстві України, встановлює основи для контролю та управління інформаційними ресурсами, забезпечуючи владі країни власність на ці ресурси та регулювання їх доступу та використання.

Дійсно, у сучасному світі інформаційна безпека вважається критично важливою для функціонування держави та суспільства. Інформаційні ресурси в сучасному світі є невід'ємною складовою, що зазнає постійних змін у якісному та кількісному вимірах. Захист національного інформаційного простору української держави є пріоритетним завданням, особливо в умовах гібридних загроз та викликів.

У наукових публікаціях і експертних оглядах з цього питання часто підкреслюється, що захист інформаційної безпеки залежить від комплексного підходу. Цей підхід включає в себе не лише систему регулятивних норм і принципів законодавства, але й ефективну діяльність регулятивних інститутів, які відповідають за контроль, управління та забезпечення безпеки інформаційного простору.

Більш того, важливою є також відповідальність і зобов'язання політичних і державних акторів, які мають забезпечувати ефективний захист інформаційної безпеки. Це включає в себе розробку та виконання стратегій, вжиття заходів, спрямованих на протидію загрозам, а також прийняття рішень, спрямованих на підвищення рівня інформаційної безпеки.

Отже, для забезпечення ефективного захисту національного інформаційного простору України потрібна комплексна система нормативних правил, дієвість відповідальних інститутів та ретельне виконання зобов'язань політичними та державними структурами.

Зазначені загрози в інформаційній сфері, які визначалися в законі «Про основи національної безпеки України», свідчать про широкий спектр потенційних проблем, що можуть виникнути у цій сфері. Такі загрози

включають обмеження свободи слова та доступу до інформації, маніпулювання громадською думкою через розповсюдження недостовірної інформації, розголошення державної таємниці, кіберзлочинність і кібертероризм.

Закон «Про національну безпеку України» [93], який вступив в дію після закону «Про основи національної безпеки України», наголосив на пріоритетності кіберзахисту критичної інформаційної інфраструктури та державних інформаційних ресурсів. Це свідчить про важливість забезпечення захисту інформаційних ресурсів від інформаційних загроз, які можуть виникнути у інформаційному просторі.

Ця зміна в законодавстві відображає постійний розвиток та зміни в інформаційній сфері, а також підкреслює потребу адаптувати стратегії та заходи забезпечення безпеки інформаційного простору до сучасних викликів і загроз.

Указ президента України №47/2017 «Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України» став важливим документом, який визначив стратегічні напрямки і пріоритети для забезпечення інформаційної безпеки в Україні, особливо в контексті європейської та євроатлантичної інтеграції.

У цьому документі були сформульовані базові засади інформаційної безпеки, представлено категорії інформаційних загроз для суспільства та визначені напрями державної політики в цій сфері. Приділялася увага створенню інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них, розвитку інститутів, що відповідають за інформаційно-психологічну безпеку та захист технологічної інфраструктури, а також забезпеченню покриття території цифровим мовленням, включаючи прикордонні та тимчасово окуповані території.

Доктрина передбачає, що Рада національної безпеки і оборони України має визначати заходи для реалізації стратегії, зокрема, у забезпеченні координації всіх державних органів для боротьби з агресивною

інформаційною війною, яка ведеться проти України, як на її території, так і в світі. Важливою також є участь інститутів громадянського суспільства у виконанні завдань, передбачених Доктриною, в межах їх компетенції.

Цей документ став ключовим для формування стратегії та спрямовування дій в інформаційній сфері, особливо в умовах сучасної повномасштабної війни та інформаційних викликів.

У документі, який присвячений доктрині інформаційної безпеки України, пропонується декілька ключових напрямків у класифікації загроз національній безпеці в інформаційній сфері. Однак, зазначається, що цей перелік не є повним та вичерпним у характеристиці загроз.

Зокрема, фахівці відзначають, що документ не надає конкретних ознак для класифікації загроз, що ускладнює точну і детальну оцінку цих загроз.

Науковці вважають, що загрозами у сфері інформаційної безпеки можуть бути такі сценарії [94]:

1. Спеціальні інформаційні операції направлені на порушення обороноздатності країни, деморалізацію військових формувань, створення панічних настроїв тощо.

2. Деструктивні інформаційні кампанії, спрямовані на формування негативного іміджу України.

3. Проблеми, пов’язані з недосконалістю законодавства щодо регулювання суспільних відносин у сфері інформації.

4. Недостатній рівень медіакультури. Як результат, суспільство може бути вразливим до інформаційної маніпуляції.

5. Пропаганда сепаратистських настроїв в країні, яка може призвести до загострення міжетнічних і міжконфесійних конфліктів.

Класифікація загроз інформаційній безпеці має важливе значення для адекватного реагування та розвитку стратегій захисту в цій сфері. Однак, важливо враховувати динамічний характер інформаційних загроз і постійно оновлювати методи їх виявлення та протидії.

Так, уведення в дію одночасно двох ключових документів – «Доктрини інформаційної безпеки України» і «Стратегії кібербезпеки України» – є показником рівночасного удосконалення заходів та стратегій у сферах інформаційної та кібернетичної безпеки. Обидва ці документи відображають стратегічний підхід до захисту інформаційного простору країни в контексті розвитку та зміни загроз у цифровій епохі. Разом вони створюють основу для комплексного підходу до забезпечення інформаційної безпеки України, враховуючи внутрішні та зовнішні виклики і загрози в цих сферах.

Так, мета «Стратегії кібербезпеки України» полягає в створенні умов для безпечного функціонування кіберпростору та його використання на користь особи, суспільства та держави. Для досягнення цієї мети стратегія визначає ряд основних напрямків:

1. Створення національної системи кібербезпеки, що означає належну організацію, координацію та співпрацю між різними урядовими та недержавними структурами для ефективного реагування на кіберзагрози.

2. Посилення спроможності сектору безпеки та оборони, що включає підвищення військових та оборонних сил для ефективного протидії кіберзагрозам воєнного характеру, кібершпигунству, кібертероризму та кіберзлочинності.

3. Забезпечення кіберзахисту державних електронних інформаційних ресурсів та інформації. Особлива увага приділяється захисту державних електронних ресурсів та інформації, доступ до яких регулюється законодавством.

4. Розвиток кіберпростору та інформаційного суспільства, що включає розвиток інформаційного простору, електронного урядування, забезпечення безпеки та сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів.

Стратегія кібербезпеки України встановлює базові принципи та підходи для забезпечення безпеки в кіберпросторі, ураховуючи важливість цієї сфери для забезпечення національної безпеки та стабільності держави.

Закон України «Про основні засади забезпечення кібербезпеки України» встановлює правові та організаційні основи для захисту важливих інтересів людини, громадянина, суспільства та держави у кіберпросторі. Цей закон визначає:

1. Правові основи. Конституція України, закони про основи національної безпеки, внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, а також міжнародні договори, які набули чинності після їх ратифікації Верховною Радою України, укази Президента, акти уряду та інші нормативно-правові акти, ухвалені з метою виконання законодавства України.

2. Основні цілі і напрями державної політики у сфері кібербезпеки. Закон визначає основні цілі і напрями у сфері кібербезпеки для забезпечення захисту інтересів особи, суспільства та держави у кіберпросторі.

3. Повноваження державних органів та інших суб'єктів: Закон визначає повноваження державних органів, підприємств, установ, організацій, осіб та громадян у сфері кібербезпеки.

4. Організаційні засади координації діяльності. Встановлюються основні засади координації діяльності суб'єктів, відповідальних за забезпечення кібербезпеки.

Зазначений закон спрямований на створення узгодженої системи правових та організаційних засад, які мають забезпечити ефективний захист інформаційної безпеки України.

Заслуговує на увагу також ініціатива з поглиблення державно-приватного партнерства в сфері кібербезпеки є важливим кроком для спільної роботи держави та приватного сектору у забезпеченні інформаційної безпеки країни.

Варто констатувати, що забезпечення захисту від інформаційних загроз вимагає комплексного підходу, який включає технічні, правові, організаційні та людські ресурси для запобігання, виявлення та реагування на потенційні

атаки та небезпеки, особливо в умовах повномасштабного вторгнення рф в Україну.

Отже, інституціональні засади інформаційної безпеки України становлять складну систему, що базується на розвитку та впровадженні системної політики захисту національних інтересів. Це охоплює різноманітні аспекти, такі як:

1. Розробка стратегічних документів, що включає розробку і впровадження стратегій, доктрин, політик і стратегій інформаційної безпеки, які визначають стратегічні цілі, принципи та шляхи захисту національних інтересів в кіберпросторі.

2. Законодавча база, зокрема розробка та прийняття законів, нормативних актів, що регулюють питання інформаційної безпеки, захисту даних та інформаційних ресурсів, а також визначення відповідальності за порушення цих законів.

3. Розвиток інноваційних технологій – створення та використання передових технологій, програм та методів захисту інформації та кіберінфраструктури.

4. Міжнародне співробітництво – співпраця з міжнародними організаціями та іншими країнами для обміну досвідом інформаційної безпеки, створення спільних стандартів і заходів протидії кіберзагрозам.

5. Захист критично важливої інфраструктури, де особлива увага приділяється захисту критичних інформаційних систем та інфраструктури, що визначається як стратегічно важлива для функціонування країни.

6. Навчання – збільшення рівня усвідомленості інформаційних загроз серед населення та навчання у відповідних програмах інформаційної безпеки.

7. Співпраця держави та приватного сектору – розвиток партнерства між урядовими органами та приватним сектором для спільної реалізації заходів інформаційної безпеки.

Варто зазначити, що усі ці аспекти тісно пов’язані між собою і створюють комплексний підхід до захисту інформаційної безпеки України.

3.2. Інструменти забезпечення безпекоорієнтованого інформаційного середовища в Україні

Існуючі інноваційні підходи до формування системи інформаційної безпеки в Україні враховують сучасні технології та комунікаційні засоби. Для ефективної боротьби з новітніми загрозами і підвищення рівня інформаційної безпеки нами були визначені пріоритети державної політики в інформаційній сфері, які включають:

1. Використання комунікативних інструментів, що включає розробку спеціальних платформ, програм або технологій, спрямованих на виявлення, аналіз і відстеження потенційних загроз в інтернеті та інших медійних джерелах.

2. Інформаційно-пропагандистські кампанії, які включають розробку та реалізацію інформаційних кампаній для поширення правдивої інформації, яка спрямована на виявлення та розкриття негативних загроз, а також усвідомлення громадськістю необхідності захисту інформації.

3. Залучення соціальних мереж, зокрема використання платформ соціальних мереж для поширення інформації, залучення уваги до питань кібербезпеки, інформування громадськості про можливі загрози та способи їх запобігання.

Ці підходи спрямовані на покращення рівня свідомості громадськості, формування культури безпеки в онлайн-середовищі та розширення можливостей для виявлення, захисту та реагування на інформаційні загрози. Реалізація таких пріоритетів може сприяти покращенню загального рівня інформаційної безпеки в країні.

Так, модернізація інструментів інформаційної безпеки тісно пов’язана з геополітичною конкуренцією міжнародних акторів. Сучасні стратегії національної безпеки мають враховувати використання нових засобів і методів інформаційного протиборства, оскільки комунікативні інструменти

впливають на сприйняття політичних лідерів та формують поведінку громадськості стосовно безпекових ініціатив на міжнародному рівні.

Функція комунікативних технологій у доктринах інформаційної безпеки полягає у визначенні та розробці ефективних методів взаємодії з громадськістю, іншими країнами та міжнародними організаціями через інформаційні канали. Ці технології можуть використовуватися для впливу на погляди, переконання та рішення громадськості, керівників держав та інших важливих акторів на міжнародній арені.

Підвищення уваги до комунікативних інструментів в інформаційній безпеці стає важливою складовою стратегій забезпечення національних інтересів країни в умовах глобалізації та активних інформаційних воєн. Такий підхід дозволяє ефективно реагувати на виклики та загрози, що походять як від інших держав, так і від незаконних або ворожо налаштованих груп, і забезпечує захист національних інтересів у світі цифрової дипломатії і інформаційних технологій.

Питання трансформації політики інформаційної безпеки стає дедалі більш актуальним в контексті розвитку нових технологій та їх впливу на міжнародну безпеку. У світі цифрової епохи інформаційні засоби набувають великого значення у формуванні поглядів громадськості та прийнятті рішень в сфері політики. Використання нових технологій інформаційного впливу може мати значний руйнівний вплив на систему міжнародної безпеки та баланси сил.

Зокрема, важливими стали питання забезпечення безпеки в інформаційному просторі, контролю за маніпуляціями та впливом на громадську думку, а також захисту від цифрових загроз, що виникають з використанням новітніх технологій. Це призвело до перегляду стратегій безпеки та удосконалення інструментів контролю та захисту від нових форм загроз у сфері інформаційної безпеки.

Погляди вчених та фахівців [95] виявляються різними відносно того, як використовувати ці нові інформаційні засоби впливу. Деякі вважають, що

вони можуть спричинити руйнівний вплив на міжнародні відносини, створюючи нові конфліктні ситуації. Інші ж вбачають можливість збалансованого використання цих засобів для забезпечення національних інтересів та зміцнення стійкості суспільства до цифрових загроз.

У зв`язку з цим, важливо вдосконалювати політику інформаційної безпеки, розробляти ефективні заходи контролю та реагування на виникаючі загрози, а також створювати міжнародні механізми співпраці для протидії новим викликам у цій сфері.

Справді, розпізнання інформаційних загроз, які є або можуть бути потенційно шкідливими для національної безпеки, викликало необхідність оновлення стратегій інформаційної безпеки в багатьох країнах, включаючи Україну. Цей процес відбувається через удосконалення ключових стратегічних документів, які визначають політику країни у цих сферах.

Україна активно переглядає свої стратегічні документи, враховуючи нові виклики та потенційні загрози, зокрема в інформаційному просторі. Розробка нових доктрин, класифікація основних термінів, встановлення засобів захисту інформаційного середовища та підготовка спеціалізованого персоналу – це деякі зі стратегічних заходів, спрямованих на зміцнення інформаційної безпеки.

Також, досвід сучасних воєнних конфліктів підтверджує важливість використання різноманітних інформаційних озброєнь для дій під час конфліктів. Це впливає на формулювання та реалізацію доктрин інформаційної безпеки не лише в Україні, а й в інших країнах.

Розуміння значущості інформаційних загроз та створення ефективних механізмів для протидії потенційним агресивним діям у сфері інформаційної безпеки стає ключовим для забезпечення національної безпеки кожної країни у сучасному цифровому світі.

Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради [96] фактично відображає той комплексний підхід, який необхідний для визначення пріоритетів та напрямків у сфері інформаційної

безпеки. Саме у цьому звіті акцентується на урахуванні сучасних реалій – глобалізації та вільному обігу інформації, які створюють нові виклики і загрози для національної безпеки. Цей документ відображає потребу у використанні інноваційних підходів для захисту та розвитку інформаційного простору України, враховуючи актуальні загрози, які стали значущими у цифрову епоху. Використання інформаційної технології та забезпечення захисту інформаційного простору від зовнішніх та внутрішніх загроз стали одними з ключових завдань у політиці держави.

Цей документ є частиною важливої інституціональної практики, яка відображає важливі аспекти управління державними справами та покликана відображати ситуацію в країні з точки зору її національної та інформаційної безпеки.

Згідно з доктринальними положеннями, викладеними у документі про інформаційну безпеку України, інформаційна безпека розглядається як невід'ємна складова національної безпеки. Серед ключових понять, пов'язаних із комунікативними інструментами інформаційної безпеки, автори визначають:

1. Стратегічний курс. Спеціально підготовлений текст для вербального впливу на цільову аудиторію.

2. Стратегічні комунікації. Координація і використання комунікативних можливостей держави, таких як публічна дипломатія, зв'язки з громадськістю, військові комунікації, інформаційно-психологічні операції та інші, для просування інтересів держави.

3. Урядові комунікації. Комплекс заходів, що включають комунікації уповноважених представників уряду з цільовою аудиторією для роз'яснення урядової позиції та/або політики з певних проблемних питань.

4. Кризові комунікації. Сукупність заходів, що здійснюються у кризових ситуаціях і передбачають зв'язки з громадськістю.

5. Іміджеві комунікації. Програми і заходи з формування та підтримки позитивного іміджу України у міжнародному вимірі.

Розбіжності визначення понять у нормативно-правових документах, таких як Закон України «Про основні засади розвитку інформаційного суспільства в Україні» та інші нормативно-правові акти, можуть виникати через різні підходи до тлумачення поняття «інформаційна безпека». Це може бути обумовлене традиційними уявленнями або експертними поглядами на сутність інформаційної безпеки, а також змінами у технологічному прогресі та впливі інновацій на розвиток та модернізацію інформаційних озброєнь.

Це стає причиною різних тлумачень та розуміння термінології у вітчизняних дослідженнях. Зокрема, у переході від уявлень, які були актуальні на час прийняття Закону «Про основні засади розвитку інформаційного суспільства», до сучасних тенденцій інформаційної безпеки може виникати розрив у розумінні певних аспектів цього поняття.

Однак, важливо розуміти, що такі різниці в тлумаченні не обов’язково є протиріччями. Вони можуть відображати еволюцію уявлень та внесення коректив у правові документи для відповідності новим викликам і вимогам сучасного інформаційного середовища.

Так, конкретизація комунікативних інструментів в рамках інформаційної безпеки дозволяє більш глибоко аналізувати та розуміти різноманітність стратегічних комунікацій. Одним із важливих елементів є публічна дипломатія, яка орієнтована на вивчення та інформування зарубіжної аудиторії та побудову взаємовідносин. Також до цих інструментів належать Public Affairs, які займаються зв’язками з громадськістю та управлінням громадською думкою, а також спеціальні інформаційно-психологічні операції, спрямовані на вплив на поведінку спільноти.

Ці операції включають в себе політичні, військові та ідеологічні заходи, які мають за мету змінити мотивацію поведінки окремих осіб або груп суспільства у бажаному напрямку. Вони є частиною державної політики та здійснюються з метою впливу на громадську думку та формування певних установок серед населення.

Аналіз та розуміння цих стратегічних комунікаційних інструментів в контексті інформаційної безпеки є важливим для визначення ефективних стратегій захисту та підтримки національних інтересів держави в інформаційному просторі.

У зарубіжному науковому дискурсі [97] стратегічні комунікації розглядаються як комунікативні технології, спрямовані на розвиток міжнародних взаємодій та створення тривалих зв'язків між урядовими структурами, міжнародними акторами, дипломатичними установами та політичними лідерами для втілення політичних, економічних, безпекових, культурних, соціальних та гуманітарних ініціатив та проектів. Це підкреслює Е. Голдман [97], зазначаючи, що інформація, вплив та переконання у потрібності підтримки національної політики вимагають розуміння мети.

Якщо мета національної політики розуміється як конкретний набір установок масової свідомості, мотивації поведінки або процесів сприйняття цієї політики, суспільство буде підтримувати цю мету. Ефективні стратегічні комунікації, в цьому випадку, вимагатимуть чітких, послідовних повідомлень, які випливають з мети національної політики.

Це підкреслює важливість розуміння та використання спеціальних комунікативних інструментів для сприяння реалізації національних стратегій у різних сферах, сприяючи формуванню стійких зв'язків та співпраці між різними державними та міжнародними структурами.

Аналіз українських наукових досліджень свідчить про складний і суперечливий характер комунікативних інструментів інформаційної безпеки. Цей аналіз розкриває можливості взаємодії між урядовими та неурядовими структурами, а також значний вплив інноваційних технологій на різні сфери функціонування країни.

У вітчизняних дослідженнях висвітлюються параметри стратегічного наративу та стратегічних комунікацій, їх роль у сфері державного управління та міжнародній діяльності України. Важливо відзначити, що стратегічні комунікації визначаються як національний ресурс для керування дипломатією,

інформацією, збройними силами та економікою, охоплюючи всіх міжнародних акторів і включаючи системну оцінку їх значущості для зовнішньої та безпекової політики країни.

Зокрема, умови протистояння агресії РФ активно використовуються Україною для формування та поширення загальнодержавних позицій щодо поточних та надзвичайних подій, з метою їх представлення глобальній громадськості за допомогою наявних телекомунікаційних каналів, інтернету та соціальних медіа.

Систематизація стратегічних комунікацій України показує їхню важливість у різних сферах діяльності держави, таких як європейська та євроатлантична інтеграція, зовнішня та внутрішня політика, антитерористична діяльність, а також у протидії агресії РФ. Ці стратегічні комунікації використовуються для формування і поширення загальнодержавних позицій з поточних і надзвичайних подій з метою їх представлення глобальній громадськості через доступні телекомунікаційні канали, Інтернет та соціальні мережі.

Важливим кроком стала ініціатива створення трастового фонду зі стратегічної комунікації НАТО та Великої Британії, спрямованого на посилення боротьби з гібридною військовою загрозою та російською пропагандою в Україні, Молдові та Грузії.

Ці стратегічні комунікації стали важливими компонентами політики інформаційної безпеки України, включені у державні нормативні та аналітичні документи різного рівня, такі як Воєнна доктрина України, аналітичні звіти до щорічних послань Президента України до Верховної Ради України, Концепція стратегічних комунікацій Міністерства оборони України та Збройних сил України [97].

Залучення стратегічних комунікацій до національних програм з інформаційної безпеки свідчить про їхню ефективність і сучасність у досягненні відповідного рівня спроможності держави протистояти реальним і потенційним загрозам.

Урядові комунікації є критично важливим інструментом для поширення достовірної інформації про стан справ в країні та впливу на різні аспекти суспільства. До важливих аспектів урядових комунікацій на нашу думку слід віднести:

1. Поширення успіхів та реформ. Сповіщення про досягнення та реформи у різних сферах діяльності держави дозволяє підкреслити прогрес і зусилля, спрямовані на покращення у всіх аспектах життя суспільства.

2. Залучення інвестицій. Інформація про стан економіки, бізнес-середовище та інвестиційні можливості, надана урядом, може сприяти залученню іноземних інвестицій, що відіграє ключову роль у розвитку країни.

3. Захист незахищених верств суспільства. Комунікаційні кампанії можуть інформувати про соціальні програми та заходи, спрямовані на захист та підтримку найбільш вразливих груп населення.

4. Об’єднання громадян. Ефективна комунікація може сприяти формуванню спільної свідомості та об’єднанню громадян навколо спільних цілей та цінностей.

5. Забезпечення безпечного розвитку. Інформування про стратегії безпеки, заходи захисту та запобігання загрозам допомагають забезпечити стабільний та безпечний розвиток країни.

Урядові комунікації включають в себе різноманітні інструменти, такі як прес-релізи, соціальні медіа, прямі звернення до громадян, публічні заходи тощо [98]. Ці інструменти спрямовані на забезпечення доступу до достовірної та вичерпної інформації для громадян, бізнесу та інших зацікавлених сторін. Ретельно сплановані та ефективні урядові комунікації можуть значно підвищити довіру до влади та сприяти стабільному розвитку країни.

Дезінформація та деструктивні інформаційні впливи, особливо з боку РФ, становлять серйозну загрозу для національної безпеки України. Ці впливи можуть бути спрямовані на порушення стабільності, формування негативного уявлення про країну, дискредитацію урядових інститутів та суспільства, інформаційну маніпуляцію та зміну перспективи на події.

Змістове наповнення, реалізація та позиціонування національних інтересів в інформаційному просторі є ключовими завданнями для забезпечення інформаційної безпеки країни. Для боротьби з деструктивними інформаційними впливами необхідна комплексна стратегія, що включає:

1. Розвиток медіаосвіти. Ініціативи з підвищення медіаграмотності серед громадян допомагають створити у населення навички критичного мислення та розрізнення достовірної інформації від маніпуляцій та дезінформації [99].

2. Створення інформаційних контрзаходів. Розробка та впровадження заходів з підвищення інформаційної безпеки, виявлення та протидія деструктивним інформаційним впливам.

3. Міжнародне співробітництво. Україна може співпрацювати з міжнародними партнерами для обміну досвідом та підтримки у боротьбі з дезінформацією.

4. Трансформація інформаційних підходів. Адаптація до сучасних технологій та платформ, удосконалення інформаційних каналів та мереж для ефективної комунікації.

5. Створення ефективної комунікаційної стратегії. Розробка чіткої та доступної комунікаційної стратегії, спрямованої на боротьбу з дезінформацією та підвищення довіри до державних інститутів.

Ці заходи вимагають системного та комплексного підходу для ефективного протистояння деструктивним інформаційним впливам та забезпечення інформаційної безпеки України.

Отже, зазначені інструменти інформаційної безпеки в сучасному світі виступають ключовим чинником зміни традиційних підходів до політики національної безпеки та оборони. Вони сприяють не лише передачі інформації, а й формуванню сприятливого інформаційного середовища, забезпеченню захисту від дезінформації та деструктивного впливу, а також сприяють вирішенню безпекових проблем. Комунікативні інструменти інформаційної безпеки:

1. Змінюють традиційні підходи до політики безпеки, дозволяють не лише реагувати на загрози, але й прогнозувати, адаптуватися та протидіяти їм завчасно, реагуючи на рівні інформаційного простору.

2. Поглиблюють взаємодію між урядовими та неурядовими структурами. Співпраця урядових органів, громадських організацій, експертів та ЗМІ є важливою для ефективного спільного реагування на інформаційні загрози.

3. Перерозподіляють відносини в державному управлінні. Зміцнення ролі комунікаційних інструментів може призвести до переосмислення стратегій та підходів управління, зокрема, управління кризовими ситуаціями та інформаційними загрозами.

4. Збільшують інтенсивність економічної взаємодії. Стабільне та довірче інформаційне середовище сприяє покращенню бізнес-клімату, залученню інвестицій та сприяє розвитку економіки.

5. Підвищують ефективність комунікації у розв’язанні безпекових проблем. Чітка та ефективна комунікація дозволяє швидше та ефективніше реагувати на кризові ситуації, мінімізуючи їхні наслідки.

Отже, комунікативні інструменти інформаційної безпеки відіграють важливу роль у сучасному світі, змінюючи підходи до безпеки, сприяючи взаємодії та підвищуючи ефективність державного управління та розв’язання безпекових проблем.

3.3. Основні напрями діяльності держави у сфері забезпечення інформаційного суверенітету України

Стратегічний вимір інформаційної безпеки України включає в себе протидію інформаційним впливам на критично важливі сфери функціонування держави. Інформаційні інтервенції в цьому контексті описуються як комплекс заходів, спрямованих на розповсюдження

специфічно підібраних повідомлень чи їх тлумачень через різні комунікаційні канали. Ці заходи спрямовані на вплив на громадську думку, формування певного контексту чи погляду на певну ситуацію та прийняття важливих рішень у керівництва держави. Інформаційні технології, обладнання іноземного виробництва, які використовуються в країні, також можуть бути задіяні в таких інтервенціях.

Важливо зауважити, що ці дії можуть бути частиною гібридних інформаційних війн, де комбінуються різні інструменти, включаючи кібератаки, дезінформацію, маніпуляції інформацією та інші методи для досягнення стратегічних цілей.

Однією з ключових проблем є забезпечення енергетичної, технологічної та медичної безпеки в умовах інформаційних втручань. Це включає захист критичних інфраструктур, даних та систем у сферах енергетики, технологій та охорони здоров’я від кібератак та негативного інформаційного впливу.

Загальний підхід до стратегії інформаційної безпеки України включає розвиток ефективної системи захисту від таких загроз, зміцнення кібербезпеки, виявлення та протидію дезінформації, а також забезпечення стійкості та резильєнтності критичних секторів у разі можливих впливів.

Г. Почепцов, експерт з інформаційно-психологічних операцій та війн, акцентує увагу на активному використанні РФ зовнішніх і внутрішніх інтервенцій як інструменту для підсилення інформаційно-психологічного тиску на Україну [100]. Він визначає ці інтервенції як самостійний та важливий ресурс інформаційних озброєнь, порівнянний у важливості з військовим потенціалом. Зазначається, що російське втручання у регіонах колишнього СРСР (таких як Україна, Грузія та Молдова) спричиняє серйозні наслідки для політики інформаційної безпеки. Ці інтервенції можуть бути спрямовані на вплив на наміри цих країн стосовно їхнього європейського та євроатлантичного шляху, спроби змінити їхній курс і відвести від інтеграції до Європейського Союзу чи НАТО. У публікаціях дослідника також відзначається, що російське втручання у зовнішню і безпекову політику

деяких балканських держав може мати менш агресивний характер. В цих випадках воно спрямоване на формування громадських рухів, які сприятимуть стримуванню урядів цих країн від європейської та євроатлантичної інтеграції.

Такий підхід РФ до впливу на різні країни може свідчити про різноманітність методів та підходів, які вона використовує для досягнення своїх стратегічних цілей в різних регіонах, а також про різні рівні активності та агресивності цих дій.

М. Ожеван, експерт з інформаційної безпеки, розглядає зовнішні впливи на Україну в контексті конструктивних та маніпулятивних. Він виділяє «конструктивні» впливи, спрямовані на підтримку демократії, прав людини, свободи слова, торгівлі тощо, які можуть бути в інтересах країни-об’єкта і України. У той же час, у маніпулятивних ситуаціях присутній зовнішній інтерес, що може відноситися до впливових держав або транснаціональних бізнес-структур, що частково або повністю узгоджується з національно-державними інтересами України або не загрожує їм у короткостроковій перспективі.

Експерт виділяє специфічні групи зовнішніх впливів, які можуть здійснювати зовнішнє управління і відносяться до організацій, членство в яких має значення для України, і виключення з яких може призвести до міжнародної або єврорегіональної ізоляції.

У той же час, деструктивні антидержавні інформаційні впливи, які включають інформаційні інтервенції, експансію, агресію, тероризм чи війну, потребують негайної або програмно-планової реакції держави. М. Ожеван визначає такі впливи як потенційно небезпечні через їхню здатність спровокувати серйозні соціально-політичні потрясіння, що можуть бути штучно спровоковані ззовні.

Згідно з аналітикою М. Ожевана, протидія таким деструктивним зовнішнім інформаційним впливам вимагає використання різноманітних концептуально-ідеологічних, розвідувально-контррозвідувальних,

моніторингово-аналітичних, нормативно-правових, організаційно-технічних та оперативних технологій [101].

Отже, експертна аналітика Михайла Ожевана розкриває широкий спектр зовнішніх впливів на Україну, відмежовуючи «конструктивні» від маніпулятивних, та виділяє необхідність системного підходу до протидії деструктивним антидержавним інформаційним впливам.

У науковій розвідці С. Даниленка акцентується на руйнівних впливах зовнішніх інформаційних інтервенцій на національну безпеку України. Автор пропонує ряд заходів для виявлення та запобігання загрозам у сфері інформаційної безпеки, робить акцент на необхідності реагування на навмисне зовнішнє інформаційне втручання.

С. Даниленко зазначає, що «гібридизація» інформаційних загроз може призвести до розробки та використання інструментів протидії для нейтралізації зовнішніх інформаційних інтервенцій. Автор аналізує російську зовнішню політику, вказуючи, що РФ використовує різноманітні інструменти тиску, такі як інформаційна, дипломатична та розвідувальна інформація, а також енергетичні ресурси, особливо в регіонах України, де РФ прагне зміцнити свою присутність та контроль над місцевими державними структурами.

У публікації вказується, що РФмає досвід у застосуванні спеціальних акцій російських спецслужб, енергетичного шантажу, пропагандистських медіа, що дає їй можливість використовувати подібний інструментарій в інших країнах та субрегіонах.

Автор вважає, що для здійснення таких інтервенцій РФ буде змушена витрачати дедалі більше ресурсів, у той час як ефективність цих дій буде зменшуватися через потужні роз’яснювальні кампанії місцевих державних структур, громадських організацій та активних мас-медіа. Зазначається, що ці органи роблять зусилля для спростування деструктивного контенту, який може використовуватися різними засобами масової інформації, радикальними

громадськими об’єднаннями та політичними популістами для розбалансування інформаційного середовища [102].

Економічна сфера є однією з важливих складових стратегічного виміру інформаційної безпеки України. Російська війна проти України, яка охоплює інформаційно-психологічний вплив, спрямована на дестабілізацію та дискредитацію української держави, включає в себе інформаційні атаки, спрямовані на економічний сектор.

Повномасштабне вторгнення РФ в Україну створило напружену економічну ситуацію. Це стало однією зі складових війни, яка залучає інформаційно-психологічні методи для впливу на економіку країни.

Зокрема, російські суб’єкти впливу використовують інформаційні канали для створення негативного образу української економіки, розповсюдження дезінформації щодо її стабільності та розвитку. Це може впливати на інвестиційний клімат, внутрішній та зовнішній економічний потенціал країни, а також загальну довіру до українських фінансових та економічних інституцій.

Україна змушена реагувати на ці загрози і підвищувати рівень інформаційної безпеки в економічному секторі. Це охоплює заходи зі зміцнення кібербезпеки фінансових інститутів, захист від кібератак на економічні об’єкти, розвиток інформаційних кампаній для збереження довіри до фінансових систем, та створення механізмів відповіді на дезінформацію щодо економічного стану країни.

Розбудова і підтримка інформаційної безпеки в економічному секторі важлива для забезпечення стабільності та розвитку української економіки в умовах війни і інформаційних загроз.

Квантова кібербезпека стане одним з найважливіших аспектів у майбутній кібербезпеці, оскільки розвиток квантових технологій відкриває нові можливості і створює значні виклики для захисту інформації та інформаційних систем. Ці технології можуть забезпечити високий рівень

конфіденційності, надійності та безпеки у сфері комунікацій та обчислень. Однак вони також можуть стати об’єктом нових загроз у кіберпросторі.

Наразі багато країн та корпорацій вкладають значні ресурси у розробку квантових технологій і програмного забезпечення. Розширення використання квантових технологій може змінити парадигму кібербезпеки, забезпечуючи нові методи шифрування та захисту даних, що можуть стати важливими у галузі обміну конфіденційною інформацією між державними структурами, фінансовими установами, оборонними секторами та іншими критичними системами.

Проте, з розвитком квантової кібербезпеки виникають нові виклики. Зокрема, розробка квантових комп’ютерів може допомогти розшифрувати деякі системи шифрування, які використовуються зараз. Це означає, що існуючі методи захисту можуть стати менш ефективними, що потребує розвитку нових криптографічних методів для забезпечення безпеки в умовах квантових обчислень.

Таким чином, квантова кібербезпека представляє собою як нові можливості, так і нові загрози. Розвиток цієї сфери вимагає постійного вдосконалення методів захисту та криптографічних засобів, а також співпраці між державами та приватним сектором для забезпечення безпеки у кіберпросторі.

Україна, подібно багатьом іншим країнам, у своїй Стратегії кібербезпеки враховує значення квантум-безпеки для захисту важливих державних інформаційних ресурсів та критичної інформаційної інфраструктури. Квантові технології можуть стати важливим елементом у захисті від сучасних і майбутніх кіберзагроз.

У контексті Стратегії кібербезпеки України, пріоритети стосуються:

1. Розроблення та адаптація державної політики кібербезпеки. Створення та постійне оновлення стратегій із захисту від кіберзагроз, включаючи аспекти квантум-безпеки.

2. Відповідність стандартам ЄС та НАТО. Узгодженість з міжнародними стандартами кібербезпеки є важливою для забезпечення взаємодії з іншими країнами та організаціями у цій сфері.

3. Технічний та криптографічний захист інформації. Розвиток та вдосконалення систем технічного захисту, які використовують квантові технології для забезпечення безпеки обміну даними.

4. Залучення інноваційних стартапів для впровадження квантових технологій. Важливо враховувати перспективні технології та сприяти їхньому впровадженню в сферу кібербезпеки через співпрацю з інноваційними компаніями та стартапами.

Отже, квантум-безпека стає не лише важливою частиною Стратегії кібербезпеки України, а й ключовим напрямком для забезпечення безпеки державних інформаційних систем та інфраструктури в умовах сучасних та майбутніх кіберзагроз.

COVID-19, крім своєї безпосередньої загрози для здоров’я і життя, також став об’єктом інформаційних маніпуляцій і місцем поширення дезінформації. Фахівці з інформаційної безпеки відносять цей аспект до стратегічного виміру інформаційної безпеки, оскільки дестабілізація ситуації в державі та суспільстві через поширення фейкових повідомлень про коронавірус стає частиною гібридних загроз.

Зовнішні та внутрішні інформаційні інтервенції, що поширюють фейкову та маніпулятивну інформацію про COVID-19, можуть містити різноманітні твердження, які не мають наукового обґрунтування або базуються на конспірологічних теоріях. Це може призвести до ігнорування необхідних профілактичних заходів, неправильного лікування, відмови від карантину та зміцнення негативних відносин до влади через формування протестної поведінки серед громадськості.

Такі маніпуляції можуть мати серйозні наслідки для суспільства та держави. Посилення відповідності інформаційних кампаній, публічна освіта та підвищення обізнаності громадян щодо фактів, достовірної інформації та

вірусних загроз є важливими кроками у боротьбі з дезінформацією та підвищенні рівня covid-безпеки в країні.

Так, інноваційні інструменти політики інформаційної безпеки, такі як квантум-безпека та covid-безпека, мають потенціал бути важливими чинниками в протидії кіберзагрозам та в контролі за їх можливим використанням у гібридних конфліктах. Розвиток цих напрямків дозволяє використовувати передові технології і наукові досягнення для покращення інформаційної безпеки.

Співпраця України з інститутами ЄС та європейськими організаціями, а також промисловим сектором, може стати ключовим елементом в цьому процесі. Ця співпраця може сприяти обміну знаннями, передовими методами та технологіями, що стосуються кібербезпеки, включаючи аспекти квантової та біологічної безпеки. Важливою також є співпраця в області прикладних наукових досліджень для впровадження інноваційних підходів у практичне застосування, забезпечення кібербезпеки та захисту інформації.

Створення стратегічних цифрових можливостей і розвиток інтегрованих заходів інформаційної та кібербезпеки відіграють важливу роль у зміцненні захисту країни від кіберзагроз. Це може бути досягнуто через інтеграцію передових технологій, співпрацю та обмін досвідом з європейськими партнерами з метою створення більш стійких та інноваційних систем захисту інформації та кібербезпеки.

Забезпечення інформаційного суверенітету України передбачає комплекс заходів та напрямів діяльності, спрямованих на захист та збереження національної інформаційної системи, а також забезпечення власних інформаційних ресурсів. Основні напрями діяльності держави в цій сфері включають:

1. Кібербезпека та кіберзахист. Розробка та впровадження стратегій і політик кібербезпеки, заходів захисту від кіберзагроз, розробка систем кіберзахисту критичних інфраструктур, підвищення кібербезпеки урядових та державних мереж.

2. Інформаційна безпека та захист персональних даних. Розробка та впровадження політик та законодавства щодо захисту персональних даних, забезпечення відповідності міжнародним стандартам захисту інформації.

3. Контроль за поширенням дезінформації та фейків. Створення механізмів виявлення та протидії фейкам, вірусним новинам, а також підтримка медійної грамотності серед населення.

4. Створення та підтримка національної інформаційної інфраструктури. Розвиток та підтримка власної інформаційної інфраструктури, включаючи мережі зв'язку, центри обробки даних, інформаційні системи тощо.

5. Створення та вдосконалення законодавства. Розробка та впровадження законів та нормативно-правових актів, спрямованих на захист інформаційної безпеки держави, в тому числі стосовно кібербезпеки, захисту персональних даних, боротьби з кіберзлочинністю та дезінформацією.

6. Міжнародне співробітництво. Участь в міжнародних обмінних програмах, співпраця з іншими країнами і міжнародними організаціями з питань кібербезпеки та інформаційної безпеки.

7. Підвищення інформаційної обізнаності громадян. Розвиток освітніх програм та ініціатив, спрямованих на підвищення рівня обізнаності громадян щодо кібербезпеки, безпеки в Інтернеті, розпізнавання дезінформації та фейків.

Ці напрями дозволяють державі удосконалювати свої системи захисту інформації та боротьби з кіберзагрозами для забезпечення стабільності і безпеки інформаційного простору України.

Висновки до розділу 3

Регулювання інформаційної безпеки є ключовим напрямом для державних інституцій України з метою забезпечення захисту та безпеки

національного інформаційного простору. У роботі нами визначено ключові аспекти регулювання інформаційної безпеки:

1. Установлення принципів регулювання. Важливим етапом є встановлення єдиної системи принципів регулювання інформаційних ресурсів, яка відповідала б національним потребам та міжнародним стандартам безпеки і конфіденційності.

2. Нормативні засади. Розробка та впровадження нормативних актів, законів, положень та правил, що регулюють діяльність суб'єктів інформаційного простору, а також визначення відповідальності за порушення інформаційної безпеки.

3. Захист і безпекові інтереси. Забезпечення захисту від несанкціонованого доступу до інформаційної інфраструктури, а також захист інформаційних ресурсів від зовнішніх загроз і атак.

4. Система правового регулювання. Створення системи правового регулювання, яка охоплює всі аспекти інформаційної безпеки, включаючи кібербезпеку, захист персональних даних, боротьбу з дезінформацією тощо.

5. Стратегія інформаційного суверенітету. Розробка і впровадження стратегій забезпечення належного інформаційного суверенітету, включаючи заходи з протидії зовнішнім та внутрішнім загрозам інформаційної безпеки.

6. Цілеспрямована системна діяльність. Реалізація цілеспрямованої політико-правової діяльності, спрямованої на підтримку та захист національних інтересів у сфері інформаційної безпеки.

Ці напрями виступають основою для розвитку системи регулювання інформаційної безпеки в Україні та визначення стратегій і дій для забезпечення національної безпеки в цій сфері.

Комунікативний інструментарій справді має вирішальне значення у сфері інформаційної безпеки, впливаючи на сприйняття суспільством подій, формування думок та уявлень про ключові проблеми. Нами обґрунтовано ключові аспекти ролі комунікативних інструментів у сфері інформаційної безпеки:

1. Підвищення усвідомленості. Комунікативний інструментарій використовується для поширення інформації щодо загроз та заходів їх запобігання. Це допомагає підвищити рівень усвідомленості громадськості про потенційні ризики і проблеми.

2. Кризовий комунікаційний план. Відповідно до сучасних загроз, комунікативний інструментарій також включає розробку планів кризової комунікації, які дозволяють ефективно реагувати на непередбачені ситуації та кризи.

3. Статусна комунікація. Важливе значення має комунікація на статусному рівні, коли державні інституції звертаються до міжнародних партнерів для забезпечення підтримки, формуючи сприятливий образ для співпраці та взаємодії.

4. Вплив на політичні рішення. Комунікаційні інструменти можуть впливати на політичні рішення, формуючи громадську думку та ставлення до певних подій та рішень уряду.

5. Вплив на поведінку. Ефективний комунікативний інструментарій може впливати на поведінку громадян, спонукуючи їх до певних дій або виключаючи небажану реакцію на загрози.

У роботі визначено, що у сучасному світі, де інформація стає важливим ресурсом, використання комунікативних інструментів в сфері інформаційної безпеки стає важливою складовою національної безпеки та стратегії взаємодії з міжнародним співтовариством.

Стратегічний вимір інформаційної безпеки для України в сучасних умовах дійсно має вирішальне значення через різноманітні внутрішні та зовнішні загрози. Важливі аспекти та завдання в цьому контексті на нашу думку, включають:

1. Протидія гібридним загрозам. Сучасні інформаційні загрози, особливо ті, що мають гібридний характер, вимагають комплексного підходу та уваги до деталей в реагуванні та запобіганні. Це охоплює дії, спрямовані на

знешкодження різних форм впливу, включаючи маніпуляції засобами медіа, кібератаки, інформаційну дезінформацію тощо.

2. Координація та співпраця. Ефективна робота в цьому напрямі передбачає не лише реагування на інформаційні загрози, але й активну координацію різних секторів суспільства, урядових органів, безпекових структур, а також співпрацю з партнерами на міжнародній арені.

3. Захист критичних секторів. Особлива увага повинна бути приділена захисту критичних секторів, таких як політичний, економічний, енергетичний, технологічний, соціальний і медичний, які можуть стати об'єктом атак та впливу з боку зовнішніх сил.

4. Розвиток стійких заходів. Усунення вразливостей та розвиток стійких заходів включає в себе як технічні заходи з кібербезпеки, так і розвиток ефективних комунікаційних стратегій для протистояння дезінформації та маніпуляціям.

5. Створення адаптивних механізмів. Загрози інформаційної безпеки неперервно змінюються. Важливо мати адаптивні механізми реагування, які швидко реагують на нові форми атак та загрози.

Нами зроблений загальний висновок про те, що здійснення ефективної стратегії інформаційної безпеки вимагає комплексного підходу та постійного аналізу з метою запобігання та реагування на сучасні виклики і загрози.

ВИСНОВКИ

Концепція «м’якої/розумної» та «гострої» сили в концепції інформаційної безпеки відображає два важливих аспекти застосування сучасних інформаційних технологій у сфері міжнародних економічних відносин:

1. «М’яка/розумна» сила – ця концепція відноситься до використання інформаційних технологій, дипломатії, культурних обмінів та інших аспектів для підтримки впливу та досягнення мети без застосування примусу. Вона передбачає використання інформаційних ресурсів для формування позитивного іміджу країни, сприяння розвитку культурного та освітнього обміну, підтримки громадянського суспільства тощо.

2. «Гостра» сила – ця концепція відноситься до застосування силових або стримуючих заходів у відповідь на загрози або напади у кіберпросторі. Вона орієнтована на захист національних інтересів в умовах кібератак або інших форм кіберзагроз, забезпечення безпеки важливих систем та мереж інфраструктури.

Врахування цих концепцій відображає сучасні виклики та можливості інформаційної безпеки в контексті міжнародних відносин. Забезпечення національної безпеки через інноваційні технології та одночасна підтримка міжнародної співпраці стають важливими компонентами стратегії країни в умовах глобальних змін у сфері інформаційної безпеки.

Так, в Україні спостерігається значний рівень розвитку наукової та прикладної діяльності у сфері інформаційної безпеки. Наукові школи, дослідницькі центри, визначні вчені та експерти активно працюють над вирішенням проблем, пов’язаних з інформаційною безпекою.

Важливим є те, що дослідження проводяться як у загальних теоретичних аспектах інформаційної безпеки, так і у специфічних напрямках, таких як кібербезпека, захист важливих інформаційних систем, захист особистої інформації громадян тощо. Результати цих досліджень можуть бути

застосовані при формуванні та реалізації національних стратегій і політик у сфері національної безпеки, враховуючи значущість інформаційного аспекту у сучасному світі.

Враховуючи актуальність цих досліджень та їх потенційні можливості для розробки ефективних стратегій забезпечення національної безпеки, українська наукова спільнота може бути ключовим партнером у вирішенні складних завдань інформаційної безпеки України.

Критичний розгляд понятєвих категорій інформаційної безпеки необхідний у зв'язку з постійними змінами у технологіях, суспільстві та геополітичних реаліях. Розвиток інформаційних технологій породжує нові загрози і вимагає удосконалення підходів до захисту інформації, систем та мереж.

Деякі усталені поняття в сфері інформаційної безпеки, такі як кіберзагрози, кіберзлочинність, кібератаки, залишаються актуальними, проте їх визначення та відповідні стратегії захисту потребують постійного оновлення, оскільки технічні засоби і підходи змінюються.

Нові категорії, такі як гібридні війни, хактивізм, кліктивізм, бот-мережі, ботоферми, тролінг, квантум-безпека, covid-безпека, відображають сучасні тенденції та виклики у сфері інформаційної безпеки. Наприклад, гібридні війни описують поєднання різних форм впливу на суспільство, включаючи інформаційні аспекти, що стають інструментом геополітичних конфліктів. Квантум-безпека та covid-безпека відображають нові виміри захисту інформації у зв'язку з розвитком квантових технологій.

Міжнародні організації, такі як ООН, НАТО, ОБСЄ та інші, розвивають стратегії інформаційної та кібербезпеки, враховуючи появу нових гібридних загроз. Вони мають відмінний статус у системі міжнародних відносин та різні компетенції щодо політики безпеки, що призводить до варіаційних підходів у їх розробці і реалізації.

Проблема забезпечення інформаційної безпеки на міжнародному рівні полягає у бажанні деяких світових акторів контролювати політичні процеси на

значних територіях за допомогою спеціальних інформаційно-психологічних та кібернетичних операцій. Це створює інформаційний дисбаланс сил у міжнародних взаємодіях, що може впливати на стабільність і безпеку.

Практичне забезпечення політики інформаційної безпеки у діяльності міжнародних організацій вимагає стратегічної спрямованості на:

1. Розвиток спільних підходів. Забезпечення співпраці та розробка спільних стратегій для підтримання міжнародного миру та захисту критичних систем міжнародних акторів.

2. Запобігання використанню інформаційних технологій як зброї. Міжнародні організації мають розвивати механізми для уникнення використання досягнень науки і технологій у сфері інформаційної безпеки як засобів масового ураження або для агресивних цілей.

3. Попередження війн «четвертого покоління». Міжнародні організації здійснюють дії для попередження конфліктів, які характеризуються широким використанням інформаційних технологій, кібернетичних атак та гібридних загроз.

Забезпечення інформаційної безпеки на міжнародному рівні вимагає співпраці та розвитку консенсусу між різними акторами з метою запобігання потенційним загрозам та забезпечення стабільності у світі.

Аналіз інформаційної складової стратегії безпеки США під різними президентськими адміністраціями відображає різні підходи до включення цієї складової у національні стратегії безпеки.

Під час президентства Б. Обами концепція «розумної сили» стала основою забезпечення переваг США в міжнародній конкуренції за лідерство. Одним з пріоритетів стала кібербезпека, розглянута як важлива складова національної безпеки та оборони. Підкреслено, що інформаційна інфраструктура та цифровий простір є стратегічними національними активами, які потребують захисту від кіберзагроз.

Під час президентства Д. Трампа була ухвалена перша Національна стратегія кібербезпеки США, в рамках якої зазначено заходи для захисту

мереж, інформації та критичної інфраструктури. Основні пріоритети цієї стратегії включають протидію кіберзлочинності та кібератакам, встановлення відповідальності за поведінку в кіберпросторі, дотримання норм міжнародного права, що стосуються конфіденційності урядової інформації та американських принципів захисту кіберпростору.

Ці стратегії також націлені на створення коаліцій союзних держав для узгодження позицій та спільної протидії кіберзагрозам. Такі різні підходи відображають еволюцію стратегій кібербезпеки та підходів до захисту інформаційних інфраструктур, що відбувається в залежності від політичних пріоритетів, технологічних змін та зростання кіберзагроз.

В контексті політики інформаційної безпеки в провідних країнах Європейського Союзу (ЄС) можна виділити спільні пріоритети, але й відмінності у їх стратегіях та діях. Важливими елементами є співробітництво у захисті інформаційного середовища та інфраструктури, поглиблення взаємодії з приватним сектором, а також запобігання гібридним загрозам, які можуть включати інформаційно-психологічні впливи та кібератаки.

Франція зосереджується на поглибленні міждержавного співробітництва у сфері інформаційної безпеки ЄС, підтримці спеціальних структур для управління інформаційними впливами та впровадженні регулятивних норм у сфері кібербезпеки.

Стратегія інформаційної безпеки Німеччини включає заходи щодо захисту інформаційної незалежності та критичної інфраструктури від кіберзагроз, але зазнала втрат через кібератаки у важливих сферах життєзабезпечення, спричинені інноваційними технологіями. Ці виклики вимагають відповідної реакції від урядових структур, зокрема Федерального міністерства оборони, Бундесверу та МЗС.

Відмінності між стратегіями визначаються різними підходами до пріоритетних напрямків дій у кіберпросторі, а також рівнем вразливості перед кіберзагрозами та готовності реагувати на них.

Інституціональні засади інформаційної безпеки в Україні базуються на різних рівнях правових документів, які регулюють інформаційні відносини, ресурси та діяльність в інформаційному середовищі країни. Деякі з найважливіших документів включають:

1. Закони: Закон «Про основи національної безпеки України», Закон «Про основні засади забезпечення кібербезпеки України».

2. Доктрини та концепції: Доктрина «Про Доктрину інформаційної безпеки України», Концепція розвитку сектору безпеки і оборони України.

3. Стратегії та програми: Стратегія кібербезпеки України та відповідні програми, спрямовані на регулювання інформаційної сфери та актуалізацію доктринальних і стратегічних документів.

Ці правові акти мають важливе значення для забезпечення інформаційної безпеки в Україні. Однак, існують підзаконні акти, що потребують удосконалення, оскільки їхні положення можуть викликати дискусії через нечіткі визначення чи наближені норми. Подальше удосконалення таких актів та їх адаптація до нових викликів і контексту інформаційної безпеки може бути важливим для покращення цілісності та ефективності політики інформаційної безпеки в Україні.

Комунікативний інструментарій у сфері інформаційної безпеки має важливе значення для просування та захисту інтересів держави на міжнародній арені, а також для переконання внутрішньої та зовнішньої громадськості у правильності прийнятих рішень політичними та безпековими інститутами стосовно захисту основних пріоритетів країни.

Політика інформаційної безпеки України на стратегічному рівні зосереджена на захисті національних інтересів та зміцненні безпеки країни на національному, регіональному та міжнародному рівнях. Оскільки інформаційна безпека виступає ключовим фактором в сучасному світі, ця політика є важливою складовою зовнішньополітичної діяльності України та спрямована на протидію гібридним загрозам.

Важливими аспектами стратегії інформаційної безпеки України є:

1. Протидія гібридним загрозам. Створення захисного механізму проти гібридних війн, які включають деструктивні інформаційні втручання, енергетичні або газові інформаційні воєнні та інші форми агресії для спровокування внутрішніх суперечностей та негативних реакцій в суспільстві.

2. Зміцнення міжнародної безпеки. Політика інформаційної безпеки спрямована на підвищення обізнаності та мобілізацію міжнародної співпраці для захисту країни від зовнішніх загроз.

3. Прозорість та інформаційна відкритість. Забезпечення прозорості та доступності інформації для громадськості є важливим елементом політики, що сприяє захисту від деструктивного впливу.

4. Захист внутрішньополітичних процесів. Захист від інформаційних атак, спрямованих на спровокування внутрішньополітичних конфліктів та негативного впливу на рішення, пов’язані зі справами країни.

Ці стратегічні пріоритети інформаційної безпеки в Україні спрямовані на забезпечення захисту держави від зовнішніх та внутрішніх загроз, а також на збереження стабільності та безпеки на різних рівнях – від національного до міжнародного.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Daßler B., Kruck A., Zangl B. Interactions between hard and soft power: The institutional adaptation of international intellectual property protection to global power shifts // European Journal of International Relations, 2018. URL: https://journals.sagepub.com/doi/abs/10.1177/1354066118768871.

2. Nye J. Smart Power // Belfer Center, 2008. URL: https://www.belfercenter.org/publication/joseph-nye-smart-power.

3. Information Technology Security Evaluation Criteria (ITSEC), Luxembourg: Office for Official Publications of the European Communities, 1991. URL: https://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf

4. Копійка М.В. Понятійно-категоріальні характеристики інформаційної безпеки // Вісник Львівського національного університету. Серія «Міжнародні відносини», Вип. 46, 2019, с. 169-181, DOI: http://dx.doi.org/10.30970/vir.2019.46.0

5. Starr Forum: The Assault on Intelligence: American National Security in an Age of Lies // Center for International Studies, 2020. URL: http://cis.mit.edu/events/transcripts/starr-forum-assault-intelligence-american-nationalsecurity-age-lies

6. Nye J.S., The Decline of America's Soft Power: Why Washington Should Worry. Foreign Affairs,Vol. 83, No. 3 (May - Jun., 2004), pp. 16-20

7. Lundgren, B., Möller, N. Defining Information Security // Science and Engineering Ethics, 25, 419–441 (2019). URL: https://link.springer.com/article/10.1007/s11948-017-9992-1

8. Hoffman F. Hybrid vs Compound War // Small Wars Journal, 2009. URL: http://smallwarsjournal.com/blog/journal/docs–temp/189–hoffman.pdf

9. Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналіт. доп. / за заг. ред. А. Баровської, К.: НІСД, 2016, 109 с.

10. Don B.W., Frelinger D.R., Gerwehr S., Landree E., Jackson B.A. Network Technologies for Networked Terrorists. Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations, RAND Corporation, 2007. URL: http://www.rand.org/pubs/technical_reports/TR454.html

11. Hate speech and violence // Council of Europe, 2020. URL: https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/hatespeech-and-violence

12. Curtis W. M. Hate speech // Encyclopedia of Political Theory, 2010. URL: https://www.britannica.com/topic/hate-speech

13. Sedova I., Pechonchyk T., others. Hate Speech in the Media Landscape of Crimea: An Information and Analytical Report on the Spread of Hate Speech on the Territory of the Crimean Peninsula, Kyiv, 2018, 40 p.

14. Clicktivism // Oxford Dictionaries, 2023. URL: https://en.oxforddictionaries.com/definition/clicktivism

15. Буряк А.А., Маховка В.М., Сторожук Л.М. Стратегія і механізми запровадження цифрової економіки в країнах ЄС та Україні як умова подолання кризових явищ. Економіка і регіон. 2023. № 2(89). С. 53–59.

16. Howard E. How 'clicktivism' has changed the face of political campaigns // The Guardian, 2014. URL: https://www.theguardian.com/society/2014/sep/24/clicktivism-changed-politicalcampaigns-38-degrees-change

17. Nye J.S. The Paradox of American Power: Why the World’s Only Superpower Can’t Go it Alone. New York: Oxford University Press, 2002, 240 p.

18. Libicki M.C. What is Information Warfare // National Defense University Strategic Forum, Washington D.C.: National Defense University, 1995, 105 p.

19. Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge: Cambridge University Press, 2007, 336 p.

20. Lynn W.J. Defending a New Domain. The Pentagon's Cyberstrategy // Foreign Affairs, 2010, Vol. 89, No. 5, p. 97-108. URL: https://www.law.upenn.edu/live/files/6465-12-lynn-defending-a-new-domainpdf

21. Bunker R.J. Generations, Waves, and Epochs. Modes of Warfare and the RPMA // Air Power Journal, URL: https://scholarship.claremont.edu/cgi/viewcontent.cgi?article=1138&context=cgu_fac_pub

22. Taleb N. The Black Swan: the Impact of the Highly Improbable. Penguin, 2008, 446 p.

23. Світова гібридна війна: український фронт / За заг. ред. В. П. Горбуліна. Національний інститут стратегічних досліджень, К.: НІСД, 2017, 496 с.

24. Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: Монографія, К.: НІСД, 2003, 239 с.

25. Ожеван М.А. Інформаційна стратегія нового президента США Барака Обами // Актуальні проблеми міжнародних відносин. К., 2010, Вип. 93, Ч. І, с. 20-25.

26. Ожеван М.А. Глобальна війна гранд-наративів у сучасну добу // Стратегічні комунікації в міжнародних відносинах: Монографія, Київ: Вадекс, 2019, с. 60.

27. Дубов Д.В Кіберпростір як новий вимір геополітичного суперництва : Монографія, К.: НІСД, 2014, 328 с.

28. Дубов Д.В Державна інформаційна політика України в умовах гібридного миру та війни // Стратегічні пріоритети, 2016, № 3, с. 86-93.

29. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова, К.: НІСД, 2018, 84 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavnpryvatn_partnerstvo_Ciberbezpeka.pdf

30. Почепцов Г. Інформаційні війни. К.: Ваклер, 2001, 576 с.; Почепцов Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війнах, Київ : Києво-Могилянська акад., 2016, 316 с.

31. Зовнішня та безпекова політика США: аналітичні дослідження. Монографія // Макаренко Є.А., Рижков М.М., Погорська І.І., Піпченко Н.О., К.: Центр вільної преси, 2016, 456 с.

32. Макаренко Є.А. Національна ідея як інструмент деструктивних стратегічних комунікацій // Стратегічні комунікації у міжнародних відносинах. Монографія. К.: Вадекс, 2019, с. 369-407.

33. Андрєєва О.М. Національна безпека України в контексті національної ідентичності і взаємовідносин з Росією, К.: Парламентське вид-во, 2009, 360 с.

34. Бєлоусова Н.Б. Концептуальні підходи до визначення природи й сутності «сили» в зовнішній політиці держави // Регіональні стратегії США і Європи: зовнішньополітичний і безпековий вимір. Монографія, К. : Центр вільної преси, 2016, с. 81-105.

35. Даниленко С. І. Політико-правовий вимір інформаційного суспільства в Україні: здобутки та проблеми на шляху до ЄС // Stosunki polsko-ukrainskie 1991-2014, Wydawnictwo UMCS: Lublin, 2016, с. 333-346.

36. Kapitonenko M., Ukrainian crisis as an ongoing threat to regional security. Studia Politica. Vol. XVI, no. 1 (2016), p. 9-20. URL: http://www.studiapolitica.eu/Archive/2016/studia-politica-vol-xvi-no-1-2016-1.

37. Кучмій О.П. Інформаційна безпека США у сучасних зарубіжних дослідженнях. // Регіональні стратегії США і Європи: зовнішньополітичний і безпековий вимір. Монографія, К.: Центр вільної преси, 2016, с. 106-138.

38. Мінгазутдінов І., Мінгазутдінова Г. Стратегічні комунікації європейських країн: Велика Британія, Франція, ФРН // Стратегічні комунікації в міжнародних відносинах. Монографія, К.: Вадекс, 2019, с.254-285.

39. Pipchenko Nataliya, Makarenko Ievgeniia and Ryzhkov Mykola. Current Challenges to the EU Integration Policy. On-Line Journal Modelling the

New Europe, № 31/2019, p. 37-60. DOI: https://doi.org/10.24193/OJMNE.2019.31.03.

40. Рижков М.М. Стратегії політики США: від стримування до глобальної демократизації // Зовнішня та безпекова політика США: аналітичні дослідження: Монографія, К.: Центр вільної преси, 2016, с. 9-118.

41. Романенко Ю.В. Маніпулювання макроідентичністю в масових комунікаціях: до постановки проблеми // Грані, 2013, № 8 (100). URL: https://core.ac.uk/download/pdf/268618786.pdf.

42. Фролова О.М. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки // Вісник Львівського університету. Серія міжнародні відносини, 2019, Вип. 46, с. 123-136.

43. Frolova O. EU role in ensuring international information security // Political Sciences, Issue 14/ 2019, p. 89-102.

44. Тихомирова Є.Б. Комунікативна політика ЄС: інформаційна безпека vs транспарентність // Actual Problems of International Relations, Т. 1, № 102 (2011). URL: http://journals.iir.kiev.ua/index.php/apmv/article/view/2112.

45. Карпчук Н. Медіа як невоєнний метод упливу в гібридній війні // Міжнародні відносини, суспільні комунікації та регіональні студії, 2018, № 2 (4), с. 41-49.

46. Копійка М. В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки // Політичне життя, №1 (2020), с. 102-109.

47. Andreatos A., Benias N. and others. Cyber-Security and Information Warfare. Ed. By N. J. Daras. Nova, 2018, 397 p.

48. Bachmann S.D. The emergence of hybrid warfare // Bournemouth University, 2020. URL: https://www.bournemouth.ac.uk/research/projects/emergence-hybrid-warfare

49. Nye J.S. Cyber Power. Cambridge: pub by Belfer Center for Science and International Affairs, 2010, 26 p.

50. Friedman N. Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars. Naval Institute Press, 2009, 360 p.

51. Ожеван М.А. Глобальна війна гранд-наративів у сучасну добу // Стратегічні комунікації в міжнародних відносинах. Монографія. К.: Вадекс, 2019, 442 с.

52. Фролова О.М. Роль ООН в системі міжнародної інформаційної безпеки // Міжнародні відносини. Серія: Політичні науки, № 18 (2018). URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468

53. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security // UN. Secretary-General, 2017. URL: https://digitallibrary.un.org/record/1301308

54. Advancing responsible State behavior in cyberspace in the context of international security: resolution // General Assembly, 2019, A/RES/74/28. URL: https://digitallibrary.un.org/record/3839870?ln=en

55. Henriksen A. The end of the road for the UN GGE process: the future regulation of cyberspace // Journal of Cybersecurity, Volume 5, Issue 1, 2019. URL: https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865

56. NATO Cooperative Cyber Defence Centre // NATO CCDCOE, 2020. URL:https://www.cybersecurityintelligence.com/nato-cooperative-cyber-defence-centre-ccdcoe395.html

57. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched // NATO CCDCOE, 2017. URL: https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html.

58. Україна стала учасником Партнерства розширених можливостей НАТО, орієнтованої на взаємозамінюваність важливих партнерів Альянсу // Міністерство оборони України, 2020. URL: https://www.mil.gov.ua/news/2020/07/24/programarozshirenih-mozhlivostej-nato-dlya-ukraini/

59. Уряд ухвалив проект Річної національної програми під егідою Комісії Україна-НАТО на 2022 рік // Кабінет Міністрів України.

URL:https://www.kmu.gov.ua/news/uryad-uhvaliv-proekt-richnoyi-nacionalnoyi-programi-pid-egidoyu-komisiyi-ukrayina-nato-na-2022-rik

60. Organization for Security and Cooperation in Europe // OSCE, 2023. URL: https://www.osce.org/whatistheosce

61. Austrian OSCE Chairmanship Conference on Cyber Security // OSCE, 2017. URL: https://www.osce.org/event/austrian-cyber-security-2017

62. Cyber/ICT Security for a safer future: The OSCE's role in fostering regional cyber stability // OSCE, 2019. URL: https://polis.osce.org/cyberict-security-safer-futureosces-role-fostering-regional-cyber-stability

63. Копійка М.В. Стратегічні ризики інформаційної безпеки європейських країн // Міжнародні та політичні дослідження, 2019, Вип. 3, с. 85-100. URL: http://heraldiss.onu.edu.ua/article/view/173847/1938231

64. Америка і Європа у сучасних міжнародних трансформаціях. Монографія, К.: Центр вільної преси, 2014, 472 с.

65. Hoehn A. R., Parasiliti A., Efron S., Strongin S. Discontinuities and Distractions-Rethinking Security for the Year 2040, RAND Corporation, 2018. URL:https://www.rand.org/pubs/conf_proceedings/CF384.html

66. A Global Strategy for the European Union's Foreign and Security Policy // European External Action Service, 2016. URL:https://www.iss.europa.eu/sites/default/files/EUISSFiles/EUGS_0.pdf

67. Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats // European Commission, 2016. URL:https://ec.europa.eu/regional_policy/en/newsroom/news/2016/07/07-05-2016-commission-signs-agreement-with-industry-on-cybersecurity-and-steps-up-efforts-totackle-cyber-threats

68. The Global State of Information Security // PwC Survey, 2018. URL:https://www.pwc.com/us/en/services/consulting/cybersecurity/library/informationsecurity-survey.html

69. Digital Trust Insights // PwC Survey, 2018. URL:https://www.pwc.ru/en/publications/2018-insights.html

70. National Cyber Security Strategies Guidelines & tools // ENISA. URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cybersecurity-strategies-guidelines-tools

71. Handbook on Security of Personal Data Processing // ENISA, 2018. URL:https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-dataprocessing

72. General Data Protection Regulation (GDPR) // Proton Technologies AG, 2023. URL: https://gdpr.eu/tag/gdpr/

73. European Agenda on Security // European Commission. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/elibrary/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

74. Kriz D. A Global Model: UK's «National Cyber Security Strategy» // SecurityRoundtable.org, 2017. URL: https://www.securityroundtable.org/global-modeluks-national-cyber-security-strategy/

75. French national digital security strategy // ANSSI, 2016. URL:https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategymeeting-the-security-challenges-of-the-digital-world/

76. Agence nationale de la sécurité des systèmes d'information // ANSSI, 2023. URL: https://www.ssi.gouv.fr/en/cybersecurity-in-france/

77. Laudrain A. France's New Offensive Cyber Doctrine // Lawfare, 2019. URL:https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

78. Бойко В.О. Досвід Німеччини у функціонуванні платформ державноприватного партнерства в сфері кібербезпеки // НІСД, 2018. URL:http://old2.niss.gov.ua/content/articles/files/1_AZ_Boyko_var77_FIN-4d2ef.pdf

79. Diplomacy Development, and Security in the Information Age. Kalathil Sh. and in the Arsène S., Faris D., Granger S., Hayden. URL: https://cpb-use1.wpmucdn.com/blogs.roosevelt.edu/dist/a/14/files/2010/09/Diplomacy_Development_Security_in_the_Information_Age-1.pdf

80. Banerjee S. National Security Strategy Trump and Obama // Indian Council of World Affairs. URL: https://www.researchgate.net/publication/322355672_National_Security_Strategy_Trump_ and _Obama

81. Lisle J., Cozen S. Political Warfare, Sharp Power, the U.S., and East Asia // Foreign Policy Research Institute, 2020. URL:https://www.fpri.org/article/2020/04/editors-corner-spring-2020-political-warfaresharp-power-the-u-s-and-east-asia/

82. Nye J. Soft Power, Hard Power and Leadership, 2012. URL:https://numerons.files.wordpress.com/2012/04/soft-power-hard-power-andleadership.pdf

83. Gray C. S. Hard power and soft power: the utility of military force as an instrument of policy in the 21st century. SSI Monograph, 2011, 60 p. URL:https://www.files.ethz.ch/isn/128690/pub1059-1.pdf

84. National Security Strategy of the United States // The White House. URL: http://nssarchive.us/NSSR/1990.pdf

85. США і світ XXI століття: монографія / Пахомов Ю.М., Коваль І.М., Шергін С.О. та ін., К: Центр вільної преси, 2013, 620 с.

86. Wong-Diaz F. Smart Power and U.S. National Strategy. Monograph. Press Mac Dill Air Force Base, Florida, 2013. URL:https://www.socom.mil/JSOU/JSOUPublications/JSOU13-3_Wong-Diaz_SmartPower.pdf

87. Marks J. Obama's Cyber Legacy: He Did (Almost) Everything Right and It Still Turned Out Wrong // Nextgov. URL:https://www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy-he-did-almosteverything-right-and-it-still-turned-out-wrong/134612/

88. National Security Strategy of the United States of America // The White House, 2017. URL: http://nssarchive.us/wp-content/uploads/

89. Тихоненко І. В. Стратегія національної безпеки США як інструмент підтримки глобального лідерства та міжнародного порядку за адміністрації Б.Обами та Д.Трампа // Політичне життя, 2018, № 1, с. 158-163.

90. Національна безпека в умовах інформаційних і гібридних війн: монографія; за ред. В. Куйбіди, В. Бебика, К.: НАДУ, 2019, 384 с.

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

92. Дубов Д.В. Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні. // НІСД. URL:http://www.niss.gov.ua/articles/1466/

93. Закон України «Про національну безпеку України» // Верховна Рада України, 2018. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

94. Дмитренко М.А. Проблемні питання інформаційної безпеки України // Міжнародні відносини Серія «Політичні науки» (спецвипуск), No 17 (2017). URL:http://journals.iir.kiev.ua/index.php/pol_n/issue/view/194

95. Бебик В.М. Інформаційний простір як театр військових дій: війська, зброя, розвідка, контррозвідка // Міжнародні відносини Серія «Політичні науки», № 18-19 (2018). URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3391

96. Інформаційна безпека та кібербезпека держави //Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 р.», К.: НІСД, 2017, с. 47-55.

97. Goldman E. Strategic Communication: A Tool for Asymmetric Warfare // Small Wars Journal, 2007. URL: http://smallwarsjournal.com/blog/strategic–communication–a–tool–for–asymmetric–warfare

98. Стратегічні комунікації в міжнародних відносинах. Монографія, К.: Вадекс, 2019, с. 343- 368.

99. Buriak A.A., Ovcharenko D.O. Media information support of enterprises engaged in foreign economic activity. Економіка і регіон. 2020. 1(76). С. 132–139. DOI 10.26906/EiR.2020.1(76).1927. URL: http://journals.nupp.edu.ua/eir/article/view/1927/1584

100. Почепцов Г. Війни без воєн: зовнішні інформаційні інтервенції // The Independent View, 2018. URL: http://independentview.net/2018/03/26/vijny-bez-vojenzovnishni-informatsijni-interventsiji/

101. Ожеван М.А. Основні напрями зовнішніх інформаційноманіпулятивних впливів на суспільні трансформації в Україні: засоби протидії // Стратегічні пріоритети, №3 (20), К.: НІСД, 2011, с.118-126

102. Danylenko S., Nesteriak Y., Grynchuk M. National Media as a Projection of a Devastating Effect of External Influences. Przegląd Strategiczny. Nr 11 (2018), p. 185-200. DOI: URL: https://doi.org/10.14746/ps.2018.1.13

103. Quantum Technologies Flagship // European Commission, 2020. URL: https://ec.europa.eu/digital-single-market/en/quantum-technologies.

ДОДАТКИ

Додаток А

Abstract

The concept of «soft/intelligent» and «sharp» power in the concept of information security reflects two important aspects of the application of modern information technologies in the field of international economic relations:

1. «Soft/smart» power – this concept refers to the use of information technology, diplomacy, cultural exchanges and other aspects to maintain influence and achieve a goal without the use of coercion. It involves the use of information resources to form a positive image of the country, promote the development of cultural and educational exchange, support civil society, etc.

2. «Hard» force – this concept refers to the use of force or deterrent measures in response to threats or attacks in cyberspace. It is aimed at protecting national interests in the face of cyber attacks or other forms of cyber threats, ensuring the security of important infrastructure systems and networks.

Consideration of these concepts reflects modern challenges and opportunities of information security in the context of international relations. Ensuring national security through innovative technologies and simultaneously supporting international cooperation are becoming important components of the country's strategy in the face of global changes in the field of information security.

Thus, a significant level of development of scientific and applied activity in the field of information security is observed in Ukraine. Scientific schools, research centers, prominent scientists and experts are actively working on solving problems related to information security.

It is important that research is conducted both in general theoretical aspects of information security and in specific directions, such as cyber security, protection of important information systems, protection of personal information of citizens, etc.

The results of these studies can be applied in the formation and implementation of national strategies and policies in the field of national security, taking into account the importance of the information aspect in the modern world.

Given the relevance of these studies and their potential for developing effective strategies for ensuring national security, the Ukrainian scientific community can be a key partner in solving complex tasks of Ukraine's information security.

Critical consideration of conceptual categories of information security is necessary in connection with constant changes in technologies, society and geopolitical realities. The development of information technologies creates new threats and requires the improvement of approaches to the protection of information, systems and networks.

Some established concepts in the field of information security, such as cyberthreats, cybercrime, cyberattacks, remain relevant, but their definitions and corresponding protection strategies require constant updating, as technical means and approaches change.

New categories such as hybrid warfare, hacktivism, clicktivism, bot networks, bot farms, trolling, quantum security, covid security reflect current trends and challenges in the field of information security. For example, hybrid wars describe a combination of various forms of influence on society, including informational aspects, which become a tool of geopolitical conflicts. Quantum security and covid security reflect new dimensions of information protection due to the development of quantum technologies.

International organizations such as the UN, NATO, OSCE and others are developing information and cyber security strategies, taking into account the emergence of new hybrid threats. They have an excellent status in the system of international relations and different competences regarding security policy, which leads to variation approaches in their development and implementation.

The problem of ensuring information security at the international level is the desire of some world actors to control political processes in large territories with the help of special informational, psychological and cybernetic operations. This creates an information imbalance of forces in international interactions, which can affect stability and security.

Practical provision of information security policy in the activities of international organizations requires a strategic focus on:

1. Development of joint approaches. Ensuring cooperation and developing joint strategies to maintain international peace and protect critical systems of international actors.

2. Preventing the use of information technology as a weapon. International organizations should develop mechanisms to avoid the use of science and technology achievements in the field of information security as means of mass destruction or for aggressive purposes.

3. Prevention of «fourth generation» wars. International organizations take actions to prevent conflicts, which are characterized by the wide use of information technologies, cybernetic attacks and hybrid threats.

Ensuring information security at the international level requires cooperation and development of consensus among various actors in order to prevent potential threats and ensure stability in the world.

An analysis of the information component of the US security strategy under different presidential administrations reflects different approaches to the inclusion of this component in national security strategies.

During the presidency of B. Obama, the concept of «intelligent power» became the basis for ensuring the advantages of the United States in the international competition for leadership. One of the priorities was cyber security, considered as an important component of national security and defense. It is emphasized that information infrastructure and digital space are strategic national assets that need protection from cyber threats.

During the presidency of D. Trump, the first US National Cyber Security Strategy was adopted, which outlines measures to protect networks, information and critical infrastructure. The main priorities of this strategy include combating cybercrime and cyberattacks, establishing accountability for behavior in cyberspace, compliance with international law related to the confidentiality of government information, and American principles of cyberspace protection.

These strategies are also aimed at creating coalitions of allied states to coordinate positions and jointly counter cyber threats. These different approaches reflect the evolution of cybersecurity strategies and approaches to protecting information infrastructures, which is taking place depending on political priorities, technological changes and the growth of cyber threats.

In the context of information security policy in the leading countries of the European Union (EU), common priorities can be identified, but also differences in their strategies and actions. Important elements are cooperation in protecting the information environment and infrastructure, deepening cooperation with the private sector, as well as prevention of hybrid threats, which may include informational and psychological influences and cyber attacks.

France is focusing on deepening interstate cooperation in the field of EU information security, supporting special structures for managing information impacts and implementing regulatory norms in the field of cyber security.

Germany1s information security strategy includes measures to protect information independence and critical infrastructure from cyber-threats, but has suffered losses from cyber-attacks in critical areas of life support caused by innovative technologies. These challenges require an appropriate response from government structures, in particular the Federal Ministry of Defence, the Bundeswehr and the Ministry of Foreign Affairs.

The differences between the strategies are determined by different approaches to priority areas of action in cyberspace, as well as the level of vulnerability to cyber threats and readiness to respond to them.

The institutional foundations of information security in Ukraine are based on various levels of legal documents that regulate information relations, resources and activities in the country’s information environment. These legal acts are important for ensuring information security in Ukraine. However, there are by-laws in need of improvement, as their provisions may cause debate due to unclear definitions or approximate norms. Further improvement of such acts and their adaptation to new

challenges and information security context may be important for improving the integrity and effectiveness of information security policy in Ukraine.

Communicative tools in the field of information security are important for promoting and protecting the interests of the state in the international arena.

Ukraine’s information security policy at the strategic level is focused on protecting national interests and strengthening the country's security at the national, regional and international levels. Since information security is a key factor in the modern world, this policy is an important component of Ukraine's foreign policy and is aimed at countering hybrid threats.

Important aspects of Ukraine’s information security strategy are:

1. Countering hybrid threats. Creation of a protective mechanism against hybrid wars, which include destructive information interventions, energy or gas information warfare and other forms of aggression to provoke internal contradictions and negative reactions in society.

2. Strengthening international security. Information security policy is aimed at raising awareness and mobilizing international cooperation to protect the country from external threats.

3. Transparency and information openness. Ensuring transparency and availability of information to the public is an important element of policy that helps protect against destructive influence.

4. Protection of domestic political processes. Protection against information attacks aimed at provoking internal political conflicts and negatively influencing decisions related to the affairs of the country.

These strategic priorities of information security in Ukraine are aimed at ensuring the protection of the state from external and internal threats, as well as at maintaining stability and security at various levels - from national to international.