Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

КАНАРСЬКИЙ ВОЛОДИМИР СЕРГІЙОВИЧ

УДК 351.86:659.3/.4:316.65](470:477)"364"

ДИСЕРТАЦІЯ

ПУБЛІЧНО-УПРАВЛІНСЬКІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Спеціальність - 281 Публічне управління та адміністрування
Галузь знань - 28 Публічне управління та адміністрування
Подається на здобуття наукового ступеня доктора філософії у галузі публічного управління та адміністрування

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Володимир Канарський

Науковий керівник – **Шипілова Лариса Миколаївна,**
кандидат політичних наук, доцент.

КИЇВ - 2023

АНОТАЦІЯ

Канарський В.С. Публічно-управлінські механізми забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни. - Кваліфікаційна наукова праця на правах рукопису. – Київ, 2023.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 28 Публічне управління та адміністрування за спеціальністю 281 «Публічне управління та адміністрування». - Київський національний університет імені Тараса Шевченка, Міністерство освіти і науки України. - Київ, 2023.

Наукова новизна одержаних результатів полягає в тому, що дисертаційна робота є комплексним дослідженням, у якому вирішено актуальне для вітчизняної науки «Публічне управління та адміністрування» завдання з обґрунтування теоретичних положень і методологічних підходів дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки та на підставі комплексного аналізу міжнародно-правових стандартів у сфері інформаційної безпеки і досвіду зарубіжних країн щодо використання публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки, науково обґрунтовано пропозиції з удосконалення цих механізмів в Україні. Розроблено основні положення Проекту документа стратегічного планування - «Концепція інформаційно-психологічної безпеки України», що представляє собою систему поглядів на забезпечення інформаційно-психологічної безпеки, як частини інформаційної та національної безпеки України. У зазначеному проекті відображено основні загрози інформаційно-психологічній безпеці України; цілі, завдання, принципи та пріоритетні напрямки діяльності уповноважених органів державної влади, організацій та інших суб'єктів, що беруть участь у забезпеченні інформаційно-психологічної безпеки відповідно до законодавства України.

Дисертантом *уперше* розроблено наукову концепцію правової інституціоналізації інформаційно-психологічної безпеки (ІПБ) в системі

інформаційного права України з позицій публічного управління з урахуванням міждисциплінарного підходу. У дисертації обґрунтовано наукову модель інформаційно-психологічної безпеки, що включає дефініції базових понять, об'єкти захисту, зміст та види деструктивного інформаційно-психологічного впливу. Доведено необхідність введення в правову систему та управлінську практику поняття «інформаційно-психологічна безпека», що детерміновано: а) потребою у термінологічному позначенні «психологічної» складової інформаційної безпеки; б) специфікою системи інформаційної безпеки; в) наявністю чіткої межі між захистом інформації та інформаційно-психологічною безпекою за критеріями та методами впливу на об'єкт; г) існуванням комплексу специфічних загроз; д) спільністю правового інструментарію, що використовується для захисту від різних форм деструктивного інформаційно-психологічного впливу.

Дисертантом *удосконалено* систему загроз інформаційно-психологічній безпеці та запропоновано її типологізація, що дозволило виділити основні групи таких загроз: а) контентні, пов'язані з поширенням негативних (шкідливих) відомостей у засобах масової інформації та інших джерелах; б) комунікаційні, що включають деструктивне міжособистісне або групове спілкування.

Встановлено, що основними контентними загрозами є такі види повідомлень, які: а) пропагують чи виправдовують війну та інші міжнародні злочини, тероризм; б) розпалюють ненависть і ворожнечу у суспільстві; в) стимулюють та сприяють скоєнню злочинів чи інших суспільно небезпечних дій; г) фальсифікують історію або оскверняють історичну пам'ять; д) сіють страх; е) мають помилковий або спотворений характер; ж) принижують (зневажають) честь, гідність та ділову репутацію особи або які ображають суспільну моральність; з) носять порнографічний та інший сексуально відвертий характер.

Серед основних комунікаційних загроз визначено такі форми деструктивного спілкування: а) публічні заклики та інші форми підбурювання

до скоєння протиправних та інших суспільно небезпечних дій; б) вербування та інші форми залучення у вчинення протиправних чи інших суспільно небезпечних процесів; в) розпалювання ненависті чи ворожнечі; г) фальсифікація історії чи образу історичної пам'яті; д) обман (дезінформація); е) маніпуляція свідомістю; ж) залякування та примус; з) образа та інші форми приниження людської гідності.

Розроблено матрицю загроз інформаційно-психологічної безпеки (ІПБ), що відображає широкий спектр загроз ІПБ у політичній, соціальній, культурній та міжнародній сферах.

Набули подальшого розвитку підходи до: визначення національних інтересів в інформаційній сфері та надано їх авторське тлумачення; визначення мети, завдань та напрямів забезпечення ІПБ та на основі аналізу нормативно-правових документів України у сфері інформаційної безпеки визначено додаткові завдання із забезпечення ІПБ. Здобувачем розроблено Паспорт загроз інформаційній безпеці, визначено завдання та функції забезпечення ІПБ.

Також уточнено поняття: *публічно-управлінський механізм забезпечення інформаційно-психологічної безпеки; інформаційно-психологічна безпека; політико-правовий механізм; правове забезпечення ІПБ; система правового забезпечення ІПБ.*

В дисертації викладено практичні пропозиції щодо удосконалення публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки, визначені заходи з її забезпечення, які поділені на 4 групи: 1) регулювання, зокрема, обмеження інформаційних потоків; 2) організація інформаційних потоків (зокрема ініціювання поширення певної інформації); 3) поширення способів та засобів обробки та оцінки інформації; 4) формування групового та індивідуального психологічного захисту.

Методологічну основу дослідження складає комплекс загальнонаукових методів пізнання: аналіз, синтез, абстрагування, узагальнення, індукція, дедукція, інші спеціальні методи. У процесі дослідження проблем правового забезпечення інформаційно-психологічної безпеки застосовувалися

загальнонаукові методи (абстрагування, аналіз, синтез, аналогія, індукція, дедукція, моделювання) та приватні методи наукового пізнання, включаючи: соціологічний та статистичний методи (при дослідженні загроз інформаційно-психологічній безпеці); формально-юридичний метод та порівняльно-правовий метод (при аналіз механізму правового регулювання забезпечення інформаційно-психологічної безпеки); структурно-функціональний метод (під час вивчення системи забезпечення інформаційно-психологічної безпеки).

Робота має практичне значення, яке полягає в тому, що обґрунтовані та розроблені в дисертації наукові результати дослідження, висновки й практичні рекомендації становлять теоретико-методологічну основу для практичного удосконалення публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки України.

Ключові слова: публічно-управлінський механізм, національна безпека, інформаційно-психологічна безпека, інформаційна безпека, кібербезпека, паспорт загроз, політико-правовий механізм, гібридна війна, інформаційна війна, загрози інформаційній безпеці, державно-управлінська практика, інформаційно-психологічні впливи.

ANNOTATION

Kanarskiy V.S. Public management mechanisms for ensuring informational and psychological security of Ukraine in the conditions of hybrid war. - Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the field of knowledge 28 Public management and administration in the specialty 281 «Public management and administration». – Taras Shevchenko National University of Kyiv, Ministry of Education and Science of Ukraine. Taras Shevchenko National University of Kyiv, Ministry of Education and Science of Ukraine. – Kyiv, 2023.

The scientific novelty of the obtained results lies in the fact that the dissertation is a complex study in which the task of substantiating theoretical provisions and methodological approaches to the study of public-management mechanisms for ensuring informational and psychological security, which is relevant for domestic science «Public management and administration», is solved and on the basis of a comprehensive analysis international legal standards in the field of information security and the experience of foreign countries regarding the use of public management mechanisms for ensuring information and psychological security, scientifically based proposals for improving these mechanisms in Ukraine.

For the first time, the doctoral student developed a scientific concept of legal institutionalization of information and psychological security (IPS) in the information law system of Ukraine from the standpoint of public administration, taking into account an interdisciplinary approach. The dissertation substantiates the scientific model of informational and psychological security, which includes definitions of basic concepts, objects of protection, content and types of destructive informational and psychological influence. The need to introduce the concept of «information and psychological security» into the legal system and management practice is proven, which is determined by: a) the need for a terminological designation of the «psychological» component of information security; b) the specifics of the information security system; c) the existence of a clear boundary between

information protection and informational and psychological security based on the criteria and methods of influencing the object; d) the existence of a complex of specific threats; e) a community of legal tools used to protect against various forms of destructive informational and psychological influence.

The doctoral student improved the system of threats to informational and psychological security and proposed its typology, which made it possible to identify the main groups of such threats: a) content related to the spread of negative (harmful) information in mass media and other sources; b) communication, including destructive interpersonal or group communication. It was established that the main content threats are the following types of messages that: a) promote or justify war and other international crimes, terrorism; b) incite hatred and enmity in society; c) stimulate and facilitate the commission of crimes or other socially dangerous actions; d) falsify history or defile historical memory; e) sow fear; e) have a false or distorted character; g) humiliate (insult) the honor, dignity or business reputation of a person or offend public morality; h) have a pornographic and other sexually explicit nature. Among the main communication threats, the following forms of destructive communication are identified: a) public appeals and other forms of incitement to commit illegal and other socially dangerous actions; b) recruitment and other forms of involvement in the commission of illegal and other socially dangerous processes; c) inciting hatred or enmity; d) falsification of history or the image of historical memory; e) deception (misinformation); f) manipulation of consciousness; g) intimidation and coercion; h) insult and other forms of humiliation of human dignity. A matrix of threats to informational and psychological security (IPS) has been developed, which reflects a wide range of threats to IPS in the political, social, cultural and international spheres.

Approaches to: determination of national interests in the information sphere have gained further development and their author's interpretation has been provided; determination of the purpose, tasks and directions of providing IPS and, based on the analysis of normative legal documents of Ukraine in the field of information security, determination of additional tasks for providing IPS. The acquirer has developed a

Passport of threats to information security, defined the tasks and functions of providing IPS.

The concept of: public-administrative mechanism for ensuring informational and psychological security has also been clarified; information and psychological security; political and legal mechanism, legal provision of IPS; the system of legal protection of the IPS.

The dissertation outlines practical proposals for improving public management mechanisms for ensuring informational and psychological security, defines measures to ensure it, which are divided into 4 groups: 1) regulation, in particular, limitation of information flows; 2) organization of information flows (in particular, initiating the dissemination of certain information); 3) distribution of methods and means of information processing and assessment; 4) formation of group and individual psychological protection. The main provisions of the Project of the strategic planning document - «Concept of informational and psychological security of Ukraine» have been developed, which represents a system of views on ensuring informational and psychological security as a part of informational and national security of Ukraine. The project reflects the main threats to the informational and psychological security of Ukraine; goals, tasks, principles and priority areas of activity of authorized state authorities, organizations and other entities involved in ensuring informational and psychological security in accordance with the legislation of Ukraine.

The methodological basis of the research is a complex of general scientific methods of cognition: analysis, synthesis, abstraction, generalization, induction, deduction, and other special methods. In the process of researching the problems of legal provision of information and psychological security, general scientific methods (abstraction, analysis, synthesis, analogy, induction, deduction, modeling) and private methods of scientific knowledge were used, including: sociological and statistical methods (when investigating threats to information and psychological security); formal-legal method and comparative-legal method (when analyzing the mechanism of legal regulation of ensuring informational and psychological security); structural-functional method (when studying the information and psychological security

system).

The work has a practical significance, which consists in the fact that the scientific research results, conclusions and practical recommendations substantiated and developed in the dissertation constitute a theoretical and methodological basis for the practical improvement of public management mechanisms for ensuring informational and psychological security of Ukraine.

Keywords: public administration mechanism, national security, informational and psychological security, information security, cyber security, threat passport, political and legal mechanism, hybrid warfare, information warfare, threats to information security, state management practice, informational and psychological influences.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Канарський В. С. Політико-правовий механізм державного управління інформаційно-психологічною безпекою України: сутність, функції та повноваження. *Наукові перспективи*, Випуск №9(15). 2021. С.99-110.

2. Канарський В. С. Інформаційні загрози як головний фактор розгортання «гібридної війни». *Електронне наукове видання «Публічне адміністрування та національна безпека»*. 2022. №2. URL: https://doi.org/10.25313/2617-572X-2022-2-7926

3. Канарський В. С. Рекомендації щодо удосконалення нормативно-правових механізмів державної політики у сфері інформаційної безпеки України. *Наукові інновації та передові технології (серія «Державне управління»*). №10(12), 2022. DOI: https://doi.org/10.52058/2786-5274-2022-10(12)-63-75

4. Канарський В. С. Аналітичний огляд джерел та наукової літератури з публічного управління інформаційно-психологічною безпекою України. *Актуальні питання у сучасній науці (Серія «Державне управління»).* Випуск № 6(12) 2023. С. 210-224. **DOI:** https://doi.org/10.52058/2786-6300-2023-6(12)-210-224

Тези, опубліковані за матеріалами наукових конференцій

5. Канарський В.С. Пріоритети державної політики інформаційної безпеки України: Збірник тез наукових доповідей XII Всеукр. наук.-практ. конф. «Актуальні проблеми управління інформаційною безпекою» (Київ: Національна академія СБУ, 26 березня 2021 р.), С.275-276.

6. Канарський В.С. Механізми оптимізації державного управління забезпеченням інформаційної безпеки в Україні. 30 років незалежності України: досягнення, виклики, перспективи : матеріали міжнар. наук.практ. конф. (Київ, 10 верес. 2021 р.) / за заг. ред. Л. Г. Комахи, О. М. Андрєєвої, В. А. Гошовської. Київ : ННІ ПУДС КНУ, 2021. С.178-179.

7. Канарський В.С. Пропозиції щодо вдосконалення організаційно-правових механізмів реагування на загрози інформаційно-психологічної безпеки України. Шевченківська весна – 2022: публічне управління та державна служба : матеріали міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених (Київ, 19 квіт. 2022 р.) / за заг. ред. Л. Г. Комахи, О. М. Андрєєвої. Київ : ННІ ПУДС КНУ, 2022 С.103-104.

8. Канарський В. Пріоритетні напрями вдосконалення державної політики інформаційної безпеки в умовах протидії гуманітарної експансії рф проти України. Глобалізаційні виклики: урядування майбутнього : матеріали міжнар. наук.-практ. конф. (Київ, 7–8 черв. 2022 р.) / за заг. ред. Л. Г. Комахи. Київ: ННІ ПУДС КНУ імені Тараса Шевченка, 2022.С.199-201.

9. Канарський В. Публічно-управлінські механізми протидії інформаційним загрозам: європейський досвід. Україна 2030: публічне управління для сталого розвитку : матеріали щоріч. міжнар. наук.-практ. конф. (Київ, 2020 р.) : у 3 т. / за заг. ред. А. П. Савкова, М. М. Білинської, О. М. Петроє. Київ : НАДУ, 2020. С.32-33.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АТО/ООС - Антитерористична операція/Операція об’єднаних сил

ЄС – Європейський Союз;

ЗС – збройні сили;

ЗСУ – Збройні Сили України;

ЗМІ – засоби масової інформації;

ІПБ – інформаційно-психологічна безпека

ІПВ – інформаційно-психологічний вплив

ІПСО – інформаційно-психологічні операції

КМРЄ – Комітет міністрів Ради Європи

КСУ – Конституційний суд України

МВС – Міністерство внутрішніх справ;

МІБ – Міжнародна інформаційна безпека

МЗС – Міністерство закордонних справ;

МКІП – Міністерство культури та інформаційної політики

МОУ – Міністерство оборони України;

НАТО – Організація Північноатлантичного договору;

ОРДЛО – окремі райони Донецької та Луганської областей

РНБ – Рада національної безпеки;

РНБОУ – Рада національної безпеки і оборони України;

рф – російська федерація;

СБУ – Служба безпеки України;

СЗНБ – система забезпечення національної безпеки;

СЗР – Служба зовнішньої розвідки;

США – Сполучені Штати Америки;

СНБ – система національної безпеки;

СЗНБ – система забезпечення національної безпеки.

ЗМІСТ

ВСТУП

Актуальність теми обумовлена недостатнім рівнем дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки України, зростанням рівня загроз в інформаційній сфері в умовах ведення рф гібридної та конвенційної війни проти України.

Сучасність характеризується появою нових викликів та загроз, інформаційно-психологічних впливів на індивідуальну, групову та суспільну свідомість. У ході російсько-української війни з 2014 року суттєво зросла активність в інформаційному просторі російських спецслужб, хакерських організацій деструктивного спрямування. Пандемія COVID-19 різко загострила проблему поширення недостовірної суспільно-значущої інформації у ЗМІ та інтернет-ресурсах, що спровокувало появу нового інформаційного феномену – інфодемії. Технології штучного інтелекту, віртуальної та доповненої реальності здатні вивести інформаційно-психологічні загрози нового рівня небезпеки. Все це вимагає від системи публічного управління формування ефективних управлінських механізмів реагування на сучасні загрози інформаційно-психологічної безпеки людини, суспільства та держави. На тлі всіх цих нових викликів та загроз з'являється потреба у формуванні науково обґрунтованих підходів та осмислення проблеми забезпечення інформаційно-психологічної безпеки.

Актуальність проблематики також зумовлюється тим, що вітчизняна система забезпечення інформаційної безпеки знаходиться на стадії розвитку та організаційно-правової інституціоналізації. Елементи даної системи не завжди пов'язані між собою, їх функції часто дублюються, все це заважає їх ефективній діяльності. Для ефективної протидії інформаційно-психологічним викликам і загрозам потрібні комплексні узгоджені дії всіх ключових суб'єктів даної системи та розробка діючих публічно-управлінські механізмів даної системи.

Крім внутрішньополітичних аспектів даної проблематики актуальним є глобальний вимір досліджуваної проблеми. Так, в умовах глобальних інформаційних викликів та регіональних конфліктів складність публічного управління сферою інформаційної безпеки обумовлена багатогранністю проявів інформації та інформаційних процесів. Гібридна війна, складовою частиною якої є інформаційно-психологічний чинник, формує довгострокові виклики для України. Зокрема, у «Стратегії сталого розвитку «Україна − 2020» заявлено про необхідність реформи системи національної безпеки і оборони, одним з основних пріоритетів якої має стати інформаційна безпека.

В Стратегії національної безпеки, яка введена у дію Указом Президента України від 15 жовтня 2021 року № 685/2021, зазначається що для досягнення інформаційної безпеки необхідно вжити заходи щодо «…стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки» [102].

Виходячи з цих цілей існує необхідність аналізу публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки, використання позитивного досвіду розвинених країн світу щодо державного реагування на загрози інформаційно-психологічної безпеки, розробки обґрунтованих пропозицій щодо вдосконалення даних механізмів в умовах умовах гібридної та конвенційної війни рф проти України, наслідком якої є сучасний збройний конфлікт та анексія Криму російською федерацією.

Ступінь наукової розробки проблеми. У процесі підготовки дисертаційного дослідження були використані фундаментальні праці вітчизняних науковців із різних аспектів державного управління національною

безпекою. Так, вивченню різних аспектів формування інформаційної політики держави та забезпечення її інформаційної безпеки присвячені роботи вітчизняних вчених М.М. Биченка, В.П. Горбуліна, Б.О Демидова, Д.В. Дубова, Я.М. Жаркова, І.В. Замаруєва, О.В. Литвиненка, Р.Р. Марутян, М.А. Ожевана, Г.Г. Почепцова, А.О. Рось, А.І. Семенченка, В.Ю. Степанова, В.Б. Толубка, В.М. Шемаєва та інших.

Проблемі правового забезпечення процесу регулювання відносин у інформаційній сфері, а саме процесів інформатизації, захисту інформації, створення та використання інформаційних ресурсів України присвячені наукові розробки І.В. Арістової, В.М. Брижка, Р.В. Власенка, В.Д. Гавловського, В.В. Грищенка, М.В. Гуцалюка, Р.А. Калюжного, Б.А. Кормича, О.В. Кохановської, П.В. Мельника, О.В. Сосніна, В.С. Цимбалюка, В.О. Шамрая, М.Я. Швеця, Ю.В. Яцишина та ін.

Зарубіжна історіографія проблематики формування та реалізації інформаційної політики держави та забезпечення інформаційної безпеки представлена низкою авторів, серед яких слід акцентувати увагу на роботи Дж.Арквілла, що є одним з авторів сучасної стратегії інформаційної безпеки США та головою Центру інформаційних операцій у системі воєнно-морських сил США. Потребують уваги також наукові праці Д. Альбертса, М. Лібікі, Д. Мальтизи, Р. Маклоріна, Д. Ронфельда, які досліджують проблеми інформаційного протиборства та ведення інформаційних війн.

Праці названих науковців створили методологічне підґрунтя для системного розгляду переважної більшості проблем у сфері публічного управління із забезпечення інформаційної безпеки.

Між тим, зазначені дослідження висвітлювали завдання держави в стабільній зовнішньо- та внутрішньополітичній ситуації. В той же час, сучасна внутрішньополітична ситуація в середині країни, зовнішньополітична ситуація навколо України та збройний конфлікт на території держави вимагають невідкладної та водночас виваженої публічно-управлінської політики,

спрямованої на ефективне використання механізмів забезпечення інформаційно-психологічної безпеки України.

Об'єктивна необхідність розв'язання зазначених проблем, їх практична значущість та недостатня розробленість зумовили вибір теми, мети та завдань дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження проводилося в рамках науково-дослідної роботи кафедри глобалістики, євроінтеграції та управління національною безпекою НАДУ за темою: «Входження України до Європейського та Євроатлантичного просторів як гарантія забезпечення національної безпеки» (ДР № 119U101583). У рамках цієї НДР автором досліджено організаційно-правові засади інформаційно-психологічної безпеки в Україні та країнах-членах ЄС і НАТО, узагальнено і систематизовано підходи до аналізу інформаційних загроз у зарубіжних країнах; обґрунтовано пропозиції щодо паспортизації загроз інформаційній безпеці України.

Мета і завдання дослідження. Метою є розробка концептуальних засад формування та функціонування публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни й розробка на цій основі практичних рекомендацій щодо напрямів їх удосконалення .

Відповідно до мети дослідження поставлено такі **завдання:**

- узагальнити основні наукові підходи щодо дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки та з'ясувати місце інформаційно-психологічної безпеки в системі національної безпеки;
- дослідити сутність, функції та повноваження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки в України;

- проаналізувати зарубіжний досвід державно-управлінської практики щодо забезпечення інформаційної безпеки та можливості його використання в Україні;
- розкрити зміст інформаційно-психологічних загроз як головного фактору розгортання «гібридної війни»;
- охарактеризувати проблеми та перспективи розвитку системи правового забезпечення інформаційно-психологічної безпеки в Україні;
- визначити пріоритетні напрями та запропонувати рекомендації щодо вдосконалення публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни.

Об'єкт дослідження – інформаційно-психологічна безпека.

Предмет дослідження – публічно-управлінські механізми забезпечення інформаційно-психологічної безпеки.

Методи дослідження. Для досягнення поставленої мети використаний комплексний підхід до вивчення публічно-управлінських механізмів забезпечення інформаційної безпеки, основою якого стала система окремих, спеціальних та загальних методів. А саме: метод індукції, структурно-функціональний метод, системний, компаративний метод, метод аналізу та синтезу.

Методологічну основу дослідження складає міждисциплінарний підхід щодо дослідження проблеми, що використовує положення філософії, юриспруденції, психології, соціології, політології, теорії комунікації, журналістики, військової науки та інших галузей наукового пізнання. У процесі дослідження проблем правового забезпечення інформаційно-психологічної безпеки застосовувалися загальнонаукові методи (абстрагування, аналіз, синтез, аналогія, індукція, дедукція, моделювання) та спеціальні методи наукового пізнання, включаючи: соціологічний та статистичний методи (при дослідженні загроз інформаційно-психологічної безпеки); формально-юридичний метод та порівняльно-правовий метод (при аналізі механізму правового забезпечення інформаційно-психологічної безпеки); структурно-функціональний метод (під

час вивчення системи правового забезпечення інформаційно-психологічної безпеки).

Джерельну базу майбутнього дослідження будуть складати загальнодержавні законодавчі та нормативно-правові акти, зокрема: закони України, укази Президента України, постанови та розпорядження Кабінету Міністрів України, наукові праці вітчизняних та зарубіжних вчених.

Наукова новизна одержаних результатів. Наукова новизна одержаних результатів полягає в тому, що дисертаційна робота є комплексним дослідженням, у якому вирішено актуальне для вітчизняної науки «Публічне управління та адміністрування» завдання з обґрунтування теоретичних положень і методологічних підходів дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки та на підставі комплексного аналізу міжнародно-правових стандартів у сфері інформаційної безпеки і досвіду зарубіжних країн щодо використання публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки, науково обґрунтовано пропозиції з удосконалення цих механізмів в Україні. Розроблено основні положення Проекту документа стратегічного планування - «Концепція інформаційно-психологічної безпеки України», що представляє собою систему поглядів на забезпечення інформаційно-психологічної безпеки, як частини інформаційної та національної безпеки України. У зазначеному проекті відображено основні загрози інформаційно-психологічній безпеці України; цілі, завдання, принципи та пріоритетні напрямки діяльності уповноважених органів державної влади, організацій та інших суб'єктів, що беруть участь у забезпеченні інформаційно-психологічної безпеки відповідно до законодавства України.

Найсуттєвіші результати, які містять наукову новину:

вперше:

розроблено наукову концепцію правової інституціоналізації інформаційно-психологічної безпеки в системі інформаційного права України з позицій публічного управління та із врахуванням міждисциплінарного підходу;

обґрунтовано наукову модель інформаційно-психологічної безпеки, що включає дефініції базових понять, об'єкти захисту, зміст та види деструктивного інформаційно-психологічного впливу; доведено необхідність введення в правову систему та управлінську практику поняття «інформаційно-психологічна безпека», що детерміновано: а) потребою у термінологічному позначенні «психологічної» складової інформаційної безпеки; б) специфікою системи інформаційної безпеки; в) наявністю чіткої межі між захистом інформації та інформаційно-психологічною безпекою за критеріями об'єкту та методами впливу; г) існуванням комплексу специфічних загроз; д) спільністю правового інструментарію, що використовується для захисту від різних форм деструктивного інформаційно-психологічного впливу.

удосконалено:

наукові підходи до побудови системи загроз інформаційно-психологічній безпеці та запропоновано її типологізація, що дозволило виділити основні групи таких загроз: а) контентні, пов'язані з поширенням негативних (шкідливих) відомостей у засобах масової інформації та інших джерелах; б) комунікаційні, що включають деструктивне міжособистісне або групове спілкування. Встановлено, що основними ***контентними*** загрозами є такі види повідомлень, які: а) пропагують чи виправдовують війну та інші міжнародні злочини, тероризм; б) розпалюють ненависть і ворожнечу у суспільстві; в) стимулюють та сприяють скоєнню злочинів чи інших суспільно-небезпечних діянь; г) фальсифікують історію або оскверняють історичну пам'ять; д) сіють страх; е) мають помилковий або спотворений характер; ж) принижують (зневажають) честь, гідність та ділову репутацію особи або які ображають суспільну моральність; з) носять порнографічний та інший сексуально відвертий характер. Серед основних ***комунікаційних*** загроз визначено такі форми деструктивного спілкування: а) публічні заклики та інші форми підбурювання до скоєння протиправних чи інших суспільно-небезпечних діянь; б) вербування та інші форми залучення у вчинення протиправних чи інших суспільно-небезпечних процесів; в) розпалювання ненависті чи

ворожнечі; г) фальсифікація історії чи образу історичної пам'яті; д) обман (дезінформація); е) маніпуляція свідомістю; ж) залякування та примус; з) образа та інші форми приниження людської гідності.

матрицю загроз інформаційно-психологічної безпеки (ІПБ), що відображає широкий спектр загроз ІПБ у політичній, соціальній, культурній та міжнародній сферах.

набули подальшого розвитку:

підходи до: визначення національних інтересів в інформаційній сфері та надано їх авторське тлумачення; визначення мети, завдань та напрямів забезпечення ІПБ та на основі аналізу нормативно-правових актів України у сфері інформаційної безпеки визначено додаткові завдання із забезпечення ІПБ. Здобувачем розроблено Паспорт загроз інформаційній безпеці, визначено завдання та функції забезпечення ІПБ;

уточнено поняття: публічно-управлінський механізм забезпечення інформаційно-психологічної безпеки; інформаційно-психологічна безпека; політико-правовий механізм; правове забезпечення ІПБ; система правового забезпечення ІПБ;

викладено практичні пропозиції щодо удосконалення публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки, визначено заходи з її забезпечення, які поділені на 4 групи: 1) регулювання, зокрема, обмеження інформаційних потоків; 2) організація інформаційних потоків (зокрема ініціювання поширення певної інформації); 3) поширення способів та засобів обробки та оцінки інформації; 4) формування групового та індивідуального психологічного захисту;

Теоретичне та практичне значення отриманих результатів полягає в тому, що обґрунтовані та розроблені в дисертації наукові результати дослідження, висновки й практичні пропозиції становлять теоретико-методологічну основу для практичного удосконалення публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки України, а також створюють основу для розроблення нового практичного підходу до

забезпечення інформаційно безпеки України в умовах збройної агресії рф.

Результати дослідження з обґрунтування теоретико-методологічних засад дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки України та розробки науково-обґрунтованих пропозицій щодо вдосконалення цих механізмів в Україні використані у роботі: Київської обласної прокуратури (довідка від 12 вересня 2022 року №09/1/1-498) та Комітету Верховної ради України з питань гуманітарної та інформаційної політики (довідка від 12 вересня 2022 року).

Особистий внесок здобувача. Дисертаційне дослідження є самостійною науковою роботою. Основні ідеї та розробки, що характеризують наукову новизну, мету, завдання, методологічні основи й методичні підходи до їх вирішення та практичне значення одержаних результатів, виконані в межах дисертаційного дослідження, належать особисто авторові.

Апробація матеріалів дисертації. Основні положення дисертаційного дослідження апробовані автором на науково-практичних конференціях, зокрема міжнародних та за міжнародною участю, а саме: «Актуальні проблеми управління інформаційною безпекою» (Київ: Національна академія СБУ, 26 березня 2021 р.); «30 років незалежності України: досягнення, виклики, перспективи» міжнар. наук.практ. конф. (Київ, 10 верес. 2021 р.); «Шевченківська весна – 2022: публічне управління та державна служба»: міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених (Київ, 19 квіт. 2022 р.); «Публічне управління: традиції, інновації, глобальні тренди» (м. Одеса, 2019 р.); «Глобалізаційні виклики: урядування майбутнього»: матеріали міжнар. наук.-практ. конф. (Київ, 7–8 черв. 2022 р.); «Україна 2030: публічне управління для сталого розвитку»: матеріали щоріч. міжнар. наук.-практ. конф. (Київ, 2020 р.)».

Публікації. Загальні положення та зміст дисертації відображено у 9 публікаціях, зокрема 4 статтях у наукових фахових виданнях з державного управління, 5 тезах доповідей у матеріалах науково-практичних конференцій, у тому числі міжнародних та за міжнародною участю.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, трьох розділів, висновків, списку бібліографічних посилань, додатків. Загальний обсяг 189 с., основного тексту - 150 с. Список включає 167 найменувань (іншомовних - 25) на 20 с.

РОЗДІЛ 1
ТЕОРЕТИЧНЕ ДОСЛІДЖЕННЯ ПУБЛІЧНО-УПРАВЛІНСЬКИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ

1.1. Наукові підходи до дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки

У рамках аналізу управлінських механізмів забезпечення інформаційної безпеки теоретики та практики звертають усе більшу увагу на необхідність активної розробки проблематики формування ефективних механізмів забезпечення інформаційно-психологічної безпеки особистості, суспільства та держави, адже без докладного аналізу цієї проблематики неможливий подальший стійкий розвиток суспільства. Напрацювання ряду напрямів дослідження механізмів забезпечення публічного управління інформаційно-психологічною складовою національної безпеки є нагальною потребою сьогодення для України, особливо в умовах протидії агресору - російській федерації, що визначено рядом нормативно-правових актів України. Проблема ефективного управління інформаційно-психологічною безпекою держави сьогодні висувається на перше місце в публічно-управлінській практиці. При аналізі ступеню розробки проблем публічного управління інформаційно-психологічною безпекою України слід констатувати, що більшість вітчизняних науковців досліджують саме державно-управлінські механізми забезпечення інформаційної безпеки. В цілому, джерела та наукову літературу за цим напрямом досліджень можна поділити на сім груп. Перша група представлена нормативно-правовою базою забезпечення національної безпеки України в цілому [97-107]. Другу групу джерел складають закони та нормативно-правові акти України з основних питань забезпечення інформаційної безпеки України [97;100-103; 105-107]. Результати аналізу цієї групи джерел дозволяють констатувати, що система інформаційної безпеки України сформована проте, нормативно-правова база в галузі інформаційної безпеки має низку недоліків, а

саме:

недосконалість понятійно-категоріального апарату, який використовується у сфері забезпечення інформаційної та кібербезпеки;

неузгодженість та дублювання функцій і завдань суб'єктами забезпечення інформаційної та кібербезпеки в період воєнного стану, а також під час їх взаємодії між собою в умовах гібридної війни.

Третю групу складають дисертаційні роботи в галузі знань «Державне управління» та наукові праці, в яких розглянуто проблеми формування та реалізації публічної політики України із забезпечення національної безпеки. Проаналізувавши третю групу наукових досліджень, формуємо висновок про наявність таких нагальних проблем у здійсненні державної політики у сфері національної безпеки України, як [46]:

постійна потреба в оновленні концептуальних і організаційно-правових засад формування та реалізації державної політики національної безпеки з урахуванням трансформацій зовнішнього та внутрішнього безпекового середовища;

подолання етатичних тенденцій у сфері розробки політики національної безпеки України шляхом широкого обговорення проектів таких документів, як Стратегії національної безпеки України, Стратегія інформаційної безпеки України та ін.

Четверту групу складають дисертаційні роботи в галузі знань «Державне управління», в яких розглянута державно-управлінська проблематика забезпечення інформаційної безпеки України, а також визначаються шляхи вдосконалення системи забезпечення інформаційної безпеки. Так у дисертаційному дослідженні В. Гурковського «Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки» обґрунтовано пропозиції щодо удосконалення системи державного управління інформаційною безпекою, а саме розроблено правовий механізм взаємодії, координації діяльності органів державної влади у цій специфічній сфері [25]. В. Гурковським запропоновано включити до понятійно-категоріальної сітки

державного управління інформаційною безпекою таку категорію, як «правова підтримка національної інформаційної безпеки» [25].

В дисертації Л. Євдоченко «Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації» [35] проведено історичний аналіз становлення та розвитку системи державного забезпечення інформаційної безпеки України, а також здійснено оцінку стану нормативно-правового та інституційного забезпечення інформаційної безпеки України на основі чого обґрунтовано напрями удосконалення цієї системи. На увагу заслуговують такі наукові результати дослідження Л. Євдоченко:

1) класифікація інформаційних загроз інформаційній безпеці;

2) можливі державно-управлінські заходи протидії загрозам інформаційній безпеці;

3) модель національної інфраструктури захисту інформації.

В дисертаційному дослідженні З. Коваля «Політико-правові механізми державного управління інформаційно-психологічною безпекою України» [56] в рамках системно-синергетичного підходу і загальної теорії організацій обґрунтовано пропозиції щодо удосконалення державних механізмів забезпечення інформаційно-психологічної безпеки України. В дисертаційному дослідженні автор вивчив зарубіжний та вітчизняний досвід забезпечення інформаційно-психологічної безпеки, ввів у науковий обіг низку понять, а саме: «інформаційна безпека держави», «інформаційно-психологічна безпека особи та суспільства», «інформаційно-психологічний простір України», «інформаційно-психологічний захист», «інформаційно-психологічний вплив». Також заслуговують на увагу такі наукові результати З. Коваль, як класифікація моделей інформаційно-психологічних впливів за такими параметрами, як: традиційність або креативність, відкритість або прихованість. В дисертаційному дослідженні О. Власенко «Механізми державного регулювання захисту громадян від негативних інформаційних впливів» [18] обґрунтовано пропозиції щодо удосконалення механізмів реактивного реагування на загрози інформаційно-психологічного характеру в умовах інформаційного суспільства.

Зокрема, Власенко: 1) ввів у науковий обіг поняття «негативний інформаційний вплив», «механізми подолання негативних інформаційних впливів»; 2) розробив модель механізмів та концепцію реактивного реагування на загрози інформаційно-психологічного характеру. Вітчизняний дослідник О. Зозуля в дисертаційному дослідженні «Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства» [40] узагальнив та систематизував зарубіжний досвід державного управління забезпеченням інформаційної безпеки, виявив актуальні проблеми державного управління забезпеченням інформаційної безпеки України. Вітчизняний дослідник В. Антонюк в дисертаційному дослідженні «Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України» [5] обґрунтував пропозиції щодо удосконалення державних механізмів формування і реалізації державної політики інформаційної безпеки України в умовах гібридної війни. Заслуговують на увагу такі наукові результати В. Антонюка, як: 1) введення у науковий обіг таких понять: «критична інформаційна структура», «об'єкт критичної інформаційної інфраструктури», «спеціальний режим використання інформаційного простору»; 2) структурно-функціональна модель Штабу проведення спеціальних інформаційних операцій Збройних Сил України, що складається із стратегічної, оперативної та тактичної ланок управління; 3) визначено ієрархію керівних документів у сфері забезпечення інформаційної безпеки: Закон – Доктрина – Концепція – Стратегія – державна цільова програма – план; 4) вивчено зарубіжний досвід функціонування механізмів державного реагування на загрози інформаційній безпеці. Аналіз захищених дисертацій, що присвячені дослідженню державно-управлінських проблем у сфері забезпечення інформаційної безпеки України, дає підстави констатувати, що основними проблемами у цій сфері є недосконалість правових та інституційних засад забезпечення інформаційної безпеки в умовах динамічного безпекового середовища. П'яту групу складають праці науковців, котрі розглядають проблеми теорії та практики розбудови системи забезпечення

інформаційної безпеки України. Це роботи Р. Марутян, М. Шевченка, Ю. Сурміна, Г. Ситника, А. Семенченка, Є. Магди, Г. Почепцова та інших [67-71; 91-94;118-119]. У цих працях дослідники вказують на необхідність використання в ході соціального конструювання вказаної системи таких теорій, як: теорії інформаційного суспільства, теорії мережевого суспільства, теорії інформаційного насильства, теорії інформаційної війни, теорії гібридної війни, теорії державного управління, теорії національної безпеки, теорії інформаційної безпеки, теорії кібербезпеки. Аналіз результатів наукових досліджень цієї групи наукових праць дозволяє констатувати нагальну необхідність удосконалення теоретико-методологічних засад розбудови системи інформаційної безпеки з урахуванням сучасних наукових досягнень в галузі безпекознавства, права, політології, державного управління. Шосту групу джерел складають наукові та аналітичні дослідження, основною метою якої є розгляд проблем забезпечення інформаційної безпеки України в умовах гібридної війни. Доцільно передусім назвати роботи таких вітчизняних дослідників, як В. Алещенко, В. Телелима, Д. Музиченко, Ю. Пунди, Ю. Радковця, Д. Дубова та ін.[1-3; 31]. Аналіз результатів вказаних досліджень дозволяє констатувати, що недостатня визначеність та систематизація проблем державної політики забезпечення інформаційної безпеки України в умовах гібридної війни, підходів до їх розв’язання обмежує можливості щодо розробки та застосування формальних методів та моделей при розробці та реалізації вказаної політики.

Сьома, малочисельна група джерел та наукової літератури стосується саме публічно-управлінських механізмів забезпечення інформаційної безпеки. Вона представлена такими дослідниками як Є. Катаєв, В. Алещенко[1-3;55;], які досліджують проблеми інформаційно-психологічної безпеки особистості в сучасному (інформаційному) суспільстві, яке місце ця безпека займає в системі інформаційної безпеки держави в умовах війни та які чинники на неї впливають. О.Дахно[28] досліджує адміністративно-правове регулювання у сфері протидії інформаційно-психологічним операціям на стратегічному рівні, аналізує негативні наслідки та небезпеки інформаційно-психологічних

операцій; обґрунтовує тезу про те, що особливістю стратегічного рівня протидії інформаційно-психологічним операціям є те, що інструменти публічного управління, які застосовуються на цьому рівні, спрямовані на досягнення стратегічної мети, яка полягає у створенні стійкого стану інформаційної безпеки та інформаційного суверенітету держави. Українські дослідники Д. Вєдєнєєв та О. Семенюк [16] в своїх працях розглядають організаційно-управлінську будову сил і засобів ІПсО ЗС України в зоні проведення АТО та ООС на Сході України, їх основні завдання із захисту особового складу ЗС України та населення від негативного інформаційно-психологічного впливу противника, у т.ч. у взаємодії із національними спецслужбами. Попередньо підсумуємо: аналіз стану джерел з досліджуваної проблеми свідчить, що вітчизняні науковці досліджують здебільшого державно-управлінські механізми забезпечення інформаційної безпеки, систему інформаційної безпеки, систему забезпечення інформаційної безпеки та критерії (характеристики), що визначають ступені розвитку цих систем, а також сферу теорії, методології й проблематики забезпечення інформаційної безпеки [46]. Проте комплексних досліджень з проблематики формування та реалізації публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки на сьогодні обмаль, водночас не в повній мірі приділяється увага дослідників щодо визначення місії, функцій та завдань системи інформаційно-психологічної безпеки, прогнозів можливих наслідків накопичення проблем забезпечення інформаційно-психологічної безпеки для сталого розвитку України.

1.2. Понятійно-категорійний апарат дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки

Понятійно-категорійний апарат, який застосовують у сфері публічного управління інформаційною безпекою, перебуває на стадії динамічного розвитку разом з розвитком теорій публічного управління інформаційною безпекою.

Проте недосконалість понятійно-категоріального апарату теорії публічного управління інформаційною безпекою, що представлено як у наукових дослідженнях [2;6;10-11;13;18] так і нормативно-правових актах [58-59;97-107], стримують розроблення та впровадження сучасних методів, моделей і методик державного управління інформаційною безпекою, що значно обмежує можливість підвищення його ефективності.

У статті 17 Конституції України визначено, що забезпечення інформаційної безпеки – одна з найважливіших функцій держави, справа всього Українського народу [58].

Відповідно до Статті 17 Конституції України, забезпечення інформаційної безпеки є однією з найважливіших функцій держави, що стоїть на рівні з захистом суверенітету і територіальної цілісності України, справою всього Українського народу [58].

Сьогодні управління забезпеченням інформаційної безпеки відіграє ключову роль для життєво-важливих інтересів держави і суспільства. Це пов'язано з постійними тенденціями глобалізації, швидким розвитком сучасних медіа та інформаційних технологій, засобів інформатизації та зв'язку, а також технологій психологічного впливу і маніпуляції. Як наслідок, відбувається збільшення впливу інформаційної сфери на всі аспекти державного управління та життєдіяльності суспільства.

Незважаючи на важливість та актуальність державного управління забезпеченням інформаційної безпеки України , саме поняття «інформаційна безпека» немає чіткого усталеного та уніфікованого визначення в законодавстві України. Зокрема, про що свідчить аналіз наступних нормативно-правових актів:

– Закон України «Про національну безпеку України»[58] – не містить вищезазначене визначення;

– Закон України «Про основні засади забезпечення кібербезпеки України»[100] – містить визначення тільки «кібербезбеки» (яка є складовою забезпечення інформаційної безпеки) - захищеність життєво важливих інтересів

людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

– Закон України «Про основи національної безпеки України» (втратив чинність від 08.07.2018, підстава - 2469-VIII) [99] також не містив вищезазначене визначення;

– Указ Президента України Про рішення Ради національної безпеки і оборони України від 29.12.2016 «Про Доктрину інформаційної безпеки України» (чинний станом на 01.10.2019) [102] - не містить вищезазначене визначення;

– Закон України «Про інформацію» (чинний станом на 01.10.2019) [97] - не містить вищезазначене визначення;

– Розпорядження Кабінету міністрів України від 15.05.2013 «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» (чинне станом на 01.10.2019) [106] - не містить вищезазначене визначення;

– Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» (чинний станом на 01.10.2019) [101] – визначає поняття «інформаційна безпека» як - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

На основі дослідження наукової літератури в сфері державного управління забезпеченням інформаційної безпеки держави можна зробити висновок, що поняття «інформаційна безпека» розглядається з різних ракурсів. Результати узагальнено в Таблиці 1.1.

Таблиця 1.1. Порівняння визначення «інформаційна безпека»

Автори визначення	Визначення поняття «інформаційна безпека»
М. Горбатюк	Стан захищеності потреб в інформації особистості, суспільства і держави, за якого забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз
Л.Дж. Хоффман	Стан інформації, за якого забезпечується збереження визначених політикою безпеки властивостей інформації
О. Юдін **В. Богуш**	Стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави
Л. Гевко **О.А. Сороківська**	Суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності
І. Крюков	Суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації),

	суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини пов'язані з організацією технологій створення, поширення, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави
А. Кормич	Захищеність установлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, усього суспільства та держави
О. Литвиненко	Один із аспектів розгляду інформаційних відносин у межах інформаційного законодавства

Джерело: складено автором за [1;8; 10; 21; 28;31;35].

Варто зазначити, що поняття «інформаційна безпека» вперше було визначено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». В цьому Законі поняття «інформаційна безпека» трактувалося виключно в рамках парадигми захисту національних інтересів в інформаційній сфері [101]. В Законі України «Про телекомунікації» (втратив чинність у 2020 році з прийняттям Закону України про електронні комунікації від 16.12.2020 № 1089-IX) визначалося, що ІБ, стосується не інформаційної безпеки України, а лише деякої технічної системи, якою є телекомунікаційна мережа, а саме: «Інформаційна безпека

телекомунікаційних мереж – це здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації».

В Стратегії кібербезпеки України 2021 року зазначається, що «….російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України» [105]. У Доктрині інформаційної безпеки, прийнятої в 2017 році вживаються такі терміни, як-от: стратегічні комунікації, урядові комунікації, кризові комунікації, стратегічний наратив. Серед національних інтересів України в інформаційній сфері Доктрина визначає, зокрема захищеність від руйнівних інформаційно-психологічних впливів, а серед життєво важливі інтересів суспільства і держави - створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди [102].

В Законі України «Про основні засади забезпечення кібербезпеки України» 2017 року [100], вживаються такі терміни, як: кібербезпека, кіберзагроза, кіберзахист, кібероборона, індикатори кіберзагроз, інформація про інцидент кібербезпеки, інцидент кібербезпеки, кібератака, кіберзлочин, кіберзлочинність, кіберпростір, кіберрозвідка, кібертероризм, кібершпигунство, критична інформаційна інфраструктура, критично важливі об'єкти інфраструктури, національна телекомунікаційна мережа, національні електронні інформаційні ресурси, об'єкт критичної інформаційної інфраструктури, система управління технологічними процесами, системи електронних комунікацій.

В сучасній Стратегії інформаційної безпеки, прийнятої в 2021 році, інформаційна безпека України визначається як «складова частина національної

безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [103].

Отже в науковій літературі та законодавстві України поки не вистачає єдиного погляду на зміст поняття «інформаційна безпека». Для одних воно відображає процес, для інших стан, систему гарантій, здатність, властивість, діяльність, функцію тощо. Тому існує необхідність в угрупованні напрямків визначення даного поняття.

Так само слід наголосити, що деякі дослідники зводять інформаційну безпеку тільки до захисту інформації. Проте, інформаційна безпека за своєю суттю є більш широким поняттям і охоплює майже всі сфери життєдіяльності.

Як зазначає У. Ільницька, інформаційна безпека є інтегрованою складовою національної безпеки, і з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій (див. Рис. 1.1. Взаємозв'язок національної безпеки та інформаційного середовища). Отже, комплексне забезпечення інформаційної безпеки дасть змогу як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об'єктивної та якісної інформації [46, с. 222].

Інформаційну безпеку також визначають як неможливість заподіяння шкоди духовній сфері суспільства, культурним цінностям, соціальним регуляторам поведінки людей, інформаційній інфраструктурі й повідомленням, що передаються за її допомогою [117].

Інформаційну безпеку у контексті національної безпеки трактують двома методами. З одного боку, інформаційну безпеку можна розглядати як самостійний елемент національної безпеки будь-якої країни, а з іншого – це інтегрована складова будь якої іншої безпеки: військової, економічної, політичної тощо.

Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

Відповідно до наукових розробок А. Ліпкана, Є. Максименка та М. Желіховського [65, с. 33], можна виокремити декілька підходів окреслення сутності феномену «інформаційної безпеки», а саме розуміння інформаційної безпеки в якості:

- стану захищеності інформаційного простору;
- процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України;
- стану захищеності національних інтересів України в інформаційному середовищі;

Рис 1.1. Взаємозв’язок національної безпеки та інформаційного середовища

- захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі;
- вжиття певних заходів;
- стану захищеності національних інтересів країни в інформаційній сфері;
- суспільних відносин, пов'язаних із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі;
- важливої функції держави;
- невід'ємної частини політичної , економічної, оборонної та інших складових національної безпеки.

Прийнята в національному законодавстві України класифікація напрямків забезпечення інформаційної безпеки побудована відповідно до специфіки її основних об'єктів, якими є людина, суспільство, держава. Але, одночасно, держава, людина та суспільство виступають і в якості суб'єктів інформаційної безпеки [79].

Таким чином, базовою характеристикою забезпечення інформаційної безпеки слід вважати ймовірність появи або реалізації загрози або небезпеки для людини, суспільства і держави; а критерієм ефективності забезпечення інформаційної безпеки – високий рівень безпеки, вчасне виявлення загроз, оперативне реагування на загрози інформаційній безпеці України, аналіз безпекового середовища, прогнозування можливих загроз із врахуванням як внутрішніх та і зовнішніх чинників при мінімумі відповідних витрат.

Основною метою функціонування системи забезпечення інформаційної безпеки можна визначити створення необхідних правових й організаційних механізмів формування, розвитку та забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах діяльності лю дини, суспільства та держави, а також управління загрозами і небезпеками, за якого забезпечується вибір оптимального шляху їх усунення і мінімізації впливу негативних наслідків, та забезпечення реалізації національних інтересів [65 с. 34; 36] .

Національні інтереси в інформаційній сфері є похідними від національних цінностей. Отже, інтереси інформаційної безпеки випливають із таких цінностей, як права людини, свобода, економічне процвітання, могутність країни. Саме тому головним інтересом для України є її виживання як вільної, незалежної держави при збереженні фундаментальних цінностей та інститутів безпеки. Одним з механізмів гарантування даного процесу є ефективно функціонуюча система державного управління, яка є суб'єктом і об 'єктом забезпечення інформаційної безпеки одночасно [25].

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи державного управління, яка при впливі внутрішніх та зовнішніх

загроз та небезпек зберігає суттєво важливі характеристики для власного існування [31].

Інформаційна безпека як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. У той же час, ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку в різних соціальних групах і окремих осіб, почасти не співпадають. Саме у цьому знаходить свій безпосередній вираз вплив держави, яка за допомогою значного арсеналу методів виражає і забезпечує реалізацію спільних цінностей людини, суспільства та держави в інформаційній сфері [40, с. 11; 45].

Таким чином, за останні десять років з'явилась низка системоутворюючих документів зі сфери інформаційної безпеки.

1. Доктрина інформаційної безпеки України, яка була покладена в основу нової Стратегії інформаційної безпеки України. В останній рік українські вчені написали цикл публікацій на різних Інтернет-ресурсах присвячених змінам в доктрину комунікацій, які потрібно обговорювати і реалізовувати вже зараз.

2. Біла книга протидії дезінформації [8], створена за керівництва Інститут інформаційної безпеки. Вона включає системний 360-degrees підхід до розуміння феномену дезінформації та державного регулювання сфери інформаційної безпеки.

3. Нещодавно, в рамках проекту Інститут постінформаційного суспільства було презентовано white paper по розвитку системи практик OSINT в державному і громадському секторі України [41].

В науковому дискурсі поняття «інформаційна безпека» та «інформаційно-психологічна безпека» трактується в рамках парадигм захисту та розвитку об'єкту безпеки. В жодному із згаданих документів стратегічного планування у сфері національної безпеки України немає визначення поняття «інформаційно-психологічна безпека». В цілому, у вітчизняному офіційному та науковому дискурсах виокремлюють три рівня забезпечення інформаційної безпеки: рівень особи; суспільний рівень; державний рівень.

Розглянемо поняття, які визначено в офіційному та науковому дискурсах,

що описують процес державного управління інформаційною безпекою, а саме: поняття «державне управління», «державна політика», «система державного управління інформаційною безпекою», «система інформаційної безпеки».

Під поняттям «державне управління» будемо розуміти діяльність держави, яка спрямована на створення умов для реалізації функцій держави, прав і свобод громадян, партисипаторної взаємодії між державою та інститутами громадянського суспільства, суспільного розвитку [118, с. 150].

Поняття «державна політика» в науковому дискурсі трактується як дії органів державної влади в напрямку реалізації визначених цілей у різних сферах суспільного життя [122, с. 145-146]. Поняття «державна політика забезпечення інформаційної безпеки» в науковому дискурсі трактується як діяльність органів державної влади, яка спрямована на реалізацію національних інтересів в інформаційній сфері, збереження цілісності об'єктивно диференційованого суспільства та досягнення на цій основі прогресивного суспільно-політичного та соціально-економічного розвитку за умови узгодження інтересів різних соціальних груп і держави [117, с. 89-90].

В науці «Державне управління» під функціями держави зазвичай розуміють роль, яку держава виконує у суспільстві у властивих їй формах і притаманними їй методами, а також основні напрями і види її діяльності, які обумовлені її завданнями і цілями і такі, що характеризують її сутність та соціальне призначення в суспільстві.

За соціальним значенням функції держави поділяються на основні та додаткові. Основні функції – це найзагальніші та найважливіші комплексні напрями діяльності держави щодо здійснення стратегічних завдань і цілей, що стоять перед державою у конкретний історичний період (оборона, безпека, регулювання економіки тощо). Додаткові функції держави – це напрями діяльності держави щодо здійснення конкретних завдань у другорядних сферах суспільного життя (управління державним майном, юридичні функції тощо) [143].

Аналіз результатів наукових досліджень щодо розробки термінологічного

апарату у сфері забезпечення інформаційної безпеки [2;6;8;11;13;15] дозволив нам сформулювати авторське визначення поняття «державне управлінням інформаційною безпекою» в широкому та вузькому розумінні. У широкому розумінні під поняттям «державне управління інформаційною безпекою» пропонуємо розуміти організаційно-управлінську діяльність держави, яка спрямована на створення інституційного середовища інформаційної безпеки, формування системи інформаційної безпеки та системи забезпечення інформаційної безпеки, розробку та реалізацію державної політики у сфері інформаційної безпеки. У вузькому розумінні під державним управлінням інформаційною безпекою пропонуємо розуміти практичні заходи, засоби, важелі, стимули за допомогою яких реалізуються державно-управлінські впливи на процес забезпечення інформаційної безпеки.

Зазначимо, що поняття «система державного управління інформаційною безпекою» в науковому дискурсі трактується, як цілісна система, що органічно поєднує у своїй такі структурні компоненти, як-от:

об’єкти та суб’єкти забезпечення інформаційної безпеки;

суспільно-інформаційні відносини між державою та суспільством, між спільнотою професіоналів та суспільством, між державою та спільнотою професіоналів;

державно-управлінські процеси у сфері забезпечення інформаційної безпеки [13, с. 39].

Під поняттям «система інформаційної безпеки» вітчизняний дослідник О. Зозуля пропонує розуміти «цільову, функціональну систему, що відображає процеси взаємодії об'єктів, суб'єктів, ідейно-теоретичної та законодавчої баз, цілей, завдань, державних органів, громадських організацій, посадових осіб та окремих громадян, що несуть в межах своєї компетенції відповідальність за формування заданого рівня інформаційної безпеки України, а також сукупність сил і засобів, що функціонують в інтересах забезпечення інформаційної безпеки» [40, с. 37].

Розглянемо поняття, які визначено в науковому дискурсі, що описують

процес розробки та реалізації державної політики у сфері інформаційної безпеки, а саме: поняття «цикл політики», «механізм розробки державної політики у сфері інформаційної безпеки», «механізм реалізації державної політики у сфері інформаційної безпеки».

Вітчизняний дослідник О. Валевський в рамках телеологічного підходу [13] наводить цикл політики (цикл розробки та впровадження державної політики), який вважається універсальною моделлю та методологічним орієнтиром для вироблення політики.

До суб'єктів розробки державної політики належать органи законодавчої та виконавчої влади, а також суб'єкти політичного процесу та лобістські структури впливу.

Зазвичай виокремлюють довгострокову та поточну державні політики. На підставі аналізу наукових результатів представлених в [1-2;4;10;15] систему формування та реалізації державної політики у сфері інформаційної безпеки пропонуємо умовно представити сукупністю механізмів розробки та впровадження державної політики, за допомогою яких реалізується «цикл політики».

Механізм розробки державної політики у сфері інформаційної безпеки включає в себе пакет концептуально-установчих документів, нормативно-правову базу, систему прийняття рішень, систему програмно-цільового планування у цій сфері.

Під механізмом реалізації державної політики у сфері інформаційної безпеки пропонуємо розуміти сукупність засобів та методів впливу на функціонування та розвиток сфери інформаційної безпеки з метою досягнення цілей державної політики у цій сфері. Основними складовими даного комплексного механізму є такі механізми, як: правовий, інституційний, організаційний, фінансово-економічний, інформаційно-аналітичний, кадровий, науково-методичний та інші. Згадані механізми взаємодіють між собою з метою досягнення визначених цілей державної політики у сфері інформаційної безпеки.

Зауважимо, що реалізація державної політики у сфері інформаційної безпеки передбачає здійснення управлінського впливу в декілька етапів:

формування системи забезпечення інформаційної безпеки;

оцінка оперативної обстановки в інформаційному просторі;

оцінка стану та можливостей системи забезпечення інформаційної безпеки;

розробка та впровадження в державно-управлінську практику технологій реагування на загрози інформаційного характеру;

моніторинг, спостереження та контроль.

Проведений нами аналіз термінів і понять, що представлені у вітчизняному офіційному та науковому дискурсах публічного управління та адміністрування у сфері національної безпеки дозволяє констатувати відсутність поняття «інформаційно-психологічна безпека» у стратегічних документах держави у сфері інформаційної безпеки.

Таким чином, аналіз нормативно-правової бази в сфері національної безпеки України, результатів наукових досліджень із досліджуваної теми свідчить, що реалізація державно-управлінських механізмів забезпечення інформаційної безпеки України залишається актуальною науковою проблемою, що на сьогодні, незважаючи на значну кількість наукових розробок у цій сфері, характеризується недостатнім ступенем вивчення. В контексті пріоритетних цілей державної політики у сфері інформаційної безпеки України, які визначені в Законі України «Про національну безпеку України», Законі України «Про основні засади забезпечення кібербезпеки України», Доктрині інформаційної безпеки України, Стратегії інформаційної безпеки України, Стратегії кібербезпеки України, особливого значення набуває комплексне вивчення і розв’язання державно-управлінських проблем інформаційного розвитку України та реформування системи забезпечення інформаційної безпеки з урахуванням нових викликів і загроз в умовах глобалізації та гібридної війни.

В той же час, питання формування та реалізації публічно-управлінських механізмів забезпечення інформаційної безпеки України знаходиться на стадії

розробки та обговорення в рамках наукового дискурсу. На думку автора *публічно-управлінський механізм забезпечення інформаційно-психологічної безпеки - це ефективно функціонуюча система засобів, заходів та важелів інформаційно-психологічного впливу суб'єкту управління (органів публічної влади та місцевого самоврядування) на об'єкти управління.* Від рівня розвитку інформаційно-психологічного простору вирішальним чином залежать суспільна думка населення, соціальна поведінка людей, формування суспільно-політичних рухів, та внутрішньополітична безпека країни в цілому.

1.3. Місце інформаційно-психологічної безпеки у системі національної безпеки.

У науці склався певний алгоритм аналізу проблем правового забезпечення інформаційної безпеки. Він передбачає визначення понятійного апарату в даній сфері, місця і ролі інформаційної безпеки у системі національної безпеки, встановлення національних інтересів у цій галузі, розкриття змісту принципів, завдань та функцій забезпечення інформаційної безпеки, і навіть характеристик системи правового регулювання суспільних відносин аналізованої сфері. У відповідності до Закону України «Про національну безпеку», національна безпека України - захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [98]. У документах стратегічного планування у сфері національної безпеки та законодавстві України немає чітко визначеної класифікації видів національної безпеки та затвердженого поділу її на сфери життя суспільства. Скоріше спостерігаються різні підходи до визначення видів безпеки. Так у Конституції України йдеться про економічну та інформаційну безпеку. У Стратегії НБ 2020 року згадується про біо- та екологічну безпеку, кібербезпеку та енергетичну безпеку. Воєнна безпека та її характеристики описані в Стратегії воєнної безпеки, інформаційна та кібербезпека у відповідних галузевих Стратегіях. Схожа картина має місце і в науковій

літературі, оскільки дослідники не завжди дбають про дотримання логічних правил класифікації видів національної безпеки. Виокремлення інформаційної безпеки (англ. information security) у системі видів безпеки є загальновизнаним як в Україні, так і за кордоном. Вперше термін «інформаційна безпека» було виведено на державний рівень у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [101] 2007 року, де інформаційна безпека була визначена як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [101]. Визнання субстантивної ролі інформаційної безпеки у системі національної безпеки в Україні відбулося у 2009 році з прийняттям першої Доктрини інформаційної безпеки України (далі – Доктрина ІБ), яка визначила її як «….невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки». У Доктрині ІБ вперше було визначено, що «діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена за трьома головними напрямами, один з яких було визначено як інформаційно-психологічний, а саме «… забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей» [102].

В 2017 році було затверджено нову Доктрину інформаційної безпеки України», яка закріпила пріоритети державної політики України у інформаційній сфері, закріпила розуміння актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері, але Доктрина не містить дефініцію інформаційної безпеки. Більш сучасне визначення поняття

«інформаційна безпека» закріплено у Стратегії інформаційної безпеки України 2021 року: «інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [103].

Таким чином, згадані у законодавстві України обидві дефініції мають досить широкий зміст і наповнюються конкретним змістом через визначення національних інтересів України у інформаційній сфері. Але просте вивчення їх переліку прямо не виявляє потрібний психологічний компонент інформаційної безпеки.

Крім того, аналіз різних статей даних документів стратегічного планування, що визначають загрози та стан інформаційної безпеки та основні напрями її забезпечення, виявляє набагато чіткішу фіксацію блоку питань ІПБ. Так, у Стратегії воєнної безпеки України 2021 року серед цілей, пріоритетів та завдань реалізації державної політики у воєнній сфері, сфері оборони і сфері військового будівництва виділено «військово-патріотичне виховання молоді, що може бути в короткі строки посилене підготовленим і вмотивованим військовим резервом» [104]. Стратегія визначає, що серед «ймовірних сценаріїв, які потребуватимуть застосування сил безпеки і оборони України для виконання завдань з оборони України є: ескалація російською федерацією збройної агресії проти України, повномасштабне застосування воєнної сили проти України шляхом проведення військових операцій з рішучими діями, що може супроводжуватись інформаційними кампаніями, інформаційно-

психологічними операціями, кібероперaціями та спеціальними операціями проти України» [104].

В українській науці серед дослідників інформаційної безпеки довгий час домінував вузький підхід до розуміння інформаційної безпеки як захисту інформації та інформаційних систем. Таке урізане бачення лягло в основу базового законодавчого акту для інформаційної сфери початку 2000-х років. - «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [101]. Багато в чому підхід зберігся і в Законі України «Про телекомунікації» 2003 року, що втратив чинність в 2022 році. В ньому йдеться про інформаційну безпеку телекомунікаційних мереж, яка визначається як «здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації». [108]

Однак, починаючи з 2000-х років частина дослідників починає застосовувати альтернативний підхід. Серед них слід виділити роботи українських авторів В. Петрика, В. Остроухова, О. Юдіна та М. Богуша [84] які є одними із основоположників теорії правового забезпечення інформаційної безпеки. Вони надали широкий підхід до трактування інформаційної безпеки, що передбачає включення до її змісту психологічних аспектів, виокремлення інформаційно-психологічної безпеки людини, суспільства та держави, як окремих наукових дефініцій.

Таким чином, в даний час можна впевнено зробити висновок про те, що ІПБ входить до змісту інформаційної безпеки (див. рис. 1). З цього випливає висновок, що ІПБ має загальні ознаки, властиві даному виду безпеки, найважливішими з яких є інформаційний характер загроз безпеці та інформаційна сфера як сфера прояву даних загроз.

Рис. 1.1. Місце інформаційно-психологічної безпеки у структурі національної безпеки

Таким чином, у законодавстві України сформувалися такі правові інститути у структурі підгалузі правового забезпечення інформаційної безпеки:

1) захист інформації, включаючи захист окремих видів інформації обмеженого доступу;

2) захист конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації;

3) захист від інформаційних кампаній, інформаційно-психологічних операцій, кібероперацій, що проводить країна-агресор - рф;

4) протидія розповсюдженню протиправної інформації у ЗМІ та мережі Інтернет.

Але, сам термін «інформаційно-психологічна безпека» поки не отримав загальновизнаний статус ні в інформаційному праві, ні в інших науках, хоча він зустрічається в дисертаційних дослідженнях та інших наукових працях українських учених.

Автор бачить необхідність у введенні поняття *«інформаційно-психологічна безпека»* в юридичні науки та правову практику через наступні причини:

а) потреба у рельєфному позначенні «психологічної» складової інформаційної безпеки;

б) наявність її яскраво вираженої специфіки у системі інформаційної безпеки;

в) наявність чіткої межі між захистом інформації та інформаційно-психологічною безпекою за критеріями об'єкта та методів впливу;

г) існування комплексу специфічних загроз;

д) перевага перед іншими конкуруючими термінами (духовна, культурна, інформаційно-комунікаційна безпека), що дозволяють інтегрувати психологічні компоненти інформаційної безпеки у цілісний об'єкт правового регулювання;

е) спільність правового інструментарію, що використовується для захисту від різних форм деструктивного інформаційно-психологічного впливу. Принципова відмінність ІПБ від традиційного блоку інформаційної безпеки полягає в тому, що її змістом є не захист інформації, а захист від інформації. Захист людини та суспільства в цілому. З урахуванням цього ІПБ можна визначити, як захист особистості та суспільства від негативного інформаційно-психологічного впливу. Такий підхід підтримується низкою дослідників. Такої позиції дотримувалися інші провідні дослідники, включаючи В.Остроумова, В.Петрика та М.Присяжнюка [84].

Як базовий методологічний підхід вивчення ІПБ вважаємо необхідно використовувати міждисциплінарний підхід. У філософії міждисциплінарні дослідження трактуються як «спосіб організації дослідницької діяльності, що передбачає взаємодію у вивченні того самого об'єкта представників різних дисциплін» [9, с.24-35]. Ми розглядаємо міждисциплінарний підхід як методологічний принцип проведення індивідуального наукового дослідження, що передбачає запозичення та застосування знань та методів з інших сфер наукового знання.

Вчені з НАН України називають розвиток міждисциплінарних правових знань одним із ключових напрямів трансформації права, наголошуючи на потребі знаходження юридичною наукою взаємозв'язку з іншими науковими

дисциплінами технічного та гуманітарного профілю. Акцент на міждисциплінарність пов'язаний з тим, що розглядається предметна область ІПБ спочатку має гібридний характер і знаходиться на стику низки сфер: інформаційних технологій, психології та безпеки. Тому для вивчення проблеми правового забезпечення ІПБ, крім базової юридичної науки, найбільший інтерес представляють три галузі наукового знання: психологія, соціологія масової комунікації та науки про інформаційні технології. Психологія вивчає зміст та механізм роботи індивідуальної та колективної психіки – основних об'єктів ІПБ, а також механізм інформаційно-психологічного впливу. Саме психологічні знання дозволяють виявити потенційну небезпеку певної інформації/комунікації для людей та соціальних груп різних категорій, наприклад, для дітей різних вікових груп. Соціологія масової комунікації досліджує особливості сучасної інформаційного середовища суспільства, її вплив на соціум, а також вивчає основні інститути та типи масової комунікації. Знання з даної наукової області допомагають правильно підібрати інструментарій для нейтралізації загроз ІПБ та їх джерел та ранжувати за значимістю об'єкти для його застосування. Інформатика та інші науки про інформаційні технології вивчають канали та способи технічної передачі інформації, за допомогою якої виявляється деструктивний інформаційно-психологічний вплив. Ця область науки дозволяє розуміти особливості технічних каналів. На значенні використання «міждисциплінарної рефлексії» щодо інформаційно-психологічної безпеки наголошують у своїх працях такі авторитетні українські психологи, як С. Максименко [66]. Застосування міждисциплінарного підходу дозволяє нам скласти уявлення про об'єкти ІПБ. Об'єкти безпеки є однією з ключових характеристик будь-якого виду безпеки, які багато в чому визначають стратегію та інструменти її забезпечення. В теорії безпеки під ними розуміють «реально існуючі явища, процеси і відносини, попередження або усунення загроз яким, становить мета і основний зміст політики безпеки» [118, с.224]. Що стосується сфери ІПБ йдеться про об'єкти деструктивного інформаційно-психологічного впливу. Серед дослідників

відсутня єдина думка щодо об'єктів ІПБ. Так В.Кормич відносить до них «окремих осіб та групи осіб» [60], В.Богуш - «індивідуальну психіку та суспільну свідомість» [142], В.Остроухов – «індивідуальну, групову та суспільну свідомість»[79], Г.Почепцов – «індивідуальну, групову та суспільну психологію та відповідно соціальні суб'єкти різних рівнів спільності, масштабу, системно-структурної та функціональної організації представники психо-екологічного спрямування [92] О. Кокун, В. Клименко, О. Корніяк – «внутрішній світ людини» [111]. У поданих варіантах спостерігається двоїстість об'єктів ІПБ: до них відносять як саму людину, групи людей і суспільство в цілому, так і їх психологічні складові – індивідуальну психіку та суспільну свідомість. На нашу думку, тут немає протиріччя, а зазначений дуалізм обумовлений різним рівнем деталізації за характеристикою об'єктів ІПБ. Більше того, слід також виділити і третій рівень деталізації, на якому як об'єкти ІПБ розглядатимуться, як окремі індивідуальні та групові психічні процеси та явища.

У плані правового регулювання вибір необхідного рівня деталізації залежатиме від характеру та предмета правового акту: для базового закону або документа стратегічного планування у сфері інформаційно-психологічної безпеки, якщо такий буде прийнято в Україні, доцільніше використовувати перший та другий рівні, тоді як для більш вузького предмета правового регулювання може підійти третій рівень деталізації. Так, у Доктрині ІБ 2017 року йдеться про «захист українського суспільства від агресивного інформаційного впливу російської федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України» [102].

Представимо власне бачення об'єктів ІПБ на трьох рівнях деталізації, використавши наукові знання із загальної та соціальної психології та соціології.

На першому рівні об'єктами ІПБ виступають особистість, великі та малі соціальні групи. Вочевидь, що первинним об'єктом ІПБ є особистість, на яку

здійснюється інформаційно-психологічний вплив. Саме людина як особистість і активний соціальний суб'єкт, його психіка схильні до безпосередньої дії інформаційних факторів, які, трансформуючись через його поведінку, дії (або бездіяльність), надають дисфункціональний вплив на соціальні суб'єкти різного рівня спільності, різної системно-структурної та функціональної організації. Об'єктом деструктивного інформаційно-психологічного впливу може бути конкретний індивід при цілеспрямованому впливу чи певна абстрактна людина під час впливу невибіркового типу.

Наступним об'єктом ІПБ є соціальні групи. Український словник-енциклопедія за редакцією Мирослава Поповича дає визначення соціальної групи як «група людей, між якими виникають будь-які суспільні стосунки; люди, об'єднані суспільним зв'язком, які демонструють його усвідомлення» [123].

Соціальні групи в науці розглядаються як психологічні спільності людей, які мають спільну ідентичність і групову психіку. У суспільних науках існує ціла низка класифікацій соціальних груп, відповідно до яких вони поділяються на великі та малі, первинні та вторинні, формальні та неформальні, стійкі (міцні) та нестійкі («швидкі»), однофункціональні та багатофункціональні, відкриті та закриті і т.д. Нами за основу буде взята класифікація соціальних груп на великі та малі, тому що зазначені види груп значно відрізняються один від одного в плані характеристик їх психічних структур.

Під великою соціальною групою розуміється реальна, значна за розміром та складно організована спільність людей, залучених до тієї чи іншої громадської діяльності. Саме вони, за справедливим зауваженням Г.Почепцова [94] визначають перебіг історії. Вищим рівнем великих соціальних груп (далі – ВСГ) є суспільство в цілому, що існує в рамках державних кордонів. На наступному рівні виділяються різні види ВСГ у рамках соціальної стратифікації: соціальні класи, соціальні верстви, етнічні групи, гендерні та вікові групи і т.д. Під малою соціальною групою (далі – МСГ) розуміється нечисленна за складом група, члени якої об'єднані спільною соціальною

діяльністю та знаходяться безпосередньо в особистому спілкуванні, що є основою для виникнення емоційних відносин, групових норм та групових процесів [94]. Приклади МСГ дуже численні: до них можна віднести сім'ю, навчальний клас, трудовий колектив, спортивну команду і т.п.

Великі та малі соціальні групи переважно виступають об'єктами впливу невибіркового чи обмежено вибіркового інформаційно-психологічного впливу з боку засобів масової комунікації чи під час масових офлайнових заходів.

Новим видом соціальних груп, що виникли завдяки розвитку соціальних інтернет-сервісів стали віртуальні групи (спільноти). Формування та стійке існування віртуального співтовариства як соціальної групи можливе лише за наявності в учасників мережного ресурсу спільних інтересів, спільно вироблених цілей та організованих дій щодо їх досягнення, які реалізуються в рамках єдиного комунікативного простору. Пріоритетним об'єктом правового захисту від деструктивного інформаційно-психологічного впливу на рівні соціальних груп виступають діти (неповнолітні) внаслідок їх особливої вразливості, обумовленої їх психологічними особливостями, включаючи некритичність сприйняття інформації, нестійкість та еластичність ціннісних орієнтацій та поведінкових установок, високим ступенем несвідомого зараження емоційними станами, схильністю до наслідування поведінки показаних героїв, реалізмом уяви. На другому рівні деталізації ми переходимо до розгляду конкретних «психологічних складових» об'єктів ІПБ, зазначених вище. Щодо особистості таким об'єктом виступає людська психіка. У вітчизняній науці вона визначається як «системна властивість високоорганізованої матерії, що полягає в активному відображенні суб'єктом об'єктивного світу, у побудові суб'єктом невідчужуваної від нього картини цього світу та саморегуляції на цій основі своєї поведінки та діяльності» [128]. Остання теза, що показує значення карти навколишнього світу як основи регуляції поведінки людини, представляється нам винятково важливою. Впливаючи на картину світу людини, ми тим можемо впливати на її поведінку. Вибір позначення об'єкта ІПБ терміном «психіка» замість «індивідуальної

свідомості», пропонованої іншими авторами (К.Д. Ридченко, Т.Б. Мельницької та ін.), пов'язаний з тим, що поняття психіки є ширшим і крім свідомості включає також несвідоме (підсвідомість), яка також може виступати об'єктом деструктивного інформаційно-психологічного впливу. Такого погляду дотримувалися багато провідних дослідників ІПБ у 1990-х роках (В.М. Лопатін, В.Є. Лепський, А.А. Стрільців та ін.).

Переходячи до характеристики психологічних компонентів соціальних груп як об'єктів ІПБ, ми стикаємося з певними труднощами, викликаними відсутністю усталеного термінологічного апарату. Очевидно, що по суті, йдеться про групову психіку. Колективні психічні структури не зводяться до «суми психік» членів соціальних груп, але становлять самостійну соціальну реальність, а в нашому дослідженні розглядаються як відокремлені об'єкти ІПБ. За словами В.А. Василенко, «по відношенню до кожної окремої «свідомості» групова психологія виступає як якась соціальна реальність, яка виходить за межі свідомості окремого індивіда і впливає на неї разом із іншими об'єктивними умовами життя» [15].

Незважаючи на те, що переважна більшість психічних характеристик соціальних груп розглядаються як елементи «групової свідомості» [149], наукова література виділяє окремі групові психічні неусвідомлювані елементи [145], що свідчить про збереження дихотомії «свідоме - несвідоме» на груповому рівні.

Таким чином, на другому рівні як об'єкти ІПБ визначено: психіка людини, що включає свідомість і несвідоме, та групові психічні структури, що складаються з групової (суспільної) свідомості та колективного несвідомого.

На третьому рівні деталізації ми повинні виділити дрібніші психічні компоненти індивідуальної та групової психіки, які можуть виступати об'єктом інформаційного впливу.

Щодо елементів індивідуальної психіки, то тут у сучасній психології сформовані усталене уявлення та досить чіткий понятійний апарат. Для системного викладу його у нашому дослідженні ми використовуємо два

підходи – динамічний та статичний, що доповнюють один одного.

Динамічний підхід передбачає виділення у структурі психіки складових її психічних процесів [23], які зазвичай поділяються на три основні види: когнітивні, емоційні та регулятивно-вольові. Статичний підхід виходить із виділення психічних утворень, які є результатами психічних процесів, що протікають. За словами С.Л. Рубінштейна, «будь-яке психічне утворення (чуттєвий образ речі, почуття і т.д.) – це, по суті, психічний процес у його результативному вираженні» [110]. Незважаючи на складність та трудомісткість завдання побудови вичерпного переліку психічних процесів та утворень, її вирішення має важливе значення для правильної ідентифікації об'єктів правової захисту.

Підсумовуючи проведений аналіз, слід виділити три основні групи об'єктів ІПБ (деструктивного інформаційно-психологічного впливу):

1) особистість, великі та малі соціальні групи, суспільство в цілому;

2) психіка людини, що включає свідомість і несвідоме, та групові психічні структури, як групова (суспільна) свідомість та колективне несвідоме;

3) індивідуальні та групові психічні процеси свідомого та несвідомого характеру.

Як основу для визначення ІПБ вважаємо за доцільне використовувати перший рівень об'єктів деструктивного інформаційно-психологічного впливу.

Насамкінець, перед тим як сформулювати визначення поняття ІПБ, звернемося до питання про зміст базової категорії, що лежить в його основі «безпека». У більшості документів стратегічного планування та законів України у сфері безпеки поняття «безпека» визначається як стан захищеності певних об'єктів чи інтересів від загроз. Такий підхід поділяється більшістю українських дослідників проблем національної та інформаційної безпеки.

Американський військовий словник закріплює таке визначення безпеки, як стану недоторканності (state of inviolability) від шкідливого впливу, що забезпечується за рахунок реалізації комплексу захисних заходів [161].

Проведений нами аналіз критичних підходів до трактування безпеки,

представлених у науковій літературі, дозволив дійти висновку про оптимальність використання конструкції «стан захищеності» як основи визначення базової категорії «безпеки» та окремих її видів. При цьому саме поняття «стан захищеності» трактується як «сукупність внутрішніх та зовнішніх умов, що запобігають або мінімізують негативний вплив загроз на об'єкти безпеки та забезпечують тим самим можливість існування та збереження даного об’єкту.

На основі вищевикладеного ми визначаємо *інформаційно-психологічну безпеку як складову частину інформаційної системи безпеки, що є станом захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу.*

Висновки до першого розділу

1. Теоретичний аналіз проблеми дає підстави стверджувати, що у вітчизняній та зарубіжній науці накопичено суттєвий науковий багаж знань з окремих аспектів забезпечення інформаційно-психологічної безпеки. Проте цілісна концепція інформаційно-психологічної безпеки як об'єкта публічно-управлінського регулювання та системне бачення механізмів її забезпечення від гібридної та конвенційної війни, яку веде України проти рф досі відсутні.

2. Аналіз понятійно-категорійного апарату дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки, що міститься у нормативно-правових документах та результатах наукових досліджень із досліджуваної теми свідчить, що реалізація державно-управлінських механізмів забезпечення інформаційної безпеки України залишається актуальною науковою проблемою, що на сьогодні, незважаючи на значну кількість наукових розробок у цій сфері, характеризується недостатнім ступенем вивчення. В контексті пріоритетних цілей державної політики у сфері інформаційної безпеки України, які визначені в основних документах стратегічного планування у сфері національної безпеки України особливого значення набуває комплексне вивчення і розв’язання державно-управлінських

проблем інформаційного розвитку України та реформування системи забезпечення інформаційної безпеки з урахуванням нових викликів і загроз в умовах гібридної та конвенційної війни. В той же час питання формування та реалізації публічно-управлінських механізмів забезпечення інформаційної безпеки України знаходиться на стадії розробки та обговорення в рамках наукового дискурсу. Висновком автора є теза про те, що *публічно-управлінський механізм забезпечення інформаційно-психологічної безпеки - це ефективно функціонуюча система засобів, заходів та важелів інформаційно-психологічного впливу суб'єктів управління (органів публічної влади та місцевого самоврядування) на об'єкти управління. Від рівня розвитку інформаційно-психологічного простору вирішальним чином залежать суспільна думка населення, соціальна поведінка людей, формування суспільно-політичних рухів, та внутрішньополітична безпека країни в цілому.*

3. Проведений нами аналіз критичних підходів до трактування безпеки, представлених у науковій літературі, дозволив дійти висновку про оптимальність використання конструкції «стан захищеності» як основи визначення базової категорії «безпеки» та окремих її видів. При цьому саме поняття «стан захищеності» трактується як «сукупність внутрішніх та зовнішніх умов, що запобігають або мінімізують негативний вплив загроз на об'єкти безпеки та забезпечують тим самим можливість існування та збереження даного об'єкту. На основі вищевикладеного ми визначаємо *інформаційно-психологічну безпеку* як складову частину інформаційної системи безпеки, що є станом захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу.

4. Основні наукові результати розділу опубліковані в праці [46].

РОЗДІЛ 2.
ПУБЛІЧНО-УПРАВЛІНСЬКІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ УКРАЇНИ: СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ ФОРМУВАННЯ

2.1. Політико-правовий механізм публічного управління інформаційно-психологічною безпекою України: сутність, функції, проблеми та перспективи розвитку

Напрацювання ряду напрямів дослідження механізмів забезпечення державного управління інформаційно-психологічною складовою національної безпеки є нагальною потребою сьогодення для України, особливо в умовах протидії агресору - російській федерації, що визначено рядом нормативно-правових актів України.

Потрібно зазначити, що в державному управлінні на перше місце сьогодні висувається проблема ефективного управління інформаційно-психологічною безпекою держави. У свою чергу вчені стверджують, що передбачити всі можливі загрози в галузі інформаційної безпеки неможливо, оскільки вони здатні міняти свої зміст та динаміку, а правове регулювання вимагає стабільності. Саме тому наголошуємо на необхідності спрямовувати політику інформаційної безпеки не на пошук відповіді на певну загрозу, а на створення безпечних умов функціонування інформаційно-психологічної сфери, за яких ця сфера буде несприйнятливою до можливих негативних впливів, як всередині держави, так і ззовні.

У рамках аналізу інформаційної безпеки дослідники й практики звертають усе більшу увагу й на необхідність активної розробки проблематики інформаційно-психологічної безпеки особистості, суспільства та держави, адже без докладного аналізу цих проблем неможливий подальший стійкий розвиток суспільства.

Політико-правовий механізм державного управління інформаційно-психологічною безпекою - це ефективно функціонуюча система засобів, заходів

та важелів органів державної влади, яка виступає одночасно і суб'єктом і об'єктом забезпечення інформаційно-психологічної безпеки. А *правове забезпечення інформаційно-психологічної безпеки* – це діяльність з розробки та реалізації системи правових засобів, спрямованих на забезпечення захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу.

Від рівня розвитку інформаційно-психологічного простору вирішальним чином залежать поведінка людей, формування суспільно-політичних рухів, соціальна безпека.

До завдань забезпечення ІПБ на нашу думку слід зарахувати [49]:

1) прогнозування, виявлення, аналіз та оцінку загроз ІПБ;

2) аналіз та оцінку вразливості особистості, соціальних груп та суспільства від деструктивного ІПВ;

3) стратегічне планування у сфері забезпечення ІПБ;

4) правове регулювання у сфері забезпечення ІПБ;

5) застосування комплексу оперативних та довготривалих заходів щодо профілактики, попередження, припинення та усунення загроз ІПБ, мінімізації та (або) ліквідації наслідків їх впливу;

6) застосування комплексу оперативних та довготривалих заходів щодо підвищення здібності особистості, соціальних груп та суспільства протистояти деструктивному ІПВ;

7) організацію діяльності системи забезпечення ІПБ;

8) кадрове, інформаційне, матеріально-технічне та фінансове забезпечення діяльності суб'єктів забезпечення ІПБ;

9) міжнародне співробітництво у сфері забезпечення ІПБ.

Серед широкого спектру наукових досліджень останніх років можна згадати роботи, що розглядають питання державного управління національною та інформаційною безпекою. Це роботи таких авторів, як Г.П. Ситник, Р.Р. Марутян, В.Ю. Богданович [10;67-71;118-119]; присвячені проблемам та технологіям забезпечення інформаційної безпеки в процесі політичних та

соціальних комунікацій - Б.А. Кормич [60-61]; аналізу базових аспектів інформаційної безпеки під час процесу політичної комунікації - Д. Дубов [31]; вивченню методів та засобів формування друкованими ЗМІ громадської думки в Україні відносно політичних сил держави - М. Ожеван, Г.Г. Почепцов [53;91-94] та інші.

З огляду на історичний досвід людства зазначимо, що нації, які не створили надійної та ефективно керованої системи безпеки, ризикують втратити свою самоідентичність, розчинитись в потоці історії. У результаті гіпертрофованого прагнення стати відкритим суспільством, Україна стала більш вразлива через неможливість запроваджувати дієві заходи контролю над інформаційними потоками. Сприяє такому стану речей і відсутність раціональної управлінської стратегії інформаційної безпеки і методів її реалізації. До однієї з головних причин цього слід віднести низький рівень знань керівників виконавчих органів влади всіх рівнів в питаннях інформаційних війн і інформаційних технологій і, вже як наслідок - низьку обізнаність населення в питаннях забезпечення інформаційної безпеки [49].

Розв’язання проблеми забезпечення національної безпеки є невід’ємною і дуже складною функцією кожної незалежної держави і основною сферою діяльності її політичних і державних інститутів [11, с. 65]. Найбільш фаховою, на нашу думку, є визначення поняття «безпека» як стан захищеності від можливого нанесення шкоди, здатність до стримування або протидії небезпечним впливам, а також до швидкої компенсації завданих збитків. Безпека означає збереження системою стабільності, стійкості та можливості саморозвитку.

Проблема безпеки розглядається в різних галузях наукового знання, та набуває ознак в залежності від профілю фахівців. Наприклад, в юридичній науці безпека розглядається як система встановлених законами правових гарантій захищеності особи і суспільства. З психологічної точки зору поняття «безпека» розкривається як відчуття, сприйняття і переживання потреби в захисті життєво важливих потреб і інтересів людей. У філософії безпека

характеризується як стан, тенденції розвитку і умови життєдіяльності соціуму, його структур, інститутів і установ, при яких забезпечується збереження їх якісної визначеності, оптимальне співвідношення свободи і необхідності. У політологічному трактуванні безпека – це властивість певної системи і результат діяльності ряду систем і державних органів, а також сам процес діяльності, направлений на досягнення поставлених завдань по забезпеченню захищеності особи, суспільства і держави.

В. Богданович досліджуючи національну безпеку трактує її як «показник стану нації, що означає, що сукупний вплив внутрішніх і зовнішніх шкідливих чинників не може значно знизити якість її життя і створити загрозу її існуванню» [10].

І.Л. Прохоренко визначає національну безпеку як поєднання внутрішніх і зовнішніх обставин, які впливають на життя держави, при якому відсутні загрози критичного характеру і в той же час зберігається повноцінна здатність держави адекватно реагувати на ці загрози, якщо вони виникнуть» [109, с.90-91].

Ряд дослідників під безпекою розуміють систему гарантій, що забезпечує явищу його нормальний розвиток. Практично всі приведені вище результати досліджень визначення безпеки піддавалися і продовжують піддаватися критиці і з боку фахівців-практиків і з боку учених. Неспроможність багатьох визначень очевидна. Аналіз історіографії проблеми свідчить, що більшість досліджень механізму державного управління інформаційно-психологічною безпекою присвячені саме інформаційній складовій національної безпеки. Проблеми формування та реалізації механізму інформаційно-психологічної безпеки не є достатньо дослідженими.

Можемо констатувати – безпека не може існувати без своєї діалектичної протилежності – небезпеки. Більш того, певний комплекс небезпек присутній завжди. Поняття ж «небезпека» в найзагальнішому плані необхідно досліджувати через характеристику стану об'єкту, при якому загроза його буттю за рахунок розриву або спотворення найбільш істотних зв'язків і

стосунків в системі перевищує якусь гранично допустиму суб'єктивно встановлену величину.

Основним змістом діяльності інформаційної безпеки більшість спеціалістів бачить у неможливості заподіяння шкоди об’єкту захисту, його властивостям або діяльності з виконання своїх функцій. Отже, під загальним поняттям «інформаційна безпека» в нормативно-правових актах доцільно розмежувати це поняття на «інформаційно-технічну безпеку» та «інформаційно-психологічну безпеку».

Згідно Закону України «Про національну безпеку України», національна безпека - захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [98].

Українські науковці В.Б.Толубко, С.Я.Жук, В.О.Косевцов [131] відмічають, що відповідно до загальної методології національної безпеки, інформаційна безпека повинна використовувати такі категорії, як «інформаційна сфера», «національні інтереси в інформаційній сфері», «об’єкт і суб’єкт інформаційної безпеки», «загрози інформаційній безпеці», «система забезпечення інформаційної безпеки», «політика забезпечення інформаційної безпеки» та ін. На даний час ця термінологія ще знаходиться у стані розвитку.

Під інформаційно-психологічною безпекою розуміють стан захищеності громадян, окремих груп та соціальних верств, масових об’єднань людей і населення в цілому від негативних інформаційно-психологічних об’єктів впливів. Це також і стан захищеності індивідуальної, групової та суспільної свідомості і соціальних суб’єктів різних рівнів від впливу інформаційних факторів, які викликають дисфункціональні соціальні процеси.

Даний стан дає змогу людині сформувати і відповідно належно використовувати систему адекватного сприйняття реальності й відношення до оточуючого світу та самої себе, що стає основою для подальшої соціальної поведінки людини; цей стан забезпечує цілісність людини як активного соціального суб’єкта й надає можливості для розвитку в умовах інформаційної

взаємодії з оточуючим світом.

Інформаційно-психологічну безпеку особи та суспільства вважають окремою складовою національної безпеки держави та трактують як стан захищеності гарантованих законодавством умов життєдіяльності держави, суспільства та окремої особи від зовнішніх та внутрішніх загроз. Підтримання національної безпеки є важливим напрямом державної діяльності, що актуалізується залежно від наявності та ступеня відповідних загроз [109, с. 13].

На даний момент Українському законодавстві відсутні чітко закріплені функції та повноваження суб'єктів забезпечення інформаційно-психологічної безпеки. Вважаємо за доцільне удосконалити організаційну складову даної сфери шляхом створення окремого органу при РНБО України, який би напрацював певну стратегію інформаційної політики у сферах інформаційно-технічної та інформаційно-психологічної безпеки. Відповідно виникає необхідність глибокого наукового дослідження з метою прогнозування особливостей функціонування цих політико-правових механізмів.

Інформаційне суспільство породило таку категорію як «інформаційне управління». Треба зазначити, що в теорії державного управління цей аспект проблеми ще тільки осмислюється [118, с.321]. Даний перспективний напрямок теоретичного дослідження теж ще чекає свого часу на реалізацію.

Саме зміни в характеристиках управління, пов'язані з трансформацією управління в маніпуляцію або іншими словами – злиттям понять «управління» та «інформація» в системі масових комунікацій. Найбільш повно маніпулятивні технології управління масовою комунікацією знаходять свою реалізацію в т.з. технологіях зв'язків з громадськістю (Public Relations). З більш ніж 500 визначень PR, прийнятих у всьому світі найбільш узагальненим та універсальним представляється наступне: PR – це управлінська діяльність, направлена на встановлення взаємовигідних комунікативних відносин між організацією та громадськістю, від якої залежить успіх функціонування даної організації. PR представляє собою самостійний вид діяльності організації.

Для узгодження з інформаційними процесами в системі масових

комунікацій застосовується також мотиваційне управління як частина загального процесу управління, що забезпечує усвідомлення і вибір способів перетворення впливів зовнішнього і внутрішнього середовищ на основі оцінювання ситуації, цілепокладання, прийняття рішень, очікування і коригування відповідних результатів діяльності.

Дослідження мотиваційного управління, яке по суті є різновидом інформаційного управління, що застосовується для управління соціальними комунікативними системами свідчить, що процеси управління завжди мають місце там, де здійснюється загальна діяльність людей для досягнення певних результатів. Управління здійснюється за загальними законами у всіх складних динамічних системах – соціальних, біологічних, технічних, економічних і ін. – і основане на отриманні, обробці і передачі інформації.

Основним нормативними документами, що регламентують управлінську діяльність в сфері інформаційної політики є ряд Законів України, а саме: «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про Національну раду України з питань телебачення і радіомовлення», «Про систему Суспільного телебачення і радіомовлення України», «Про рекламу», «Про державну підтримку засобів масової інформації», «Про соціальний захист журналістів».

З метою покращення державного управління інформаційно-психологічною безпекою необхідно дослідити результати можливих змін до чинного законодавства щодо: запобігання процесам концентрації власності та монополізації вітчизняного інформаційного ринку (субринків), зокрема телебачення і радіомовлення; забезпечення прозорості відносин власності стосовно засобів масової інформації з метою унеможливлення маніпулювання громадською свідомістю; удосконалення процедури реєстрації та перереєстрації друкованих засобів масової інформації; встановлення

відповідальності за порушення законодавства у сфері захисту суспільної моралі.

Для успішної реалізації державницької політики в сфері масових комунікацій необхідно внести ряд змін до Закону України «Про телебачення і радіомовлення» [107] з метою: заборони створення і діяльності телерадіоорганізацій, засновником (співзасновниками) яких є нерезидент (нерезиденти), зареєстрований (зареєстровані) в офшорних зонах або в країнах, законодавство яких не передбачає надання інформації про засновників або власників за запитом української сторони; поетапного встановлення квот щодо присутності в ефірі телерадіоорганізації аудіовізуального продукту, виробленого в одній країні.

Також необхідно здійснити впровадження широкодоступного цифрового мовлення у прийнятні строки; реалізувати заходи щодо створення та належного функціонування системи суспільного телебачення і радіомовлення з урахуванням необхідності захисту суспільної моралі, інтересів, культурних цінностей та плюралізму засобів масової інформації під час впровадження цифрового мовлення.

Забезпечення розвитку сфери телебачення і радіомовлення вимагає: збільшення покриття території України телерадіомовленням вітчизняних аудіовізуальних засобів масової інформації, зокрема в районах ОРДЛО та в тимчасово окупованому Криму. Система масових комунікацій в Україні буде неповною та відсталою без розвитку власного супутникового мовлення.

Необхідно вдосконалювати кабельне телерадіомовлення, модернізувати мережі поширення програм національного радіомовлення, оптимізувати та поновити роботу мереж середньохвильового і короткохвильового радіомовлення із збільшенням загального охоплення програмами населення в сільській місцевості, гірських районах та населених пунктах, де відбулася найбільша руйнація системи дротового мовлення.

Першочерговим управлінським завданням виступає розробка комплексної програми розвитку державної телерадіокомпанії «Культура» з

урахуванням необхідності створення системи суспільного мовлення; використання широкосмугових телекомунікаційних мереж з високою пропускною здатністю для забезпечення Інтернет-мовлення.

Потребує вдосконалення державне управління Українським національним інформаційним агентством «Укрінформ» з метою підвищення ефективності його діяльності до рівня провідних європейських інформаційних агентств.

Не в останню чергу стоїть завдання дослідження розширення міжнародного співробітництва в інформаційній сфері, зокрема сприяння обміну інформаційними продуктами між вітчизняними та зарубіжними засобами масової інформації.

Для організації ефективної взаємодії з українською діаспорою необхідно налагодити співробітництво між вітчизняними засобами масової інформації та засобами масової інформації українських громад за кордоном.

Не обійдеться Україна і без розширення мережі кореспондентських пунктів вітчизняних ЗМІ за кордоном, створення належних умов для їх діяльності.

Надійним способом формування позитивного іміджу України на міжнародній арені є збільшення обсягів розповсюдження за кордоном вітчизняної друкованої продукції, зокрема іноземними мовами; забезпечення трансляції програм вітчизняного телерадіомовлення на територію інших країн, зокрема шляхом розроблення та виконання комплексної програми розвитку державної телерадіокомпанії «Всесвітня служба «Українське телебачення і радіомовлення» та «Всесвітньої служби «Радіо Україна» Національної радіокомпанії України [124].

Уряд України уповноважив колишнього главу міністерства культури і інформаційної політики (МКІП) Олександра Ткаченко на підписання угоди з Euronews про запуск медіапроекту Euronews Ukraine у 2021 році. Функціонування української редакції міжнародного телевізійного каналу «Euronews» було припинено у 2017 році. Договір про створення української служби Euronews був укладений в жовтні 2010 року між національною

телекомпанією України (НТКУ) і європейським інформаційним телеканалом. У 2014 році нове керівництво НТКУ заявило про припинення відносин як невигідних з фінансової точки зору для української сторони, а також через неможливість впливати на контент української версії Euronews. Глава НТКУ Зураб Аласанія в січні 2015 року говорив, що заборгованість НТКУ перед Euronews становила на той момент 11 млн євро.

Завдання держави постійно вживати заходи, спрямовані на розширення сфери використання української мови як комунікативного засобу в національному інформаційному просторі України, політико-правовими механізмами державного управління не дати зруйнувати мовно-інформаційний український простір, демонтувати колективну національну пам’ять.

Світовий досвід показує, що держава повинна встановлювати заохочувальні тарифи, ставки, пільги, а також обов’язкові норми на поширення інформаційної продукції, виконання художніх творів українською мовою вітчизняними і зарубіжними виробниками, авторами тощо. Держава в свою чергу, відповідно до законів України, гарантує вільне використання в інформаційній діяльності мов народів і національних меншин України.

Держава повинна контролювати збереження, реконструкцію та реорганізацію елементів і об'єктів інформаційної інфраструктури провідного значення незалежно від форм власності, шляхом управління ними ліцензуванням та реєстраційними процедурами, сприяти дослідженню та впровадженню новітніх комунікативних технологій в інформаційній інфраструктурі України, створювати сприятливі умови для проведення науково-дослідних та конструкторських робіт у цій галузі.

Збір зарубіжними представниками на території України відкритої інформації та переміщення інформації через кордон необхідно обмежувати законодавчо на підставі інтересів національної безпеки, контролювати митними органами та органами охорони державної таємниці відповідно до законів України.

Процес реформування Збройних сил України також супроводжується

радикальними змінами в інформаційній сфері, а отже, особливої актуальності набуває потреба дослідження удосконалення наявних комунікативних систем зв'язку і автоматизації.

З досвіду інших країн наведемо приклад, коли для покращення державного управління масовими комунікаціями у воєнній сфері в США розробили версію Інтернету для військових цілей, оскільки нові мережеві загрози і атаки вимагають революційних підходів до забезпечення інформаційної безпеки. Компанія «Локхід Мартін» отримала контракт на суму 31 млн. доларів від Агентства перспективних оборонних розробок DARPA США. Інструменти, які розроблені в рамках нового проекту, забезпечують боєздатність армії США навіть в умовах масованих кібератак [131.].

Отже, для створення в Україні розвиненого національного інформаційного простору і захисту її інформаційно-психологічного простору необхідна державна підтримка вітчизняного виробника інформаційної продукції та телекомунікаційного обладнання, національних операторів телекомунікацій, зокрема, шляхом створення нормативно-правових, фінансових, фіскальних та інших передумов.

Зауважимо, що сьогоднішня ситуація з управлінням інформаційно-психологічною безпекою України призвела до того, що держава знаходиться в стані системної дезорганізації, яка проявляється в тому, що держава не являється чітко вираженим суб'єктом управління і розвитку, вона не сформувала прозору стратегію розвитку (яку розуміє і сприймає переважна частина населення), не забезпечила нормальні умови життя своїм громадянам, не гарантує дотримання основних конституційних прав. Це відбувається внаслідок нездатності України адекватно реагувати на професійно організовані рядом країн інформаційно-психологічні операції, спрямовані на перехоплення державного управління.

Виходячи із аналізу ситуації, можна запропонувати наступні пропозиції щодо оптимізації політико-правових механізмів забезпечення інформаційно-психологічної безпеки: Офісу Генерального прокурора посилити нагляд за

додержанням законів щодо правопорушень у сфері свободи слова та права на інформацію, вжити координаційних заходів щодо проведення перевірки фактів неправомірних дій окремих установ і посадових осіб органів державної влади тощо; Національній раді з питань телебачення і радіомовлення забезпечити дотримання вимог законодавства щодо контролю за реалізацією інформаційної політики держави в сфері телебачення і радіомовлення, а також посилити власну роль і відповідальність за розвиток та якісний стан телебачення й радіомовлення України, за зростання професійного, художнього рівня програм та передач телерадіоорганізацій тощо; органам місцевого самоврядування та державної виконавчої влади на місцях спільно з Фондом державного майна забезпечити ефективний захист майнових прав суб'єктів інформаційно-видавничої сфери комунальної та інших форм власності. Не допускати вилучення з цієї сфери та передачі для використання не за призначенням приміщень, устаткування та обладнання, іншого майна друкарень, редакцій, періодичних видань, телерадіоорганізацій і земельних ділянок, на яких ці об'єкти розташовані.

Таким чином, аналіз наукової літератури з дослідження державного управління інформаційно-психологічною безпекою України показав, що цей напрям управлінської діяльності тільки викристалізовуються та здійснюється пошук їх оптимальних варіантів. Сьогодні людство стоїть перед викликом гібридних війн. Саме такі війни породжують формування нового гібридного світу, точніше – гібридного світоустрою. Точкою відліку для формування гібридного світоустрою стала агресія Росії проти України. Пряма анексія Криму росією та її дії на Донбасі є основою початку нової світової гібридної війни. Саме за таких умов стає очевидним зростання впливу засобів масової комунікації та масової культури в цілому на динаміку соціальних і комунікаційних процесів. Сучасні виклики часу вимагають створення ефективної комплексної системи державного управління інформаційно-психологічним простором.

Ключова проблема інформаційної (інформаційно-технічної та

інформаційно-психологічної) безпеки України - це проблема концептуального, доктринального і законодавчого її забезпечення, формування комплексу нормативно-правових регуляторів даної сфери. На даний момент, на жаль, таке забезпечення або відсутнє, або не відповідає дійсності, штучно підігнаним під кон'юнктурні вимоги. Концептуально національну інформаційно-психологічну безпеку автор пропонує розглядати як провідний вид суспільних інформаційно-психологічних відносин щодо недопущення або зведення до мінімуму шкоди, що завдається життєво важливим інтересам особи, суспільства, держави.

Сьогоднішня ситуація з недосконалістю державного управління інформаційно-психологічною безпекою України призвела до того, що держава знаходиться в стані системної дезорганізації, посиленою негативними наслідками агресії з боку росії, в якому вона не стала чітко вираженим суб'єктом управління та розвитку. В результаті прагнення стати відкритим суспільством, Україна стала більш вразлива через неможливість запроваджувати дієві заходи контролю над інформаційними потоками. Сприяє такому стану речей і відсутність раціональної управлінської стратегії інформаційної безпеки і методів її реалізації.

Інформаційно-психологічна безпека України не виділена як одна з визначальних у спектрі безпекових складових. Політико-правові механізми державного управління нею чітко не визначені, фрагментовані та неузгоджені, а передовий іноземний досвід не запроваджується. За роки незалежності України так і не було прийнято Закон України «Про інформаційно-психологічну безпеку», де було б чітко визначено суб'єктів державної політики національної безпеки у даній сфері діяльності та політико-правові механізми її реалізації.

Проблеми та перспективи розвитку системи правового забезпечення інформаційно-психологічної безпеки в Україні. Забезпечення національної безпеки передбачає здійснення цілеспрямованої, широкомасштабної та багатопланової діяльності різних суб'єктів. Найважливішою умовою ефективності їх роботи є створення відповідним чином організованої системи, яка передбачає певне об'єднання зусиль суб'єктів, упорядкування їх функцій та

взаємовідносин, цілеспрямоване використання їх можливостей в умовах протидії сучасним загрозам, що виникають у різних сферах суспільного життя. Інституційна підсистема є елементом системи забезпечення ІПБ поряд з правовим та інструментальним компонентами, що охоплюють перелік суб'єктів такого забезпечення. З іншого боку, вона також може розглядатися як частина загальної системи забезпечення інформаційної безпеки України, яка є сукупністю сил і засобів забезпечення інформаційної безпеки [Закон про нац.безпеку]. Ми підтримуємо позицію дослідників щодо доцільності умовного поділу системи забезпечення безпеки на дві підсистеми: державну, що включає органи публічної влади та недержавну, що охоплює громадян та громадські інститути. Основним суб'єктом забезпечення інформаційно-психологічної безпеки була та залишається держава, незважаючи на тенденції зростання потенціалу недержавних суб’єктів на внутрішньополітичній та міжнародній арені. Вони виступають суб'єктами забезпечення ІПБ та реалізують свої функції в даній сфері в межах своїх повноважень.

Проаналізувавши інституційну підсистему забезпечення ІПБ, можна прийти до висновку, що в Україні є різні органи державної влади, що виконують окремі завдання в сфері інформаційної безпеки відповідно до свого профілю діяльності (оборона, державна безпека, масові комунікації та ЗМІ тощо). Серед експертів іноді виникає дискусія щодо необхідності створення спеціалізованого органу щодо забезпечення інформаційної безпеки. На наш погляд, на поточному етапі розвитку української державності доцільності у цьому немає. Оскільки сфера інформаційної безпеки, до якої входить ІПБ, надзвичайно велика і включає в себе безліч напрямків, які дуже важко об'єднати у цілісний функціонал одного державного органу.

На нашу думку є необхідність у іншому шляху удосконалення інституційної підсистеми забезпечення ІПБ – створення державної системи реагування на загрози інформаційно-психологічній безпеці. Пропонована нами система (умовна назва – система «ПСІ-РАДАР») має об'єднати мережу територіально розподілених центрів виявлення та реагування на інформаційно-

психологічні загрози, що поєднують державні органи національного та регіонального рівнів, органи місцевого самоврядування, зацікавлені громадські об'єднання, інші НКО, ЗМІ та інші інститути громадянського суспільства. У рамках даної системи необхідна координація роботи по лінії інформаційного протиборства.

Крім органів публічної влади, важливі завдання у сфері забезпечення ІПБ виконують інститути громадянського суспільства та інші структури, що входять до недержавної підсистеми забезпечення безпеки. Що стосується сфери ІПБ, роль недержавної підсистеми винятково важлива. Насамперед це зумовлено потребою задіяти потужний потенціал громадських інститутів на користь забезпечення безпеки. Крім того, у сфері масової комунікації основна частина ЗМІ, інтернет-ресурсів та інтернет-посередників знаходиться у приватній власності, а тому без їхньої участі неможливо ефективно протидіяти інформаційним ризикам [49].

До основних недержавних учасників системи забезпечення ІПБ автор відносить: 1) засоби масової інформації; 2) власників (адміністраторів) інтернет-сайтів, аудіовізуальних сервісів та соціальних мереж; 3) творців контенту, включаючи блогерів; 4) інформаційних посередників; 5) виробників засобів забезпечення інформаційної безпеки; 6) громадські та релігійні об'єднання, інші некомерційні організації; 7) освітні та науково-дослідні установи (організації).

Нами представляється необхідним доповнення вітчизняного законодавства положеннями про основи правового забезпечення інформаційно-психологічної безпеки.

Надання інформаційній безпеці статусу стратегічного національного пріоритету в Стратегії НБ вимагає зміни ситуації та повноцінної правової регламентації основ забезпечення інформаційної безпеки на рівні законів України. Найбільш перспективною нам видається ідея кодифікації інформаційного законодавства та виділення у структурі майбутнього Інформаційного кодексу окремого розділу з інформаційної безпеки. Тому на

сучасному етапі ми вважаємо за доцільним доповнення змісту Закону України «Про інформацію» базовими нормами щодо забезпечення інформаційної безпеки. Наша авторська пропозиція полягає у внесенні до цього закону окремої статті щодо забезпечення ІПБ. Таке рішення забезпечить побудову логічної та цілісної системи правового регулювання інформаційної безпеки, що включає спочатку базові основи її забезпечення, а потім правові норми щодо двох фундаментальних напрямів її забезпечення – захисту інформації та інформаційно-психологічної безпеки.

2.2. Зарубіжний досвід державно-управлінської практики щодо забезпечення інформаційно-психологічної безпеки та можливості його використання в Україні

Сьогодні, в умовах глобалізації, інтелектуалізації злочинності, охоплення інформатизацією всіх суспільних відносин, існує необхідність в удосконаленні чинних і розробці уніфікованих нормативно-правових актів щодо регулювання інформаційної безпеки України.

Розробки науковців показують, що першість у забезпеченні інформаційної безпеки у світі належить США, країнам ЄС, Японії, Канаді, Ізраїлю та РФ. В даній роботі буде досліджено досвід державно-управлінської практики щодо забезпечення інформаційної безпеки головних стратегічних партнерів України, а саме США та деяких країн Європейського Союзу.

Ефективність інформаційної безпеки будь-якої держави насамперед залежить від досконалості нормативно-правового регулювання діяльності інформаційної системи державних і громадських органів. Законодавство США у сфері зовнішньої інформаційної безпеки включає сукупність федеральних законів, законів штатів та нормативних актів, які разом складають правову основу для утворення й здійснення державної політики у сфері інформаційної безпеки. Законодавство штатів різниться одне від одного, оскільки нормативні акти окремих штатів є досить відмінними [118].

Розглядаючи положення законодавства США в інформаційній сфері, слід

відзначити, що вони, з одного боку, спрямовані на забезпечення права громадян на інформацію та конфіденційність їхнього приватного життя, а з іншого – на зовнішню інформаційну безпеку. Це свідчить про збалансованість у законодавстві інтересів людини, суспільства та держави [143].

Формування та проведення єдиної державної політики забезпечення інформаційної безпеки з урахуванням інтересів національної безпеки держави проводиться у США починаючи з 1967 року. Станом на сьогодні створена дуже міцна законодавча база політики забезпечення інформаційної безпеки [154].

Слід зауважити, що саме події 11 вересня у Нью-Йорку спричинили трансформацію уявлень як про національну безпеку США в цілому, так і про інформаційну безпеку як її ключову складову. Зокрема, відбулося формування нової парадигми національної безпеки США, яка ґрунтується на усвідомленні повної залежності національної інфраструктури від інформаційних систем та мереж країни [156].

Забезпечення інформаційної безпеки в США здійснюється за рахунок комплексного використання трьох основних складових: нормативно-правового регулювання, ефективної системи державного управління та скоординованої діяльності державних структур, постійне вдосконалення технічної бази [12]. Важливим є той факт, що фінансування забезпечення інформаційної безпеки США щорічно збільшується на сотні мільйонів доларів США.

Варто зазначити, що США мають величезний досвід у сфері впровадження інформаційних технологій в діяльність держави з усіх напрямів. Досвід США представляє зацікавленість у сфері розвитку воєнних і розвідувальних технологій не тільки всередині військово-промислового комплексу, але й у питаннях державного стимулювання та підтримки інформаційних комерційних технологій. Особливо важливим є американський досвід використання інформаційних технологій для створення систем зв'язку та військового управління, а також високоточної зброї [22].

Американський досвід державної політики у сфері інформаційної безпеки може бути актуальним для багатьох питань української зовнішньої та

внутрішньої політики. Насамперед, необхідно звернути увагу на такий аспект американського досвіду в сфері забезпечення інформаційної безпеки як ефективний підхід до регулювання ринку інформаційних технологій в умовах ринкової економіки. Україна має достатній потенціал для того, щоб бути повноправним учасником інформаційного суспільства. Зазначимо, що ефективність державної політики має не менш важливу роль, у порівнянні з рівнем технологічного розвитку [78, с. 270].

Хоча відставання України від світових лідерів в інформаційній сфері за останні роки скорочується, зберігається наша залежність від іноземних інформаційних технологій та програмного забезпечення. Це створює суттєву загрозу національній безпеці України [49].

Україні, як і іншим державам, необхідно виробити виважену політику держави в інформаційній сфері. Тому, саме досвід США у сфері забезпечення інформаційної безпеки може бути надзвичайно корисним [22].

Необхідно визнати, що забезпечення інформаційної безпеки в Україні, насичення держави новими технологіями, розвиток приватного бізнесу, тощо, відбувається на даний час при мінімальному нормативно-правовому забезпеченні. Для порівняння, в США сфера інформаційних та інших технологій, сфера руху інформації регламентується більше ніж 300 законами та підзаконними актами.

Інформаційна безпека може стати одним із основних напрямів взаємовигідного співробітництва між Україною та США [75]. Активну політику в сфері інформаційної безпеки проводить також і Європейський Союз. Сьогодні Європейський Союз об'єднує високорозвинуті країни, які здійснюють неабиякий вплив на міжнародні відносини, встановлюючи норми і стандарти поведінки держав в політичній, економічній, соціальній, інформаційній та інших сферах [37].

Варто констатувати, що країни ЄС мають злагоджену систему забезпечення інформаційної безпеки, але водночас кожна країна має свої закони, положення, інструкції щодо врегулювання питань інформаційної

безпеки [130]. Наприклад, для законодавства Німеччини характерне детальне розроблення системи різних видів інформації з обмеженим доступом, чіткі формулювання їх визначень у федеральному законодавстві (Закон «Про перевірку безпеки» [146]). Також, у Німеччині відбувається нарощування потенціалу для ведення кібервійн, що свідчить про перехід Німеччини до принципу «активної оборони», адже раніше основна увага приділялася тільки питанням гарантування безпеки інформації. Виділення наступального складника інформаційног о протиборства в окрему структуру, за оцінками німецьких експертів, є адекватною відповіддю на наявні загрози інформаційній безпеці, а також підкреслює прагнення Німеччини забезпечити відповідність можливостей бундесверу сучасним реаліям [89, с. 107].

Національна інформаційна політика Республіки Польща зорієнтована на побудову вільного відкритого суспільства, забезпечення прав людини, впровадження концепції вільного транскордонного обігу інформації, створення незалежних і плюралістичних масмедіа. Її правовим підґрунтям є «Закон про пошту і телекомунікації», «Закон про телебачення і радіомовлення», «Закон про державні відносини з римською католицькою церквою в Республіці Польща», в яких визначаються напрями інформаційної політики, встановлюються технологічні стандарти інформаційного зв'язку, форми залучення іноземних інвестицій (від 33% до 49% іноземного капіталу), ліцензування інформаційної діяльності. Окремо визначаються права церкви на інформаційну діяльність, з огляду на значний вплив клерикальної інформації на політичні пріоритети та моральність польського суспільства [129].

На відміну від Польщі, Угорщина адаптувала до вимог НАТО чинне раніше законодавство про захист державних і офіційних секретів (Закони 1995 та 2001 років). Загалом угорська політика у сфері інформаційної безпеки налаштована переважно на впровадження обмежень. Так, «Закон про засоби масової інформації», ухвалений 2010 року, піддався критиці з боку світових засобів масової інформації та ЄС, адже Угорщину звинуватили в запровадженні тотального контролю за ЗМІ, разом із Інтернетом, у ліквідації свободи слова та

навіть у прагненні встановити тоталітарний режим [129]. Згодом уряд Угорщини вніс деякі поправки, проте основні положення так і залишаються дійсними [38].

У Хорватії із 2007 року діє Акт про інформаційну безпеку, що визначає поняття інформаційної безпеки, її заходи й стандарти, а також сфери інформаційної безпеки та компетентні органи для ухвалення й реалізації рішень у сфері гарантування інформаційної безпеки, а також нагляду за дотриманням стандартів інформаційної безпеки. Зокрема, інформаційна безпека визначена як стан конфіденційності, цілісності й доступності інформації, що досягається шляхом реалізації політики зах одів і стандартів і організаційної підтримки робочих місць, планування, реалізації, оцінки й відновлення заходів і стандартів [130].

Варто зазначити, що досягнення інформаційної безпеки, зокрема й шляхом активних інформаційних операцій, наприкінці минулого століття стало важливим компонентом боротьби Хорватії за свої тимчасово окуповані території, на яких понад чотири роки існувала сепаратистська «Республіка Сербська країна». За оцінками експертів, якщо в мілітарному значенні боротьба за повернення вказаних територій закінчилася в серпні 1995 року то в інформаційному сенсі війна закінчилася лише через 15 років зі дня закінчення бойових дій [85], і запорукою перемоги в цій інформаційній війні була постійна боротьба за «вуха, очі та розум» населення окупованих територій, а також протидія інформаційній агресії супротивника [131].

Політика інформаційної безпеки на національному рівні реалізується державними органами влади та неурядовими організаціями. Урядові установи відповідають за розробку і координацію політики в сфері інформаційної безпеки. Втілення у життя державної політики належить до компетенції структурних підрозділів міністерств, комп'ютерними групами швидкого реагування на інциденти в сфері інформаційної безпеки та ус тановами з питань захисту даних. З ініціативи або за підтримки державних органів влади в країнах ЄС реалізується низка інформаційно-освітніх та дослідницьких проектів,

присвячених проблемі інформаційної безпеки. Роль неурядових організацій полягає, насамперед, в інформуванні громадськості про загрози і ризики в сфері інформаційної безпеки та способи захисту від них через розробку і реалізацію відповідних проектів, зокрема веб-сайтів, присвячених безпеці інформаційних технологій [37].

Для України як держави, що зіткнулася із проблемами втягнення в гібридну війну та наявністю тимчасово окупованих територій, досвід країн ЄС щодо гарантування інформаційної безпеки є доцільним для розгляду. Зокрема приклад Хорватії, протидія сепаратизму в якій закінчилася успішною реінтеграцією самопроголошеної «республіки». Відповідно, варто використовувати передові методи протидії російській інформаційній агресії, постійно представляти якісний інформаційний продукт на тимчасово окупованих територіях. Доцільним буде також наслідувати досвід Німеччини в переході до принципу «активної оборони» щодо інформаційної безпеки. Постійна діяльність компетентних органів, спрямована на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу може надати значні переваги в умовах гібридної війни з рф [131].

Окремо доцільно зупинитися на проблематиці встановлення міжнародно-правових стандартів у сфері забезпечення інформаційно-психологічної безпеки. Глобальний характер інформаційних загроз детермінує необхідність зближення підходів держав та світової спільноти загалом щодо протистояння їм. Міжнародне право, його норми та принципи продовжують відігравати важливу роль у регулюванні міжнародних відносин та закріпленні правових стандартів для національних правових систем. Міжнародно-правове регулювання забезпечення ІПБ здійснюється нормами цілого ряду галузей міжнародного права, включаючи право міжнародної безпеки, міжнародне гуманітарне право, право прав людини, міжнародне кримінальне право та ін. При цьому в міжнародно-правових актах поняття ІПБ не використовується. Натомість йдеться про окремі її складові: захист дітей від небезпечної інформації,

недопущення розпалювання ненависті та ворожнечі, боротьбу з поширенням дитячої порнографії та ін.

Логічно провести дослідження релевантних міжнародно-правових норм, що стосуються забезпечення ІПБ, у межах наступних тематичних груп міжнародних актів у сферах: 1) прав людини; 2) ЗМІ та мережі Інтернет; 3) боротьби зі злочинністю та тероризмом в інформаційному просторі; 4) міжнародної інформаційної безпеки.

Міжнародно-правові акти у сфері прав людини. Загальна декларація прав людини від 10 грудня 1948 року (далі - Загальна декларація) та Міжнародний пакт про цивільні та політичні права від 16 грудня 1966 року (далі - Міжнародний пакт) у числі основних прав людини закріплюють право на свободу думки, совісті та релігії (ст. 18 Загальної декларації та Міжнародного пакту), право на свободу переконань та їх вільне вираження (ст. 19 Загальної декларації та Міжнародного пакту).

Названі міжнародні акти передбачають допустимість обмеження зазначених прав. Як правомірні цілі обмеження зазначені: «забезпечення належного визнання та поваги до прав і свобод інших та задоволення справедливих вимог моралі, громадського порядку та загального добробуту в демократичному суспільстві» (ч. 2 ст. 29 Загальної декларації), «охорона громадської безпеки, порядку, здоров'я та моралі, так само як і основних прав і свобод інших осіб» (ч. 3 ст. 18 Міжнародного пакту); «для пошани прав та репутації інших осіб; для охорони державної безпеки, громадського порядку, здоров'я чи моральності населення» (ч. 3 ст. 19 Міжнародного пакту).

Крім того, у ст. 4 Міжнародного пакту закріплено право держав відступати від своїх зобов'язань під час «надзвичайного становища у державі, за якої життя нації перебуває під загрозою» (інститут дерогації). Для України це означає можливість запровадження додаткових правових обмежень в умовах особливих правових режимів надзвичайного та військового стану. Обмеження основних прав допускається «наскільки це потрібно гостротою становища, за умови, що такі заходи є несумісними зі своїми іншими зобов'язаннями з

міжнародного права і тягнуть у себе дискримінації...». Україна скористалася цим правом коли 2 грудня 2014 року було створено Міністерство інформаційної політики України, як реакція на збройну агресію рф проти України. Міжнародний пакт містить низку обмежень свободи вираження поглядів. Відповідно до ст. 20 цього акту «будь-яка пропаганда війни», а також «будь-який виступ на користь національної, расової чи релігійної ненависті, що є підбурюванням до дискримінації, ворожнечі чи насильства» мають бути заборонені законом. Такі правові заборони закріплені й інших міжнародно-правових актах, зокрема щодо «прямого і громадського підбурювання до скоєння геноциду» (п. «з» ст. III Конвенції про запобігання злочину геноциду і покарання нього від 9 грудня 1948 року) , «Заохочення злочину апартеїду» (п. «б» ст. III Міжнародної конвенції про припинення злочину апартеїду та покарання за нього від 30 листопада 1973 року), «заохочення расової дискримінації» (ст. 4 Міжнародної конвенції про ліквідацію всіх форм расової дискримінації від 30 листопада 1973 року).

Міжнародні акти в галузі ЗМІ та мережі Інтернет. Міжнародно-правові акти цієї групи регулюють технічні та змістовні аспекти поширення масової інформації. При цьому в міжнародному праві в галузі масової інформації дотепер немає базового універсального міжнародного договору.

Щодо регулювання контенту ЗМІ першорядне значення мають норми міжнародних документів про права людини, які гарантують право на свободу переконань та на вільне їх вираження, включаючи свободу шукати, отримувати, поширювати інформацію та ідеї будь-якими способами та незалежно від державних кордонів. Свобода масової інформації оцінюється як форма реалізації свободи самовираження. Відповідно до неї застосовчі норми про допустимість правових обмежень та правові заборони про пропаганду міжнародних злочинів. Останні аспекти детально висвітлено в окремій Декларації, прийнятій Генеральною конференцією ЮНЕСКО.

Ряд важливих міжнародно-правових актів у сфері свободи масової інформації прийнято в рамках Ради Європи. До них належать Декларація

про засоби масової інформації та права людини від 23 січня 1970 року та Декларація про свободу вираження поглядів та інформації від 29 квітня 1982 року. Підтверджуючи гарантії свободи та незалежності ЗМІ, включаючи заборону прямої чи непрямої цензури, ці документи встановлюють ряд вимог до ЗМІ, включаючи виконання своїх завдань із відчуттям соціальної відповідальності. З цією метою рекомендується прийняття кодексів професійної етики для журналістів, у яких мають бути принципи, пов'язані з поширенням достовірної інформації, поділом самої інформації та коментарів, неприпустимістю наклепу, а також дотриманням недоторканності приватного життя. Для контролю виконання цих правил і розгляду спорів, що виникають, необхідно створити установу щодо розгляду скарг осіб, установ та організацій, до якої можливо буде оскаржити дії відповідних осіб, як після судового розгляду та і в позасудовому порядку.

Важливе значення в контексті досліджуваної проблематики мають рекомендації КМРЄ щодо поширення негативної інформації у ЗМІ: № 7 (89) від 27 квітня 1989 року щодо принципів поширення відеозаписів, що містять насильство, жорстокість або мають порнографічний зміст та № 19 (97) від 20 жовтня 1997 року про демонстрацію насильства в електронних засобах масової інформації. В них закріплено такі правові механізми забезпечення ІПБ: а) прийняття кодексів поведінки та інших актів саморегулювання; б) застосування механізмів класифікації та маркування контенту; в) запровадження правових заборон та обмежень на поширення негативної інформації; г) контроль правил поширення контенту та застосування у разі порушення заходів юридичної відповідальності; д) інформування суспільства про можливу небезпеку інформації.

У Рекомендаціях щодо демонстрації насильства в електронних ЗМІ основна відповідальність за контроль за змістом інформації у ЗМІ покладається на їх редакції. Також підкреслюється важливе значення громадського контролю у цій сфері. На батьків та вчителів покладається відповідальність за формування у дітей фільтрів критичного сприйняття образів насильства

шляхом медіа-навчання, за застосування інструментів та методів обмежень доступу дітей до негативного контенту.

У зв'язку зі зростаючою роллю Інтернету робляться спроби міжнародно-правового регулювання відносин, пов'язаних з його використанням, включаючи питання безпеки. Проте таке регулювання досі перебуває на досить низькому рівні. Дотепер практично відсутні імперативні норми, які були б закріплені в міжнародних договорах у цій сфері, що частково компенсується прийняттям міжнародно-правових актів рекомендаційного характеру. До останніх відносяться такі вагомі акти, як Окінавська хартія Світового інформаційного суспільства від 22 липня 2000 року, Декларація принципів «Побудова інформаційного суспільства - глобальне завдання у новому тисячолітті» від 12 грудня 2003 року та інші.

У цих політико-декларативних міжнародних актах наголошується на важливості створення безпечного кіберпростору. Для цього рекомендується поширення етичних принципів на поведінку в кіберпросторі та формування глобальної культури кібербезпеки.

Цілий блок значущих міжнародно-правових актів щодо забезпечення безпеки в Інтернеті прийнятий у Раді Європи. Одним із них є Декларація про свободу обміну інформацією в Інтернеті від 28 травня 2003 року (далі – Декларація про свободу Інтернету). У цьому документі закріплена ідея знаходження балансу між приватними та публічними інтересами, з одного боку та свободою обігу інформації в мережі, з іншого. Декларація про свободу Інтернету закріплює ліберальну модель регулювання обміну інформацією в Інтернеті, що виражається в лімітуванні державного втручання в ці процеси, акценті на саморегулювання при визнанні ролі державного регулювання, а також обмеженні відповідальності інформаційних посередників за зміст інформації, що розповсюджується в мережі.

У 2018 році Комітет міністрів Ради Європи (КМРЄ) прийняв Рекомендацію про роль та відповідальність інтернет-посередників. У документі багато уваги приділено обмеженню доступу до контенту.

Встановлено, що блокування та видалення контенту можуть застосовуватись інтернет-посередниками на підставі як розпоряджень державних органів, так і своїх внутрішніх правил. Рекомендація фактично забороняє державам покладати на інтернет-посередників обов'язок моніторингу стороннього контенту («контенту третьої особи»), до якого вони забезпечують доступ, передають чи зберігають, та обмежує їхню відповідальність за такий контент. Це, у свою чергу, не виключає відповідальності посередників щодо протиправного контенту у разі, якщо вони своєчасно не вжили заходів обмеження доступу до нього, у тому числі при отриманні сповіщення. Рекомендації закріпили вимоги транспарентності та дотримання прав людини. Також у документі містяться вимоги про проходження спеціальної правової підготовки персоналом, який бере участь у модерації контенту.

Міжнародні акти у сфері боротьби зі злочинністю та тероризмом в інформаційному просторі. Проблематика боротьби з кіберзлочинністю перебуває у фокусі уваги міжнародного співтовариства як один із пріоритетних напрямків протидії загрозам цифрового середовища. Боротьбі з кіберзлочинністю присвячені спеціальні резолюції Генеральної асамблеї ООН A/55/63394 та A/KE8/56/121 «Боротьба зі злочинним використанням інформаційних технологій», A/73/187 та A/74/247 «Протидія використанню інформаційно-комунікаційних технологій злочинних цілях». До цього часу відсутній універсальний міжнародний договір, який регламентував би сферу боротьби з кіберзлочинністю.

Найбільш авторитетним регіональним міжнародним договором у сфері боротьби з кіберзлочинністю виступає Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року (далі – Конвенція про кіберзлочинність). Станом на лютий 2022 року її учасниками виступають 66 держав, причому серед них не лише країни – члени Ради Європи, а й держави Північної та Латинської Америки, Африки та Азії. Ситуацію ускладнює те, що рф не ратифікувала цю конвенцію через неприйнятність норм про транскордонний доступ до комп'ютерних даних без повідомлення та згоди

держави.

Пізніше було прийнято Додатковий протокол щодо криміналізації діянь расистського та ксенофобського характеру, що здійснюються за допомогою комп'ютерних систем, від 28 січня 2003 року (далі - Додатковий протокол до Конвенції про кіберзлочинність) та Другий протокол щодо розширення співробітництва та розкриття електронних доказів, від 1 листопада 2021 року. Дані акти визначають склади кіберзлочинів, процесуальні аспекти боротьби з ними, регламентують встановлення юрисдикції та міжнародне співробітництво у боротьбі з кіберзлочинністю.

До сфери ІПБ належать насамперед злочини, пов'язані з дитячою порнографією (ст. 9 Конвенції про кіберзлочинність). Слід зазначити, що дитяча порнографія, виробництво та обіг якої є кіберзлочином, розглядається у міжнародних актах з іншої позиції – як форма сексуальної експлуатації дітей. У такій якості вона знайшла своє відображення у Факультативному протоколі до Конвенції про права дитини, що стосується торгівлі дітьми, дитячої проституції та дитячої порнографії, від 25 травня 2000 року (далі - Факультативний договір) та Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуальних зловживань від 25 жовтня 2007 року (далі – Конвенція про захист дітей).

Даними міжнародними договорами закріплено обов'язок держав здійснити криміналізацію виготовлення та обігу дитячої порнографії, кібергрумінгу («сексуальне домагання до дітей) та інших злочинів, пов'язаних з використанням ІКТ з метою сексуальної експлуатації, встановити серйозні заходи покарання за їх вчинення для фізичних осіб, а також відповідальність юридичних. Крім того, передбачено встановлення державами заборони виробництва та розповсюдження матеріалів, які пропагують такі злочини (ч. 5 ст. 9 Факультативного протоколу, ч. 2 ст. 8 Конвенції про захист дітей).

Аналізуючи положення міжнародних актів, що стосуються тероризму в інформаційному просторі, слід зазначити, що вони стосуються аспектів використання можливостей ЗМІ та Інтернету у діяльності терористичних

організацій. У контексті теми нашого дослідження нас цікавлять питання пропаганди ідеології тероризму та інші форми деструктивного ІПВ з боку екстремістських елементів.

Один із комплексних універсальних міжнародних актів у даній галузі - Глобальна контртерористична стратегія ООН, прийнята резолюцією A/KE8/60/288 Генеральної асамблеї від 8 вересня 2006 року. В ній міститься і окрема норма, що стосується Інтернету: заклик до держав вивчати у співпраці з ООН шляхи та засоби координації зусиль, що вживаються на міжнародному та регіональному рівнях з метою боротьби з тероризмом у всіх його формах та проявах у мережі Інтернет.

Окремо необхідно виділити Конвенцію ШОС щодо протидії екстремізму від 9 червня 2017 року (далі – Конвенція ШОС). У документі багато уваги приділяється боротьбі з проявами екстремізму в інформаційному просторі. Так, серед заходів на національному рівні в Конвенції названо: а) моніторинг ЗМІ та мережі Інтернет з метою своєчасного виявлення та припинення поширення екстремістської ідеології; б) посилення пропагандистської діяльності щодо протидії екстремізму та контрпропагандистської роботи проти поширення екстремістської ідеології; в) обмеження доступу до екстремістського контенту в інформаційно-телекомунікаційних мережах.

Міжнародно-правові акти у сфері міжнародної інформаційної безпеки. Міжнародна інформаційна безпека (далі – МІБ) стійко увійшла до порядку денного роботи провідних міжнародних організацій як один із важливих аспектів міжнародної безпеки. Генеральною асамблеєю ООН починаючи з 1998 року було прийнято цілу низку резолюцій під назвою «Досягнення у сфері інформатизації та телекомунікації в контексті міжнародної безпеки». Росія відіграла ключову роль у просуванні питань МІБ на порядок денний міжнародних організацій. При цьому наша країна дотримується широкого підходу до розуміння інформаційної безпеки, включаючи як інформаційно-технічні, так і соціо-гуманітарні, політико-ідеологічні аспекти.

Надалі було прийнято низку важливих міжнародних договорів

глобального, регіонального та двостороннього рівнів, що утворюють окрему складову системи правового регулювання забезпечення інформаційної безпеки. До них, зокрема, належить Угода між урядами держав - членів ШОС про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року (далі - Угода ШОС у галузі МІБ).

В міжнародному праві, міжнародна інформаційна безпека визначається як «стан глобального інформаційного простору, при якому на основі загальновизнаних принципів та норм міжнародного права та на умовах рівноправного партнерства забезпечується підтримка міжнародного миру, безпеки та стабільності» (п. 6).

Таблиця 2.2 **Види негативного контенту у міжнародно-правових актах**

№ п/п	**Опис негативного контенту**	**Правове джерело**
Інформація, що підбурює до війни, геноциду, апартеїду, що розпалює ненависть чи ворожнечу		
1.	Пропаганда війни	Міжнародний пакт про громадянські та політичні права (ст. 20)
2.	Виступ на користь національної, расової чи релігійної ненависті, що є підбурюванням до дискримінації, ворожнечі чи насильства	Міжнародний пакт про громадянські та політичні права (ст. 20)
3.	Пряме та публічне підбурювання до вчинення геноциду	Конвенція про попередження злочини геноциду та покарання за нього від 9 грудня 1948 р. (п. «с» ст. III)
4.	Заохочення злочину апартеїду	Міжнародна конвенція про припинення злочину апартеїду та покарання за нього від 30 листопада 1973 р. (п. «б» ст. III)
5.	Заохочення расової дискримінації	Міжнародна конвенція про ліквідацію всіх форм расової дискримінації від 30 листопада 1973 (ст. 4)
6.	Расистські та ксенофобські матеріали, мотивована загроза расизму та ксенофобії; расистська та ксенофобська мотивована образа	Додатковий протокол до Конвенції про кіберзлочинність щодо криміналізації діянь расистського та ксенофобського характеру, що здійснюються за допомогою комп'ютерних систем, від 28 січня 2003 (ст. 3-5)
7.	Заперечення, надзвичайна мінімізація, схвалення чи виправдання геноциду чи злочинів проти людства	Додатковий протокол до Конвенції про кіберзлочинність щодо криміналізації діянь расистського та ксенофобського характеру, що здійснюються за допомогою комп'ютерних систем, від 28 січня 2003 (ст. 6)

8.	Програми, що сприяють расовій ненависті	Європейська конвенція про транскордонне телебачення від 5 травня 1989 р. (пп. «б» ч. 1 ст. 7)
Контент терористичного характеру		
9.	Публічне підбурювання до скоєння терористичного злочину	Конвенція Ради Європи про попередження тероризму від 16 травня 2005 р. (ст. 5)
10.	Шокуючі фотографії або зображення терористичних актів, які порушують принципи недоторканності приватного життя та людської гідності жертв або посилюють тероризуючий вплив таких актів на населення, а також на жертв та їхніх рідних	Рекомендація Парламентської асамблеї Ради Європи № 1706 (2005) «ЗМІ та тероризм» (пп. «V» п. 8), Декларація про свободу вираження думок та інформації у ЗМІ у контексті боротьби з тероризмом від 2 березня 2005 р.
11.	Новинна інформація та коментарі, що посилюють соціальну напруженість, яка є основою тероризму, зокрема висловлювання, що розпалюють ненависть	Рекомендація Парламентської асамблеї Ради Європи № 1706 (2005) «ЗМІ та тероризм» (пп. «VI» п. 8), Декларація про свободу вираження думок та інформації у ЗМІ у контексті боротьби з тероризмом від 2 березня 2005 р.
12.	Поширювані терористами через Інтернет незаконні повідомлення та зображення	Рекомендація Парламентської асамблеї Ради Європи № 1706 (2005) «ЗМІ та тероризм» (пп. «V» п. 10)
13.	Інформація, що створює загрози для безпеки людей та проведення антитерористичних операцій чи судового розслідування терористичної діяльності	Декларація про свободу вираження поглядів та інформації у ЗМІ у контексті боротьби з тероризмом від 2 березня 2005 р.
Контент, що містить жорстокість та насильство ,інша соціально небезпечна інформація		
14.	Програми, що надмірно виділяють насильство	Європейська конвенція про транскордонне телебачення від 5 травня 1989 р. (пп. «б» ч. 1 ст. 7)
15.	Відеозаписи, що містять насильство, жорстокість	Рекомендація Комітету міністрів Ради Європи № К (89) 7 від 27 квітня 1989 р. щодо принципів розповсюдження відеозаписів, що містять насильство, жорстокість або мають порнографічний зміст
16.	Нічим не виправдане зображення насильства (повідомлення, слова та зображення, що містять насильство або символізують насильство, яке займає першорядне становище і при цьому не знаходить виправдовувачів обставин у контексті)	Рекомендація Комітету міністрів Ради Європи № К (97) 19 від 20 жовтня 1997 р. про демонстрацію насильства в електронних засобах масової інформації

17.	Повідомлення, що спонукають до думки захоплюватися тими чи наслідувати тих, хто споживає тютюн, алкогольні напої чи наркотичні речовини	Рекомендація Комітету міністрів Ради Європи № К (86) 14 від 16 жовтня 1986 р. про підготовку стратегії боротьби з курінням, зловживанням алкогольними напоями та наркоманією у співпраці з органами, які проводять опитування населення, та засобами масової інформації (ст. 7)
Порнографічні матеріали, непристойна інформація		
18.	Дитяча порнографія	Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції та дитячої порнографії, прийнятий Генеральною асамблеєю ООН 25 травня 2000 р. (ст. 2, 3), Конвенція Ради Європи про кіберзлочинності від 23 листопада 2001 р. (ст. 9) та ін.
19.	Матеріали, які пропагують злочини, пов'язані з торгівлею дітьми, експлуатацією дітей, дитячою порнографією, сексуальними зловживаннями щодо дітей	Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції та дитячої порнографії, прийнятий Генеральною асамблеєю ООН 25 травня 2000 р. (ст. 9), Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуальних зловживань від 25 жовтня 2007 р. (ст. 8)
20.	Непристойні програми	Європейська конвенція про транскордонне телебачення від 5 травня 1989 р. (ст. 7)
Контент, що містить наклеп та образи		
21.	Наклепні твердження	Декларації про засоби масової інформації та права людини від 23 січня 1970 р.
Небезпечна для дітей інформація		
22.	Інформація та матеріали, що завдають шкоди благополуччю дитини	Конвенція про права дитини від 20 листопада 1989 (п. «е» ст. 17)
23.	Програми, які можуть завдати шкоди фізичному, розумовому чи моральному розвитку дітей та підлітків	Європейська конвенція про транскордонне телебачення від 5 травня 1989 р. (ч. 1 ст. 7)
Заборонені чи обмежувані види реклами		

24.	Реклама та телеторгівля: - що вводить в оману або завдає шкоди інтересам споживачів; - здатна заподіяти шкоду інтересам дітям; - закликає неповнолітніх здійснювати угоди з купівлі чи оренді товарів та послуг; впливає на підсвідомість людини; - прихована	Європейська конвенція про транскордонне телебачення від 5 травня 1989 р. (ч. 2-4 ст. 11)
25.	Реклама та телеторгівля певними видами товарів (тютюновими виробами, алкогольними напоями; ліками та способами лікування, які можна отримувати лише за рецептом лікаря)	Європейська конвенція про транскордонне телебачення від 5 травня 1989 р. (ч. 1, 3 та 5 ст. 13)

Таким чином, загрози ІПБ проглядаються у переліку основних загроз МІБ, закріплених у зазначених міжнародних актах у сфері МІБ. Так, наприклад в Угоді ШОС у галузі МІБ окремо виділено загрозу «поширення інформації, що завдає шкоди суспільно-політичній та соціально-економічній системам, духовному, моральному та культурному середовищу інших держав».

Розвиток правового регулювання забезпечення ІПБ у рамках правового поля МІБ видається нам дуже значущим, оскільки транскордонний характер багатьох інформаційних загроз зумовлює необхідність тісної міжнародної співпраці для ефективної протидії їм. При цьому ми підтримуємо включення питань забезпечення ІПБ до загального предметного порядку денного МІБ, її ухвалення в рамках ООН заклало б фундамент для міжнародно-правового регулювання у сфері МІБ на глобальному рівні, який можна розвивати на регіональному рівні та (або) за окремими напрямками забезпечення МІБ, включаючи психологічні аспекти (ІПБ).

2.3. Інформаційно-психологічні загрози як головний фактор розгортання «гібридної війни»

Збройна агресія рф проти України, яку сьогодні експерти за наявними ознаками визначають як «гібридну війну», тільки підтвердила усі прогалини в політичній, економічній, військовій, соціальній, енергетичній та інформаційній сферах життєдіяльності країни за останні п’ять років. Через ворожі дії рф, починаючи з 2014 року й донині, суспільство й держава зіткнулися з реальними загрозами в площині національної безпеки, не кажучи вже про те, що була зруйнована система міжнародних гарантій безпеки України і система європейської безпеки загалом.

Досить промовистими в аналізованому контексті є міркування колишнього радника НАТО, нідерландського парламентарія та генерал–майора у відставці Франка ван Каппена: «Гібридна війна – це змішування класичного типу війни з використанням нерегулярних військових формувань. Держава, яка веде гібридну війну, здійснює угоду з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв’язок із якими повністю заперечується. Ці виконавці можуть здійснювати такі речі, які сама держава здійснювати не може, тому що будь–яка держава зобов’язана слідувати Женевській конвенції та Гаазькій конвенції про закони сухопутної війни, домовленостям із іншими державами. Усю брудну роботу можна перекласти на плечі недержавних формувань» [89].

Цікавим аспектом є те, що фахівці вважають, що інформаційний компонент ведення «гібридної війни» справді грає чималу роль, проте залишаються й прибічники того, що він є тільки другорядним у військовій частині агресії. Але всі вони одностайні в тому, що ворожі дії РФ проти України відбуваються із використанням усіх притаманних «гібридній війни» – від збройного застосування військової потужності до комплексу економічних, енергетичних, інформаційно-психологічних та інших засобів розхитування країни зсередини.

Тематика гібридної війни стала однією з основних серед наукового

дискурсу останніх років у гуманітарних науках. Серед науковців, що присвятили свої роботи цієї тематиці можна виокремити праці В. Горбуліна, О. Полторакова та інших. Заслуговує на увагу аналіз російсько-української «гібридної війни» О. Полторакова, який виділяє таку модель–схему її ведення [89]:

1. Вектори («фронти») першого рівня: квазі–«військовий» (з акцентом на парамілітарні складові на кшталт бойовиків та «нелегальних комбатантів», місцевих «ополченців» та «козацтво», кримінал та маргінес тощо); вектори квазі–«гуманітарний» – з акцентом на забезпечення прав «російського/російськомовного населення») та квазі–«інформаційний» – з акцентом на ідеологічно–пропагандистські настанови, медіа–«картинки», масовані «симулякри», акцентуалізовані стереотипи і т. ін.

2. Вектори («фронти») другого рівня: (гео)політичний (блокування вступу України до НАТО, перспективи внутрішнього розколу в НАТО і т. ін.); (гео)економічний (гальмування розвитку відносин України з ЄС, використання «газової дипломатії» і т.ін.); соціальний (створення жевріючого джерела соціально–політичної та гуманітарно–політичної напруги з потенціалом швидкої ескалації у разі потреби).

Про масштаби інформаційної війни, розгорнуті Росією проти України, найточніше сказав Головнокомандувач об'єднаних Збройних сил НАТО в Європі (2013-2016 роки) Ф. Брідлав: «Це найбільш дивовижний інформаційний бліцкриг, який ми коли-небудь бачили в історії інформаційних воєн» [23].

Цікаву думку із цього приводу також висловлює дослідник Ю. Радковець, він робить висновки про те, що основним уроком з інформаційно-пропагандистської війни росії проти України як важливої складової «гібридної війни» є її безпрецедентний характер за своїми змістом, масштабами і спрямованістю: по-перше, інформаційна війна розпочалася задовго до військової агресії росії проти України і продовжує супроводжувати її на всіх етапах, завчасно адаптуючись під поточні цілі і задачі; по-друге, інформаційно-пропагандистські та дезінформаційні проекти, операції і заходи

спрямовані на всі верстви населення і всі регіони України, а також населення росії і країн Заходу – відповідно, з різними цільовими установками і задачами; по-третє, головна мета інформаційної війни в Україні – ліквідація державності України; в росії – отримання підтримки населення для виправдання дій керівництва росії; для країн Заходу – дискредитація дій керівництва України та її Збройних Сил [114].

Проаналізувавши низку публікацій та врахувавши думки експертів, можна стверджувати, що інформаційна війна проти України ведеться одразу в кількох напрямках. Таким чином до інформаційних фронтів, на які здійснюються пропагандистські впливи, можна зарахувати: 1) населення, що перебуває у зоні конфлікту (Донецька та Луганські області, АРК Крим); 2) громадян України, що проживають на мирній території, але через засилля ворожого інформаційного продукту піддаються сумнівним впливам; 3) населення країни-агресора, де федеральні телеканали є одним із рупорів розпалювання ворожнечі; 4) іноземці та західні політики, які активно спостерігають за подіями через російські міжнародні інформаційні канали.

Окремим пунктом слід виділити тезу британського військового аналітика Р. Торнтона, який зауважив «російський інформаційний продукт розрахований на вплив на розум. Однак ті, на кого впливають, повинні бути відповідно підготовленими. Москва є у виграші стосовно цієї умови, оскільки нові незалежні держави, що раніше були частиною Радянського Союзу, мають велику кількість етнічних росіян, як і російськомовних громадян. Ці російські меншини в таких країнах як Україна, Прибалтика, Молдова та Грузія є принциповою ціллю сьогоднішньої кампанії інформаційної війни з Москвою» [163].

Слід зазначити, що Росія перед анексією Криму і вторгненням у Донбас не один рік створювала в цих регіонах власну інформаційну платформу: медійний сегмент – телеканали, FM-радіостанції, друковані видання, а також інтернет-сайти; елементи соціального тиску – громадські організації проросійського спрямування – козачі дружини, патріотичні організації,

російські земляцтва, товариства російської історії й культури тощо; елементи суспільно-політичного впливу – організації з урядовим фінансуванням росії – «Россотрудничество», рух «Русскоязычная Украина», організації російських співвітчизників в Україні тощо [26]. Водночас найбільш потужними каналами реалізації російського інформаційно-психологічного тиску все ж таки були традиційні та електронні ЗМІ, інтернет, соціальні мережі.

Вагоме значення має той факт, що інформаційна підготовка до анексії простежуються зокрема в окремих випадках інформаційних провокацій з боку російських високопосадовців, що стали особливо помітними з 2006 року. Зокрема, заяви про відділення півострова лунали з боку депутатів російської Держдуми К. Затуліна, В. Жириновського, а у 2008 році під час урочистостей з нагоди 225-річчя Чорноморського флоту РФ у м. Севастополі мер Москви Ю. Лужков закликав порушити питання про повернення м. Севастополя до складу Росії, внаслідок чого він був оголошений персоною нон-грата в Україні [44. с.6].

Т. Черненко наголошує на тому, що свідченням ґрунтовної підготовки до активного використання інформаційного складника в нинішній гібридній війні стало те, що вже в перші дні воєнно-терористичної агресії в окремих містах Донецької та Луганської областей бойовики налагодили процес пошуку проукраїнських стримерів і систематично перешкоджали діяльності представників незаангажованих рв ЗМІ. Вже в перші хвилини після штурму телерадіокомпанії у Донецьку в центральну апаратну зайшли фахівці, які дуже швидко налаштували на частоті державної ТРК трансляцію каналу «Росія 24». Керівництво рф чітко усвідомлює, що чи не найголовніша частина перемоги у гібридній війні полягає саме в охопленні якнайбільшої аудиторії своїм інформаційним продуктом. Формуючи практично «інформаційну резервацію» для споживача такої інформації, з цієї ж причини одразу після анексії Криму прем’єр-міністр рф Д. Медвєдєв віддав розпорядження терміново забезпечити кримську молодь російськими підручниками історії. Міністерством освіти рф було негайно надіслано до видавництв «повідомлення та концепцію змісту,

історико-культурний стандарт із переліком історичних дат, подій, персоналій, понять, обов'язкових для вивчення у школі, включно з інформацією про півострів Крим та його історичне значення» [137].

Суттєвим зауваженням є те, що моніторингові спостереження дослідників засвідчили той факт, що однією із найбільших проблем українського комунікаційного простору було оперативне інформаційне ізолювання окупованих територій проросійськими ЗМІ. Такий процес був зумовлений тотальним контролем медіа та нав'язуванням населенню виключно проросійської ідеології так званого «русского мира». Внаслідок недостатньої насиченості інформаційного горизонту більшість реципієнтів Криму та Донбасу сприйняли й підтримали політику Кремля.

Реалізація інформаційного складника «гібридної війни» з використанням різноманітних негативних для населення та державності інформаційних операцій, відкритої пропагандистської діяльності на злам національної стабільності, цілісності та суверенітету також була спрямована й проти громадян всієї території України [47].

Не потребує додаткового доведення той факт, що наводить психолог Н. Колотій: «Таке явище як «інформаційна війна» досить нове для нас, українців, але ми здогадувалися про її існування вже останні 5 – 6 років, спостерігаючи інформаційний продукт російських ЗМІ. Лавина серіалів, ток-шоу, теленовин тощо. Проти України постійно велась і ведеться інформаційно-психологічна війна, спрямована на руйнування цінностей та пригнічення волі українського народу. Ми відстежуємо досить жорсткий вплив інформаційного сміття на свідомість громадян країни. Дезінформація, зневажання демократичних цінностей, прославлення диктатури «сильної руки», – цією пропагандою російські ЗМІ отруюють психіку українців [57]. Тут варто відмітити, що покриття російських федеральних телеканалів, на зразок «РТР», «НТВ», «Первый канал. Всемирная сеть», «РБК» та ін., присутнє як на окупованих територіях, так і на теренах багатьох українських регіонів, хоч і в менших пропорціях. Російські телеканали в основному були і залишаються

доступні населенню через супутникове та кабельне телебачення, а також мережу Інтернет.

Ще однією характерною ознакою російської інформаційної війни є те, що вона спрямована й проти громадян рф. Заслуговує на увагу також твердження В. Трюхана, що нинішній російській політичній «еліті» небезпечно мати на своїх кордонах економічно успішні демократії європейського зразка. Адже потенційно приклад успішної України, Грузії чи Молдови спонукав би громадян рф замислитися над тим, а чи так усе добре в самій Росії? Політичний хаос у ближньому та, за можливості, в далекому зарубіжжі, війни, економічний занепад і постійні майдани – це ті страшилки, які дозволяють тримати росіян у спокої. Мовляв, у нас все стабільно та мирно завдяки президенту і владі, яка вже набула статусу сакральності. При цьому російська пропагандистська машина навчилася максимально ефективно використовувати чітко зрежисовані картинки, в переважній більшості випадків маніпулюючи фактами та вигадуючи історії про розп'ятих хлопчиків, кров немовлят, яку п'ють українські нацисти, тощо. Саме за рахунок масованої щоденної пропаганди в російському суспільстві домінує образ України як «недодержави» і Заходу – як ворога росії [132].

Важливою, на наш погляд, є думка Г. Почепцова про те, що «у цій інформаційній війні використовуються старі смисли. Російські телеканали все ж таки активно утримують старі, радянські смисли. Населення живе у цих смислах, де влада майже як Бог. Тобто ніхто не підніме голову. Росія використовує слова, які пом'якшують або змінюють смислове навантаження, наприклад: «народний губернатор», «народний мер». Це створює відчуття законності їх дій. Не анексія Криму, а «возз'єднання», «Крим наш» і так далі. Чітко зроблено так, що система скоріше відпрацьовує вербальний фактаж, ніж реальний. Створена досить сильна і потужна система, яка всі ті слова, які ми використовуємо, замінює на інші. А людина, яка це чує, вважає, що те, що сказано і є правдою» [94]. Більшість фахівців називають інформаційний компонент ведення «гібридної війни», що розгорнула рф також, як «смислову

війну», «війну смислів» або «війну сенсів». Основним структурним елементом у цій «смисловій війні» постають «симулякри».

У сучасному словнику іншомовних слів це поняття трактується як (від лат. simulacrum – подоба, копія) – термін постмодерністської філософії, що означає зображення, копію того, що насправді не існує. Сьогодні розуміється як культурне або політичне утворення, що копіює форму вихідного зразка. Копія може бути чого завгодно і яких завгодно смислів [127, с.520].

За В. Горбуліним, прикладами таких симулякрів є: «фашисти в Києві», «звірства каральних батальйонів», «розіп'яті хлопчики», використання Україною заборонених озброєнь. Стратегічна мета експлуатації цих симулякрів – замінити об'єктивні уявлення цільових груп про характер конфлікту тими «інформаційними фантомами», які потрібні агресору [23].

У свою чергу активним послуговувачем такого роду симулякрів є ведучий телеканалу «россия» Д. Кисельов. Слід усвідомлювати, що російське телебачення поширює пропагандистський продукт, адресований передусім мешканцям росії. Живучи в ізольованому середовищі й маючи віддавна спотворену картину світу, вони готові сприймати будь-яку дезінформацію. Російській пропагандистській машині удалося змусити росіян сприймати події в Україні крізь призму радянсько-німецької війни минулого століття, де українці грають роль «фашистів». Повернули до життя навіть пропагандистський штамп «интернациональный долг», яким виправдовували вторгнення радянських військ до Афганістану [140]. Наприклад, відповідним чином подана інформація про трагічну пожежу 2 травня 2014 році в Одесі інспірувала потрапляння тисяч російських добровольців на Донбас з бажанням «вбивати фашистів» [41].

Ще одним вагомим інформаційним фронтом рф є зовнішній, спрямований на створення позитивного іміджу росії за кордоном. Й у випадку ведення «гібридної війни» – дискредитацію України на міжнародній арені. Вплив на іноземців здійснюється завдяки масштабній діяльності різноманітних проросійських «фондів», «культурних товариств», «аналітичних центрів» і

«експертів», що зосереджені в основному в Європі. Також значну російську підтримку активно забезпечують канали RT, Sputnik, що є ефективною інформаційною зброєю, засобом адресного просування російської ідеології і концепції «русского мира». Також відомо, що росія вклала $1 млрд у британський Russia Today. Це призводить також до війни бюджетів і цю війну ми неминуче програємо, оскільки євробюрократи не витрачатимуть такі неймовірні кошти на протистояння, як це робить кремль [49]. Загалом рф щорічно витрачає на ведення інформаційної кампанії не менше 3,5 млрд дол. США.

У свою чергу С. Єременко, виконавчий директор Інституту демократії ім П. Орлика, констатувала, що «Україна програє інформаційну війну на сході власної країни». Натомість на міжнародному рівні Україна виграє, адже якби вона програвала інформаційну війну, то санкцій проти росії вже не було б, вважає прес-аташе представництва ЄС Д. Стулік [63]. Дослідник Г. Перепелиця наводить історичне бачення проблеми, що залишається актуальним й на сьогодні, «вадою України є – прокляття «буферної зони», коли вона опинилася в епіцентрі геополітичного протистояння між ключовими європейськими і світовими гравцями, які намагалися захопити цю «серединну» українську територію. Можливо таке геополітичне розташування й змусило частину української еліти заради виживання відмовитися від власної державності та національної ідентичності й шукати кращої долі в лоні сильнішої російської державності ціною власної свободи. Інша ж її частина продовжувала боротися за державність і соборність України та гуртувати українську націю. Ці дві світоглядні парадигми бачення майбутнього України існують дотепер, навіть попри те, що Україна вже 30 років як незалежна держава» [85].

В цілому, фахівці засвідчують, що російська пропаганда й за кордоном вдається до перекручування фактів, подання неправдивої інформації, посилання фейкових експертів-аналітиків та ведення прихованої пропаганди з метою введення в оману іноземців про правдиві події в Україні. Все це відбувається на

тлі тотальної девальвації глобальної структури безпеки і загрожує не просто розростанням новітніх конфліктів, а й руйнуванням цивілізованого співтовариства.

Проведений аналіз дозволяє стверджувати, що інформаційний складник «гібридної війни» рф проти України об'єктивно є одним із значних чинників її ведення, а масштаби застосування інформаційних маніпуляцій і дезінформації набирають різноманітних форм та особливостей. Державне управління інформаційною безпекою в умовах гібридної війни повинно передбачати здійснення управлінського впливу в декілька етапів в які входять: формування системи забезпечення інформаційної безпеки; виявлення викликів та загроз інформаційній безпеці; оцінка стану та можливостей системи забезпечення інформаційної безпеки; розробка та впровадження інструментарію державного реагування на загрози інформаційній безпеці; моніторинг, спостереження та контроль за забезпечення інформаційної безпеки[47].

Як відомо, визначальною передумовою побудови системи забезпечення ІПБ виступає вивчення комплексу існуючих та потенційних загроз у даній області. Характер і рівень загроз визначає основні напрями діяльності щодо їх попередження та локалізації, форми, способи, засоби та методи вирішення завдань забезпечення національної безпеки при раціональному використанні наявних обмежених ресурсів. В українському законодавстві зі сфери національної безпеки використовується поняття «загроза національній безпеці». В Законі України «Про національну безпеку» зазначається, що «загрози національній безпеці України - явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України»[98].

Нас цікавить група інформаційно-психологічних загроз, пов'язаних із наданням деструктивного ІПВ на людину та соціальні групи. Загрозу інформаційно-психологічній безпеці можна визначити як фактор або сукупність факторів, здатних заподіяти шкоду інтересам особистості, суспільства та

держави за допомогою надання деструктивної інформаційно-психологічної дії.

Загрози ІПБ мають такі характерні риси:

1. Латентний (неочевидний) характер початку дії загрози та труднощі її виявлення. На відміну від традиційної зброї, факт застосування якої досить просто зафіксувати (виявлення звуку пострілу, пуску ракети тощо), загрози ІПБ часто носять неочевидний («невидимий») характер і складно виявляються.

2. Складність ідентифікації. Багато видів деструктивного ІПВ легко маскуються під звичайний психологічний вплив або застосовуються в сукупності з ним, через що визначити їх досить складно. Тому навіть у разі виявлення факту застосування ІСВ часто потрібне використання спеціальних методів ідентифікації загроз ІПЛ (наприклад, експертизи), щоб довести їхній деструктивний характер.

3. Масштаб наслідків. За допомогою вибору виду ІПВ та каналу його трансляції можна значно змінювати територіальний масштаб та об'єктове охоплення впливу. При цьому важливо відзначити, що деякі типи ІПВ здатні впливати на населення цілих країн та регіонів світу.

4. «Гуманність» впливу. На відміну від традиційної зброї багато засобів і методів ІПВ не завдають прямої та швидко відчутної шкоди людині (хоча є приклади «швидкодіючих» методів ІПВ, наприклад застосування психологічного обману для заволодіння грошовими коштами) і дозволяють досягати цілей суб'єкта впливу більш гуманним способом, знижуючи людські страждання. Однак у більш тривалій перспективі подібна «гуманність» виявляється багато в чому уявною, оскільки деструктивне ІПВ здатне детермінувати акти агресії, зростання числа суїцидів, соціальні та навіть міждержавні конфлікти та інші суспільно небезпечні наслідки.

5. Складний механізм дії. Він полягає у складному багатоступінчастому характері ІПВ на людину та соціальні групи, що зумовлюються насамперед особливостями людської психіки та суспільної свідомості. Тому, на відміну від військових засобів ураження, спрогнозувати точний ефект впливу загроз ІПБ дуже важко.

6. Опірність об'єкта впливу загроз означає наявність у людини та соціальних груп «вбудованих» механізмів психологічного захисту, а також можливість навчання технік стійкості зовнішньому ІПВ. Наслідком цієї ознаки є значущість зміцнення внутрішніх захисних «фільтрів» людини як напрямів забезпечення ІПБ.

7. Висока залежність ефекту впливу від обізнаності об'єкта проявляється у можливості значного зниження, аж до блокування, негативного ІПВ при обізнаності людини/соціальної групи про потенційну небезпеку та методи такого впливу. Цим загрози ІПБ відрізняються від деяких інших типів загроз (військових, екологічних та інших), поінформованість про які далеко не завжди дозволяє знизити шкідливий ефект їхнього впливу.

8. Вплив на інші сфери забезпечення безпеки та публічне управління загалом. За допомогою ІПВ на посадових осіб органів влади та місцевого самоуправління, осіб, що приймають рішення (ОПР) можна впливати на прийняття рішень в різних сферах забезпечення безпеки та, навіть ширше, державного управління (наприклад, рішення про розвиток певних систем озброєння, проведення економічних реформ, вступ у військовий конфлікт, оголошення війни та підписання мирних угод, тощо).

У найбільш загальному вигляді загрози ІПБ слід розглядати як сукупність всіх видів деструктивного ІПВ на людину та соціальні групи. В залежності від їх характеристик можна виділити різні види загроз ІПБ.

З метою отримання чіткого та структурованого бачення системи таких загроз дається авторська класифікація загроз інформаційно-психологічній безпеці. Слід зазначити, що у вітчизняній науці частіше приділяється увага аналізу окремих видів загроз ІПБ. На етапі побудови класифікації автор насамперед провів аналіз загроз ІПБ у основних документах стратегічного планування у сфері національної безпеки України та побудував можливу матрицю загроз ІПБ представлена у таблиці 2.3., що відображає широкий спектр загроз ІПБ у політичній, соціальній, культурній та міжнародній сферах. Також загрози ІПБ чітко проглядаються у рамках державної, громадської та

воєнної безпеки.

На основі складеної матриці основних загроз ІПБ, а також з урахуванням результатів власного наукового дослідження, представимо авторську класифікацію основних загроз ІПБ.

Класифікація загроз ІПЛ:

І. Залежно від природи походження

1) антропогенні - види негативного ІПВ, що здійснюється безпосередньо людиною або групою людей вербальними та невербальними методами, у тому числі з використанням технічних засобів, що опосередковують контакт (поширення негативного контенту, шкідлива комунікація тощо);

2) техногенні - види негативного ІПВ, що здійснюється із використанням технічних засобів або іншими штучними об'єктами без участі людини (певні типи випромінювання, голосові помічники тощо).

ІІ. Залежно від типу ІПВ:

1) контентні - загрози ІПБ, пов'язані з впливом негативної інформації (контенту), одержуваної людиною без прямої комунікації між людьми (порнографія, зображення насильства або жорсткості, матеріали, що пропагують тероризм тощо);

2) комунікаційні - загрози ІПБ, пов'язані з негативним міжособистісним чи груповим спілкуванням (обман, маніпуляція свідомістю, підбурювання до самогубства, булінг, газлайтинг тощо);

3) технічні - загрози ІПБ, пов'язані з негативним ІПВ на людину сигналів від технічних пристроїв (спрямоване електромагнітне випромінювання, звуки певної частоти тощо.

ІІІ. Залежно від ступеня сформованості:

1) потенційні - загрози ІПБ, які знаходяться на стадії зародження або формування (наприклад, маніпуляція свідомістю з боку голосових помічників);

2) реальні – загрози ІПБ, які вже набули поширення (наприклад, сексуальні домагання дітей в Інтернеті).

ІV. Залежно від місцезнаходження джерела загрози:

1) внутрішні – загрози ІПБ, джерело яких розташоване всередині країни (наприклад, поширення екстремістських сепаратистських наративів серед населення країни);

2) зовнішні - загрози ІПБ, джерело яких перебуває за кордоном (наприклад, трансляція передачі зарубіжним телеканалом);

3) гібридні (змішані) - загрози ІПБ, що мають кілька джерел, розташованих як усередині країни, так і за її межами.

V. Залежно від тривалості впливу:

1) короткострокові - форми ІПВ, що носять короткочасний характер і мають визначені когнітивні, емоційні та поведінкові реакції людини та соціальних груп (наприклад, шахрайство);

2) тривалі - тривалі форми ІПВ, що мають за мету поетапну зміну психіки людини, суспільну свідомість або колективне несвідоме (наприклад, вплив деструктивних молодіжних субкультур).

VI. Залежно від просторового масштабу впливу:

1) точкові – види негативного ІПВ, межі впливу яких обмежені конкретним місцем (квартира, службовий кабінет тощо);

2) локальні - види негативного ІПВ, що поширюється в межах обмежених територіальних зон (населеного пункту, району, області, регіону тощо);

3) національні - види негативного ІПВ, що впливають на все населення країни у межах національних кордонів;

4) глобальні - види негативного ІПВ, що впливають на певні держави чи світове співтовариство.

VII. Залежно від вибірковості впливу:

1) невибіркового впливу - види ІПВ, вплив яких носить масовий невибірковий (суцільний) характер (сюди належать, перш за все, види ІПВ, що здійснюються через великі ЗМІ та інтернет-ресурси);

2) частково вибіркової дії – види ІПВ, що надають переважний вплив на певні індивідуальні та групові об'єкти, але здатні впливати на інші об'єкти (наприклад, матеріали агітаційного характеру під час місцевих виборів чи

проповіді представника релігійної конфесій);

3) вибіркової дії – види ІПВ, вплив яких жорстко обмежено конкретним індивідуальним чи груповим об'єктом (наприклад, введення в оману конкретної людини в ході міжособистісної комунікації або вплив на членів закритої тоталітарної секти).

У викладеній авторській класифікації видів загроз ІПБ ми позначили їх, відповідно, як *контентні та комунікаційні*. Розглянемо їх послідовно.

Група контентних загроз охоплює види інформації, що має негативний (шкідливий, небезпечний) характер. Їхня ідентифікація може бути здійснена за допомогою застосування двох основних методів: аналітичного та сутнісного. Аналітичний метод вимагає проведення аналізу норм міжнародного права, вітчизняного та зарубіжного законодавства, що закріплює види негативної інформації. Для цього використовується інструментарій порівняльно-правових досліджень. За відсутності у національному законодавстві певного виду негативного контенту, його правовий режим може бути регламентований на основі міжнародних стандартів або зарубіжного досвіду під час обліку внутрішньої специфіки.

Сутнісний метод означає виявлення та обґрунтування ознак шкідливості (небезпеки) повідомлень, за якими потім вибудовується список такого контенту. Доведення суспільної небезпеки таких повідомлень може здійснюватися на основі наукового аналізу та реальних наслідків впливу таких повідомлень на особистість чи соціальну групу. За результатами проведеної оцінки визначається оптимальний правовий режим для обороту певного контенту, наприклад, його повна заборона або введення часткових обмежень.

У міжнародно-правових актах міститься велика кількість видів негативної інформації, для яких встановлено заборону обороту або накладені правові обмеження. Коротко викладено результати проведеного нами аналізу релевантних норм міжнародних актів у табличній формі (таблиця 2.2.)

Набагато більший перелік видів негативної інформації закріплений у законодавстві розвинених країн. Проте базовий набір таких видів переважно

залишається уніфікованим через імплементацію положень розглянутих вище міжнародних договорів та інших джерел міжнародного права.

Важливо, що у західних країнах застосовується підхід розмежування негативної інформації на дві основні категорії з різним правовим режимом обігу. Першу категорію складає *незаконний контент* (illegal content), обіг якого перебуває під забороною та кваліфікується як правопорушення (найчастіше як злочин). Цей підхід застосовується Міжнародною асоціацією «гарячих інтернет-ліній» INHOPE, яка реагує на кримінальний контент [152].

Друга категорія представлена *шкідливим контентом* (harmful content), під яким розуміють суспільно небезпечні відомості, які не заборонені законом до обігу. Для таких відомостей встановлюються окремі обмеження з їхньої виробництво і поширення.

Проте ідентифікації контенту як незаконного чи шкідливого є суверенним правом держави, яка самостійно приймає рішення з урахуванням конституційно закріплених принципів та цінностей, культурних та історичних традицій.

Основні контентні загрози ІПБ:

1) інформація, що пропагує або виправдовує війну та інші міжнародні злочини, тероризм;

2) інформація, що розпалює ненависть та ворожнечу в соціумі;

3) інформація, пов'язана з фальсифікацією історії чи спотворенням історичної пам'яті;

4) інформація, що стимулює або сприяє скоєнню злочинів чи інших суспільно небезпечних дій;

5) хибна чи спотворена інформація;

6) інформація, яка принижує (порочить) честь, гідність або репутацію особи або яка ображає суспільну моральність;

7) порнографічний та інший сексуально відвертий контент;

8) інформація, яка провокує почуття жаху.

Кожна з названих загроз має специфічний механізм деструктивного ІПВ на людину та соціальні групи. Найбільш вивченим є механізм впливу медіа-

насильства. Останнім часом різко актуалізувалася проблема хибної інформації (фейків), хоча вона має давню історію.

З точки зору сутнісного методу можна виділити основні критерії шкідливості контенту:

1) здатність вводити в оману;

2) здатність провокувати скоєння протиправних чи соціально-небезпечних дій, у тому числі деструктивного плану;

3) здатність викликати страх, надавати інший негативний вплив на психологічний стан особистості та завдавати шкоди психічному здоров'ю;

4) здатність ганьбити честь, гідність та ділову репутацію;

5) здатність надавати негативний вплив на індивідуальну та суспільну мораль, інші елементи ціннісно-нормативної системи;

6) здатність спотворювати історичну пам'ять.

Група комунікаційних загроз охоплює негативне ІПВ у ході контакту для людей. На відміну від попередньої групи, для якої основним джерелом загроз є мас-медіа, комунікаційні загрози виходять із міжособистісної та групової комунікації. Вона може включати в себе безпосередні форми «живого спілкування» (розмова, участь у концерті, демонстрації) чи опосередковані застосуванням технічних засобів (розмова по телефону, листування в інтернет-чаті, спілкування в режимі відеодзвінка або відеоконференції тощо). Більшість комунікаційних загроз мають вербальний характер, проте є й невербальні форми. При цьому ми виходимо з того, що «функцію впливу реалізує будь-яке висловлювання, до якої б сфери комунікативної практики воно не ставилось» [49]. Запропоновані нами методи дослідження контентних загроз є цілком застосовними і для групи, що розглядається.

Правова регламентація комунікаційних загроз ІПБ може здійснюватися двома основними способами: 1) у вигляді визначення виду негативного ІПВ, який може здійснюватися як через поширення контенту, і через спілкування; 2) за допомогою визначення конкретного типу деструктивної комунікації.

У розглянутих вище міжнародно-правових актах переважно

використовується перший спосіб (це відноситься до повідомлень, що виправдовують національну, расову чи релігійну ненависті, мотивовану загрозою расизму та ксенофобії, публічному підбурюванню до вчинення терористичного злочину, наклепницьким твердженням тощо). Разом з тим самим зустрічаються юридично закріплені форми деструктивної комунікації: а) приставання до дітей із сексуальними цілями (ст. 23 Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуальних зловживань від 25 жовтня 2007 року); б) вербування терористів (ст. 6 Конвенції Ради Європи про запобігання тероризму від 16 травня 2005 року); в) мотивована загроза расизму та ксенофобії (ст. 4 Додаткового протоколу до Конвенції про кіберзлочинність щодо криміналізації діянь расистського та ксенофобського характеру, що здійснюються за допомогою комп'ютерних систем, від 28 січня 2003 року) тощо [151].

Підсумовуючи проведений аналіз, до основних комунікаційних загроз ІПБ автор відносить:

1) обман (дезінформацію); 2) маніпуляцію свідомістю; 3) комунікацію, що розпалює ненависть чи ворожнечу; 4) суспільні заклики та інші форми підбурювання до здійснення протиправних та інших суспільно небезпечних дій; 5) вербування та інші форми залучення у вчинення протиправних та інших суспільно небезпечних процесів; 6) образу та інші форми приниження людської гідності; 7) залякування та примус; 8) негативну сексуальну комунікацію; 9) комунікацію, пов'язану з фальсифікацією історії чи спотворення історичної пам'яті.

Критерії шкідливості комунікативних загроз ІПЛ повністю збігаються з виділеними критеріями для контентних загроз. Однак, враховуючи наявність загроз залякування та примусу, ми виділимо ще один критерій – здатність змушувати особу чи соціальну групу діяти всупереч своїй волі.

При виробленні стратегії протидії контентним та комунікаційним загрозам ІПБ, у тому числі при доборі належного правового інструментарію для реагування, потрібне їх певне ранжування. В основі цієї процедури лежить

проста і очевидна думка про те, що рівень загроз ІПБ відрізняється, причому досить значно.

В інформаційному праві оцінка суспільної небезпеки загроз ІПБ також використовується як у нормотворчій, так і у правозастосовчій практиці. Однак на відміну від кримінального та адміністративно-деліктного права, де предметом оцінки виступає небезпека діяння, що з поширенням певної інформації чи веденням комунікації, для інформаційного права таким переважно є сам контент/комунікація, поза прив'язки до конкретної особи. Хоча оцінка його впливу і включає реконструкцію деяких характеристик автора, таких як мета створення, комунікативний намір тощо.

В галузі управління ризиками оцінка ризику будується на основі двох базових факторів – наслідків ризику та ймовірності їх настання. Вони оцінюються на стадії аналізу ризику, яка передбачає якісний та кількісний аналіз чи його комбінацію. У науковій літературі щодо оцінки ризиків інформаційної безпеки на підприємствах, в алгоритм такої оцінки включена стадія «визначення цінності активу». Цінність активу (об'єкта, що охороняється) можна вважати третім фактором для оцінки ризику. Спробуємо застосувати цю концепцію щодо сфери ІПБ. Критерій «наслідки ризику» означатиме негативні наслідки для особи, суспільства або держави, що настають внаслідок надання ІПВ. Вони можуть мати особистий (формування страхів, прийняття помилкового рішення), економічний (втрата майна, втрачена вигода), соціальний (зростання рівня агресивності в суспільстві) тощо.

Імовірність настання наслідків визначається, по-перше, ймовірністю зіткнення з загрозою ІПБ, по-друге, ймовірністю її шкідливого впливу на особистість/групу. Перший аспект цілком прораховується, наприклад, на основі вивчення показників медіа-споживання, аналізу статистики роботи гарячих інтернет-ліній та ліній допомоги. З другим все набагато складніше в силу описаних нами особливостей механізму ІПВ. Тому для їх оцінки застосовні методи експертних оцінок та вивчення конкретних випадків (case study).

Щодо цінності об'єктів ІПБ, то визначити її дуже складно, оскільки

йдеться не про матеріальні об'єкти, а про людей. Проте є консенсус щодо визнання дітей пріоритетним об'єктом правового захисту. Такі критерії повинні бути покладені в основу методології оцінки та ранжування загроз ІПБ під час вибору механізму реагування на загрози інформаційній безпеці та протидії їм. У практиці ж оперативного управління насамперед слід орієнтуватися на найбільш рухливі критерії – частоту прояву загроз та кількість зареєстрованих випадків настання негативних наслідків

Зазначимо ще один важливий момент. Конкретний різновид загроз ІПБ, позначається відповідним лінгвістичним маркером («хибні відомості», «жахлива інформація» і т.п.), може включати широкий спектр проявів, що відрізняються за рівнем небезпеки. Пояснимо це на прикладі контенту, що містить сцени насильства. По-перше, небезпека залежатиме від характеру самого зображення (опису) насильства, а саме: ступеня натуралістичності, рівня жорстокості, суб'єкта та об'єкта насильства, тривалості показу (опису); по-друге, від сюжетного контексту: характеру насильника (герой/лиходій/жертва), виправданості насильства, наслідків для персонажа та жертви, оцінок з боку інших учасників.

Пропонуємо такий опис актуальних загроз інформаційно-психологічній безпеці людини, сус

пільству та державі в Україні.

Таблиця 2.3. Опис загроз ІПБ

№ п/п	**Опис загроз інформаційно-психологічній безпеці**
	У сфері інформаційної безпеки
1.	Розширення використання інформаційно-комунікаційних технологій для втручання у внутрішні справи держав, підриву їх суверенітету та порушення територіальної цілісності, що становить загрозу міжнародному миру та національній безпеці.
2.	Активізація діяльності спеціальних служб іноземних держав щодо проведення розвідувальних та інших операцій в українському інформаційному просторі

3.	Поширення недостовірної, фейкової інформації, хибних повідомлень з метою дестабілізації суспільно-політичної ситуації в Україні
4.	Розміщення в мережі Інтернет матеріалів терористичних/екстремістських/ організацій, здійснення сепаратиської діяльності, пропаганда кримінального способу життя, споживання наркотичних засобів та психотропних речовин.
5.	Прагнення до монополізації діяльності в мережі Інтернет та контролю над усіма інформаційними ресурсами, запровадження цензури та блокування альтернативних інтернет-платформ
6.	Нав'язування користувачам мережі Інтернет спотвореного погляду на історичні факти, а також на події, що відбуваються в Україні та світі
7.	Низький рівень інформаційно-психологічної стійкості та медіаграмотності громадян, незабезпечення особистої інформаційної безпеки
	У сфері державної та громадської безпеки
8.	Зростання числа злочинів, скоєних з використанням ІКТ
9.	Екстремістські прояви, що надають дестабілізуючий вплив на суспільно-політичну обстановку
10.	Спроби деструктивних сил за кордоном та всередині країни використовувати об'єктивні соціально-економічні проблеми у цілях порушення соціальної стабільності та внутрішньополітичної безпеки країни, стимулювання міжнаціональних та міжконфесійних конфліктів, маніпулювання масовою свідомістю громадян.
11.	Розвідувальна та інша діяльність спеціальних служб та організацій іноземних держав в інформаційному просторі України
12.	Прагнення міжнародних терористичних та екстремістських організацій посилити пропагандистську роботу з вербування українських громадян, та залучення їх до протиправної діяльності проти національної безпеки України
13.	Зростання масштабів комп'ютерної злочинності, насамперед у кредитно-фінансовій сфері
14.	Масштабне використання мережі Інтернет для пропагування незаконного споживання наркотичних засобів
15.	Широке використання терористичними та екстремістськими організаціями механізмів інформаційного впливу на індивідуальну, групову та суспільну свідомість з метою нагнітання міжнаціональної та соціальної напруженості, розпалювання етнічної та релігійної ненависті або ворожнечі, пропаганди екстремістської ідеології, а також залучення до терористичної діяльності громадян України

16.	Діяльність, спрямована на насильницьку зміну конституційного ладу України, дестабілізацію внутрішньополітичної та соціальної ситуації в країні, дезорганізацію функціонування органів державної влади, важливих державних, військових об'єктів та інформаційної інфраструктури України
17.	Екстремістська діяльність націоналістичних, релігійних, етнічних та інших організацій та структур, спрямована на порушення єдності та територіальної цілісності України, дестабілізацію внутрішньополітичної та соціальної ситуації в країні
18.	Порушення ненависті або ворожнечі за ознаками статі, расової, національної, мовної, релігійної приналежності або приналежності до будь-якої соціальної групи, у тому числі шляхом поширення закликів до насильницьких дій, насамперед через інформаційно-телекомунікаційні мережі, включаючи мережу Інтернет
19.	Використання релігії та релігійних організацій як інструментів дестабілізації суспільно-політичної ситуації в країні та розпалювання та загострення міжконфесійних та міжетнічних конфліктів

Висновки до другого розділу

1. Аналіз стану захищеності інформаційно-психологічного простору України свідчить, що інформаційно-психологічна безпека України не виділена як одна з визначальних у спектрі безпекових складових. Політико-правові механізми державного управління нею чітко не визначені, фрагментовані та неузгоджені, а передовий іноземний досвід не запроваджується. За роки незалежності України так і не було прийнято Закон України «Про інформаційно-психологічну безпеку», де було б чітко визначено суб'єктів державної політики національної безпеки у даній сфері діяльності та політико-правові механізми її реалізації. Запропоновано авторське визначення понять : «політико-правовий механізм», «правове забезпечення ІПБ».

2. Для України як де ржави, що зіткнулася із проблемами втягнення в гібридну війну та наявністю тимчасово окупованих територій , досвід країн ЄС щодо гарантування інформаційної безпеки є доцільним для розгляду . Зокрема приклад Хорватії , протидія сепаратизму в якій закінч илася успішною реінтеграцією самопроголошеної «республіки». Відповідно, варто використовувати передові методи протидії російській інформаційній агресії , постійно представляти якісний інформаційний продукт на тимчасово

окупованих територіях. Доцільним буде також наслідувати досвід Німеччини в переході до принципу «активної оборони» щодо інформаційної безпеки. Постійна діяльність компетентних органів, спрямована на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу може надати значні переваги в умовах гібридної війни з рф.

Проаналізовано міжнародно-правові стандарти у сфері інформаційно-психологічної безпеки та складена таблиця видів негативного контенту в міжнародно-правових актах.

3. Проведений аналіз дозволяє стверджувати, що інформаційний складник «гібридної війни» рф проти України об'єктивно є одним із значних чинників її ведення, а масштаби застосування інформаційних маніпуляцій, пропаганди, дезінформації набирають різноманітних форм та особливостей. Державне управління інформаційною безпекою в умовах гібридної війни повинно передбачати здійснення управлінського впливу в декілька етапів в які входять: формування системи забезпечення інформаційної безпеки; виявлення викликів та загроз інформаційній безпеці; оцінка стану та можливостей системи забезпечення інформаційної безпеки; розробка та впровадження інструментарію державного реагування на загрози інформаційній безпеці; моніторинг, спостереження та контроль за забезпечення інформаційної безпеки.

В розділі в рамках визначення інформаційно-психологічних загроз як головних факторів розгортання «гібридної війни» викладена авторська класифікація видів загроз ІПБ та їх поділ на контентні та комунікаційні загрози. Складена матриця актуальних загроз ІПБ, а також з урахуванням результатів власного наукового дослідження, представимо авторську класифікацію основних загроз ІПБ.

4. Основні наукові результати розділу опубліковані в праці [47;49].

РОЗДІЛ 3. Шляхи вдосконалення публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки в Україні

3.1. Пріоритетні напрями вдосконалення державної політики інформаційної безпеки в умовах протидії гуманітарної експансії рф проти України

Експонентний розвиток інформаційно-комунікаційних технологій та процесів цифрової трансформації у світі ставить завдання модернізації системи правового регулювання суспільних відносин у різних сферах життя. Це особливо актуально стосовно нових викликів цифрового середовища, кількість та небезпека яких стрімко збільшуються. З початку нового тисячоліття процес нормативного регулювання інформаційної безпеки значно активізувався, особливо у зв'язку з прийняттям у 2000 році Окінавської хартії глобального інформаційного суспільства та першої Доктрини інформаційної безпеки України в 2007 році. За минулий після цього період час було проведено значну роботу, спрямовану на розвиток правового забезпечення інформаційної безпеки. Цей висновок стосується і сфери забезпечення інформаційно-психологічної безпеки, де за останні двадцять років правове регулювання набуло потужного розвитку. Причому, останніми роками дана сфера законодавства є однією з найбільш динамічних в світі. Водночас фрагментарні зміни, що вносяться до інформаційного та іншого галузевого законодавства, часто викликані поточними проблемами, позбавлені системності та опори на наукову основу.

Для українського суспільства питання державного управління забезпеченням інформаційної безпеки постають особливо гостро, через бойові дії на сході держави та агресією з боку російської федерації, ведення останньою інформаційної та смислової війни проти України. З початку 2014 року з боку росії здійснювався надпотужний інформаційно-психологічний тиск на населення України, нарощувалася інформаційна експансія в національний інформаційний простір, захоплювались стратегічні об’єкти української

телекомунікаційної інфраструктури. Зазначена складна ситуація стала можливою, насамперед, через відсутність узгодженої, послідовної та зваженої державної політики у сфері інформаційної безпеки України, низьку ефективність системи державного управління забезпеченням інформаційної безпеки, а також недосконаліть та фрагментарність вітчизняного нормативно-правового поля у сфері інформаційної безпеки [64].

Ми візьмемо за основу концептуальний підхід до вирішення правових проблем забезпечення інформаційної безпеки, що передбачає вивчення правових засобів забезпечення інформаційної безпеки у нерозривному зв'язку з цілями, завданнями та механізмами реалізації державної політики щодо забезпечення інформаційної безпеки.

Поняття «забезпечення безпеки» належить до базових категорій у теорії безпеки та імплементований в нормативно-правових актах України зі сфери національної безпеки [102;103]. Термін «забезпечення», що лежить в його основі, орієнтує на активну діяльність певних суб'єктів, спрямовану на досягнення стану захищеності об'єктів безпеки. До такої діяльності виступає реалізація уповноваженими суб'єктами політичних, правових, військових, соціально-економічних, інформаційних, організаційних та інших заходів, спрямованих на протидію загрозам національній безпеці. Тому під забезпеченням ІПБ ми будемо розуміти *діяльність державних та недержавних інститутів щодо вироблення та реалізації системи правових, організаційних, інформаційних та інших заходів, спрямованих на забезпечення захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу*. При цьому, ми будемо відштовхуватися від розширювального тлумачення поняття «стан захищеності» і поряд із протидією інформаційним загрозам у зміст забезпечення ІПБ включимо заходи щодо підвищення стійкості людини, соціальних груп та суспільства до впливу таких загроз. Останній напрямок має важливе значення через неможливість повного захисту соціальних суб'єктів від негативного психологічного впливу та недостатньої ефективності систем фільтрації інформації.

Ще один змістовний блок забезпечення ІПБ складають заходи щодо впливу на інформаційне середовище, в якому здійснюється деструктивне ІПВ на особистість та соціальні групи. Активізуючи позитивні фактори та нейтралізуючи негативні елементи цифрового середовища, можна підвищувати рівень захищеності об'єктів. Звісно ж, що цей напрямок якраз укладається в концепцію «інформаційної гігієни», що передбачає створення певного стану інформаційного середовища, безпечного для фізичного та психічного здоров'я людини, а також індивідуальної, групової та суспільної психології.

Таким чином, діяльність із забезпечення ІПБ включає чотири основні елементи: 1) протидія джерелам загроз ІПБ; 2) виключення чи зменшення деструктивного впливу загроз на об'єкти ІПБ; 3) збільшення стійкості об'єктів деструктивного ІПВ; 4) надання впливу на елементи цифрового середовища.

Можна класифікувати *заходи із забезпечення ІПБ* на такі основні групи: 1) регулювання, зокрема, обмеження інформаційних потоків; 2) організація інформаційних потоків (ініціювання поширення певної інформації); 3) поширення способів та засобів обробки та оцінки інформації; 4) формування групового та індивідуального психологічного захисту.

Найважливішу роль у механізмі забезпечення ІПБ відіграє правове забезпечення, оскільки безпосередньо право встановлює цілі, завдання та напрямки такого забезпечення, а також регламентує форми, засоби та методи діяльності уповноважених суб'єктів протидії загрозам ІПБ.

У вітчизняній науці інформаційного права сформувався підхід до розуміння правового забезпечення інформаційної безпеки насамперед як правового регулювання. Правове регулювання відносин у сфері забезпечення інформаційної безпеки передбачає встановлення певних правових норм, їх застосування та охорону від порушення з використанням державного примусу. Тобто правове забезпечення інформаційної безпеки крім правового регулювання відносин включає і правозастосовну діяльність.

Загальноприйнятим є таке визначення: *правове забезпечення національної безпеки* - це взаємопов'язана та впорядкована сукупність нормативних правових

актів, які закріплюють юридичні принципи та норми правового регулювання суспільних відносин у галузі забезпечення національної безпеки [7]. Таке визначення, на нашу думку, не є цілком правильним. По-перше, правове забезпечення, як і будь-яке забезпечення, є певною діяльністю на основі реалізації системи заходів. По-друге, неправильно зводити всю систему правових засобів лише до нормативно-правових актів. Правове забезпечення включає у собі як правове регулювання, так й елементи правового впливу. До останніх відноситься правосвідомість, правова культура, правові принципи. Ми вважаємо, що правове забезпечення національної безпеки включає у собі крім нормотворчості і правозастосування ще й інші форми реалізації права. А їх, як відомо, всього чотири: дотримання, виконання, використання, застосування. Тому автор вважає за доцільне визначення правового забезпечення ІПБ через поняття «правових засобів», що лежать в основі механізму правового регулювання. З урахуванням викладеного пропонуємо розглядати *правове забезпечення інформаційно-психологічної безпеки як діяльність з розробки та реалізації системи правових засобів, спрямованих на забезпечення захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу.*

У науці та документах стратегічного планування в сфері національної безпеки перед постановкою цілей та завдань забезпечення безпеки прийнято визначати національні інтереси. У Законі України «Про національну безпеку» 2018 року вони визначені як «життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян» [98]. Стосовно інформаційної сфери, національні інтереси визначені в чинній Доктрині інформаційної безпеки 2017 року як життєво важливі інтереси людини (захищеність від руйнівних інформаційно-психологічних впливів тощо); суспільства та держави (захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку російської федерації тощо).

З урахуванням проведеного аналізу вітчизняних нормативно-правових документів зі сфери інформаційної безпеки вважаємо за можливе сформулювати авторський перелік *національних інтересів України в інформаційній сфері*, що стосуються забезпечення ІПБ:

1) забезпечення та захист конституційних прав і свобод людини та громадянина, включаючи право на свободу, недоторканність приватного життя, захист своєї честі та доброго імені, свободу думки та слова, право на інформацію та свободу масової інформації;

2) формування середовища довіри у цифровому середовищі;

3) забезпечення доступу до інформації, що сприяє розвитку особистості та суспільства;

4) захист особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу;

5) гарантування психічного здоров'я та благополуччя громадян;

6) розвиток національної ідентичності українського суспільства, підвищення культурного потенціалу країни;

7) зміцнення національної згоди, політичної та соціальної стабільності;

8) забезпечення інформаційного суверенітету України;

9) формування позитивного іміджу України, її державної суб’єктності та авторитету на міжнародній арені, посилення політичного та культурного впливу України у світі;

10) сприяння формуванню системи міжнародної інформаційної безпеки, спрямованої на протидію загрозам деструктивного ІПВ на особистість, соціальні групи та суспільство.

Далі необхідно визначити мету, завдання та напрями забезпечення ІПБ.

На думку автора, стратегічною метою забезпечення ІПБ виступає підтримка стану захищеності особистості, соціальних груп та суспільства в цілому від деструктивного інформаційно-психологічного впливу, що забезпечує гарантовану реалізацію національних інтересів України.

На наступному рівні визначення мети необхідно дати характеристику

завдань і функцій (напрямів) забезпечення ІПБ. У Доктрині ІБ 2017 року завдання забезпечення інформаційної безпеки не виділено, а його основні напрямки визначено лише стосовно окремих сфер державного управління. Позитивно відрізняється у цьому плані Стратегія ІБ 2021 року. У ній чітко окреслено основні напрями забезпечення інформаційної безпеки України - стійкість та взаємодія, які описані у 7 стратегічних цілях Стратегії [103] .

Їхній аналіз дозволяє виділити такі *додаткові завдання забезпечення ІПБ:*

1) підтримання морально-політичного та психологічного стану особового складу Збройних сил та інших військових формувань, військово-патріотичне виховання; 2) недопущення втручання у внутрішні справи України, припинення розвідувальної та іншої діяльності іноземних держав та окремих осіб проти національних інтересів України; 3) профілактика радикалізму, екстремізму, пропаганди насильства та нетерпимості, міжнаціональної ворожнечі; 4) попередження та нейтралізація соціальних, міжконфесійних та міжнаціональних конфліктів, сепаратизму, деструктивних релігійних течій; 5) захист історичної правди, збереження історичної пам'яті, протидія фальшування історії; 6) реалізація державної інформаційної політики щодо зміцнення сприйняття суспільством культурно-історичних цінностей, неприйняття громадянами нав'язуваних ззовні деструктивних ідей, стереотипів та моделей поведінки; 7) зміцнення культурного суверенітету України та збереження її єдиного культурного простору, захист суспільства від зовнішньої ідейно-ціннісної експансії та зовнішнього деструктивного інформаційно-психологічного впливу; 8) духовно-моральне та патріотичне виховання громадян; 9) зміцнення позиції українських ЗМІ у глобальному інформаційному просторі.

Представимо авторське бачення *завдань та функцій забезпечення ІПБ.* Перші розглядаються як приватні цілі (підцілі), які потрібно вирішити, щоб досягти основної мети у заданих умовах.

При визначенні завдань забезпечення ІПБ важливо уникати низки методологічних помилок, властивих законодавчим актам та документам

стратегічного планування у сфері національної безпеки. Вони полягають у змішуванні основних та допоміжних, загальних та часткових завдань забезпечення національної безпеки. Пропонується розглядати як основні завдання забезпечення безпеки - виявлення загроз безпеки та протидію їм, а до допоміжних завдань віднести управління процесом забезпечення безпеки; підбір, підготовку та розстановку сил та засобів забезпечення безпеки; матеріально-технічне та фінансове забезпечення діяльності із забезпечення національної безпеки.

При визначенні завдань ІПБ необхідно враховувати таке:

- по-перше, підтримуючи розмежування основних та допоміжних завдань забезпечення національної безпеки, все ж таки вважаємо за доцільне їх виклад у єдиному переліку;

- по-друге, сам термін «допоміжні завдання» видається не зовсім вдалим, оскільки вирішення багатьох з них (постановка цілей, правове регулювання, визначення сил та засобів) передує діяльності з безпосереднього забезпечення національної безпеки;

- по-третє, вважаємо за необхідне трактувати протидію загрозам з урахуванням підходів, що застосовуються в чинному українському законодавстві, як діяльність, що включає три компоненти: профілактику загроз; боротьбу із загрозами (виявлення, попередження, припинення, правове переслідування); мінімізацію та (або) ліквідацію наслідків впливу загроз;

- по-четверте, пропонуємо розширити кількість основних завдань забезпечення безпеки стосовно сфери ІПБ, доповнивши їх підвищенням життєстійкості об'єктів ІПБ.

Узагальнюючи вищевикладене, до завдань забезпечення ІПБ слід зарахувати:

1) прогнозування, виявлення, аналіз та оцінку загроз ІПБ;

2) аналіз та оцінку вразливості особистості, соціальних груп та суспільства від деструктивного ІПВ;

3) стратегічне планування у сфері забезпечення ІПБ;

4) правове регулювання у сфері забезпечення ІПБ;

5) застосування комплексу оперативних та довготривалих заходів щодо профілактики, попередження, припинення та усунення загроз ІПБ, мінімізації та (або) ліквідації наслідків їх впливу;

6) застосування комплексу оперативних та довготривалих заходів щодо підвищенню здатності особистості, соціальних груп та суспільства протистояти деструктивному ІПВ;

7) організацію діяльності системи забезпечення ІПБ;

8) кадрове, інформаційне, матеріально-технічне та фінансове забезпечення діяльності суб'єктів забезпечення ІПБ;

9) міжнародне співробітництво у сфері забезпечення ІПБ.

Далі розглянемо функції (напрями) забезпечення ІПБ. Так, в умовах розвитку глобального інформаційного суспільства значущою теоретичною проблемою інформаційного права стає відокремлення функцій держави з забезпечення інформаційної безпеки. Виділення напрямів забезпечення ІПБ важливо не тільки для чіткого визначення предметного змісту діяльності уповноважених суб'єктів, а й для визначення основних векторів формування та розвитку українського законодавства у цій сфері.

В теорії управління, функції розглядаються як напрями (види) управлінської діяльності, які забезпечують досягнення цілей управління та здійснюються спеціальними прийомами і методами. Функція управління є стійкою сукупністю завдань (операцій, дій) щодо реалізації процесу управління (його частини) задля досягнення цілей управління, що заснована на поділі управлінської праці в органах управління. Виходячи з цього трактування, в теорії управління, починаючи з класика А. Файоля, прийнято виділяти такі функції управління, як планування, організація, координація, контроль [81].

Однак стосовно сфери безпеки таке трактування функцій не підходить, оскільки вона позначає стадії управлінського процесу, а не орієнтує на напрямки діяльності суб'єктів забезпечення безпеки. Вийти із цієї ситуації нам допоможе класифікація функцій управління на два класи: функції-операції, що

є функціями процесу управління та функції-завдання, що виступають функціями системи управління. Саме про останніх, на наш погляд, має йтися стосовно питань забезпечення безпеки.

З урахуванням проведеного нами аналізу нормативно-правових актів України, документів стратегічного планування в сфері національної та інформаційної безпеки, а також профільної наукової літератури пропонуємо *авторську концепцію основних напрямів (функцій) забезпечення ІПБ.*

На думку автора, при виділенні напрямів забезпечення безпеки недоцільно змішувати діяльність у рамках вирішення основних та допоміжних завдань. Для визначення основних завдань напрями діяльності державних органів відштовхуються від загроз безпеки та сфер їхнього прояву (наприклад, протидія пропаганді тероризму чи діяльності іноземних спецслужб щодо надання деструктивного ІПВ). При цьому в рамках кожного з таких напрямів діяльності необхідне вирішення однотипних забезпечувальних завдань у рамках вироблення та реалізації державної політики забезпечення ІПБ (стратегічне планування, правове регулювання, матеріально-технічне забезпечення, підготовка кадрів).

Тому ми викладемо два переліки: основних напрямів забезпечення ІПБ та основних напрямів діяльності з вироблення та реалізації державної політики забезпечення ІПБ.

Основні напрямки забезпечення ІПБ:

1) прогнозування, виявлення, аналіз та оцінка загроз ІПБ;

2) протидія поширенню негативної інформації у засобах масової інформації та мережі Інтернет;

3) протидія терористичній та екстремістській пропаганді та вербувальній діяльності, розпалюванню національної, расової, релігійної чи соціальної ненависті та ворожнечі;

4) протидія деструктивному ІПВ з боку державних органів та спеціальних служб іноземних держав, іноземних та міжнародних організацій;

5) забезпечення інформаційно-психологічної безпеки дітей;

6) захист честі, гідності та ділової репутації громадянина, ділової репутації юридичної особи;

7) захист органів громадської влади, посадових осіб від деструктивного ІПВ;

8) протидія фальсифікації вітчизняної та світової історії на шкоду інтересам України;

9) протидія поширенню деструктивних субкультур та інших форм негативного ІПВ у духовній сфері;

10) протидія злочинам та адміністративним правопорушення, пов'язаним з наданням деструктивного ІПВ;

11) інформування української та зарубіжної громадськості про внутрішню і зовнішню політику України, її офіційну позицію щодо соціально значущих подій в Україні та міжнародного життя, в тому числі подій російсько-української війни;

12) ведення контрпропаганди;

13) формування цифрової грамотності громадян та культури інформаційної безпеки.

Основні напрямки діяльності з вироблення та реалізації державної політики забезпечення ІПБ:

1) стратегічне планування у сфері забезпечення ІПБ;

2) правове регулювання у сфері забезпечення ІПБ;

3) здійснення державного контролю (нагляду) у сфері забезпечення ІПБ;

4) надання державних послуг у сфері забезпечення ІПБ;

5) координація діяльності суб'єктів забезпечення ІПБ;

6) організація матеріально-технічного, фінансового та інформаційного забезпечення діяльності суб'єктів забезпечення ІПБ;

7) проведення наукових досліджень щодо забезпечення ІПБ;

8) підготовка кадрів у сфері забезпечення ІПБ;

9) здійснення міжнародного співробітництва у сфері ІПБ.

Разом з тим, останніми роками в документах стратегічного планування

став застосовуватися дещо інший підхід до визначення системи забезпечення безпеки, що виділяє такі її елементи, як сили та засоби забезпечення національної безпеки. Він знайшов відображення у Стратегії НБ 2021 року та Законі України «Про національну безпеку» 2018 року. Згідно з останньою, під силами безпеки та оборони розуміють - «сили безпеки - правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту та інші органи, на які Конституцією та Законами України покладено функції із забезпечення національної безпеки України; «сили оборони - Збройні Сили України, а також інші утворені відповідно до законів України військові формування, правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави»[98;103];

Автор загалом поділяє офіційний підхід, проте виступає проти виділення інструментального елемента замість нормативного, оскільки це суперечить значущості правової регламентації суспільних відносин у сфері безпеки. Тому в подальшому нашому розгляді ми виходитимемо із триєдиної структури системи забезпечення ІПБ, що включає: (1) сили, (2) засоби та методи, (3) правове регулювання. З урахуванням викладеного *систему правового забезпечення інформаційно-психологічної безпеки можна визначити як впорядкований комплекс правових засобів, що використовуються для підтримки стану захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу.*

Для того, щоб оптимізувати публічне управління забезпеченням інформаційної безпеки в Україні, суб’єктами державної політики у сфері інформаційної безпеки України мають бути здійснені важливі кроки в таких напрямках:

– інтеграція України до інформаційного простору на світовому та регіональному європейському рівні;

– інтеграція України до міжнародних інформаційних та інформаційно-

телекомунікаційних систем та організацій;

– розвиток національного інформаційного простору та забезпечення розвитку інформаційного суспільства;

– модернізація системи інформаційного захисту країни, формування й реалізація ефективної інформаційної політики держави;

– удосконалення законодавства щодо інформаційної безпеки, узгодження національного законодавства з рядом відповідних міжнародних стандартів;

– ефективне регулювання інформаційних процесів в правовій площині;

– розвиток національної інформаційної інфраструктури;

– підвищення конкурентоспроможності вітчизняного інформаційного продукту та послуг інформаційного характеру;

– впровадження сучасних інформаційно-комунікативних технологій у процес державного управління;

– налагодження ефективної взаємодії між ОДВ та інститутами громадянського суспільства під час здійснення політики забезпечення інформаційної безпеки.

Відповідно, рекомендаціями, щодо оптимізації державного управління забезпеченням інформаційної безпеки в Україні є:

1. Аналіз та аудит існуючих проблем для виявлення специфічних сегментів, що вимагають реформування у сфері інформаційної безпеки. Провести комплексні аудити (правовий, технічний, комунікаційний та освітній) у сфері інформаційної безпеки у державних органах із залученням зацікавлених суб’єктів та відповідних інститутів громадянського суспільства.

2. Створення чіткої ієрархічної системи державних органів системи забезпечення інформаційної безпеки України. Визначення їх компетенцій, повноважень, функцій та методів координації.

4. Покращення якості підготовки кадрового складу системи публічного управління у сфері забезпечення інформаційної безпеки.

5. Модернізація технічного забезпечення органів державного управління інформаційною безпекою України.

6. Здійснення постійного моніторингу ефективності роботи системи забезпечення інформаційної безпеки.

7. Створення програм заохочення учених, фахівців, висококваліфікованих працівників у сфері інформаційної безпеки, щоб не допустити відтік кадрів за межі України.

8. Прискорення реформування національної медійної та комунікаційної систем , модернізація їх стандартів , створення продуктивної системи суспільного мовлення.

9. Розроблення механізмів приватного та державного партнерства у сфері забезпечення інформаційної безпеки.

10. Наукове, законодавче та науково-інтелектуальне забезпечення функціонування системи інформаційної безпеки.

Отже, державне управління в сфері забезпечення інформаційної безпеки полягає у створенні умов для гармонійного розвитку національної інформаційної інфраструктури , для реалізації конституційних прав і свобод людини та громадянина, законних інтересів особи, суспільства та держави у національному інформаційному просторі , у отриманні інформації та користування нею фізичними та юридичними особами з метою забезпечення непорушності конституційного ладу , суверенітету та територіальної цілісності України, політичної, економічної та соціальної стабільності , в забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

3.2. Рекомендації щодо удосконалення нормативно-правових механізмів державної політики у сфері інформаційної безпеки України

Слабкі та неефективні міжнародні та національні механізми правового захисту населення та держави від деструктивних інформаційно-психологічних операцій російській федерації сприяли тому, що агресор досягав переваг на

перших етапах російсько-української війни. Незважаючи на те, що наша держава вже восьмий рік протидіє російській агресії, українське суспільство так і залишається незахищеним від інформаційно-психологічних операцій рф.

Одним із недоліків протидії України в інформаційній війні з росією вважається слабке охоплення національним інформаційним продуктом закордонного інформаційного середовища та недостатнє поширення іноземного мовлення на території інших держав.

Для комплексного організаційно-правового реагування на загрози інформаційно-психологічній безпеці Україні необхідно *здійснити наступні заходи:*

– створити ефективну багаторівневу державну систему забезпечення інформаційної безпеки, у якій діятимуть єдині правові норми і механізми захисту інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури та інформаційних прав громадян, здійснюватиметься ефективна координація діяльності органів державної влади й управління.

– розробити механізм узгодження діяльності органів державної і місцевої влади у сфері забезпечення інформаційної безпеки;

– активізувати діяльність із формування державної політики в забезпеченні інформаційної безпеки регіонів;

– зміцнювати взаємодію недержавних структур із державними органами виконавчої влади при вирішенні питань забезпечення інформаційної безпеки.

Також, вважаємо за необхідне створити в Україні спеціальний Орган з питань ведення інформаційно-психологічної війни, який виконуватиме такі стратегічні завдання:

– виявлення ризиків і відстеження появи та розвитку загрозливих інформаційно-психологічних ситуацій;

– дослідження інформаційно-психологічної зброї, забезпечення здатності військ протистояти шкідливим інформаційно-психологічним впливам;

– захист військ і суспільства від деструктивної пропаганди іноземних суб’єктів;

– організація розвідувальної діяльності, використання тактик, пов’язаних із проникненням в органи влади та впливові структури інших держав з метою просування інтересів України;

– формування і захист позитивного образу нашої держави за допомогою інформаційних технологій, зокрема рекламної, просвітницької, пропагандистської діяльності, створення та підтримка національного бренду;

– міжнародне співробітництво у сфері протидії розвитку кіберзлочинності, пошук шляхів інформаційно-психологічного захисту держави та суспільства.

Для вдосконалення механізму державного реагування на загрози інформаційно-психологічної безпеки України необхідно визначитись з управлінською ланкою, яка зможе на основі одержаної інформації, з урахуванням наявних ресурсів, сил і засобів розробити альтернативні варіанти своєчасної та адекватної протидії загрозам і реагування на них.

Так, функціями Антикризового центру повинні стати: визначення проблемних галузей; збір і системний аналіз інформації у всіх сферах національної безпеки; моніторинг ескалації загроз; моделювання і прогнозування кризових явищ; визначення можливостей із запобігання ескалації кризових ситуацій і реагування на них.

Центр стратегічного та оперативного планування буде відповідальний за підготовку, розробку, експертизу фундаментальних і стратегічних документів, законодавчих і підзаконних актів, а також опрацювання оперативних питань, які виносяться на розгляд Президента, Верховної Ради України та Ради національної безпеки та оборони України – на запит Адміністрації Президента, секретаріатів ВРУ та РНБО.

Взаємодія Центру стратегічного та оперативного планування та Антикризового центру із силовими відомствами, іншими органами державної влади, науковими установами та експертами має забезпечити суцільний аналіз всіх загроз, раннє їх виявлення, відстеження, з метою запобігання їх ескалації і перетворенню на кризові ситуації.

Центр антикризового реагування забезпечує планування та координацію спільних дій з підготовки та застосування структур системи національної безпеки. У складі Центру створюються ситуативні групи, які спільно з силовими структурами проводять дії з врегулювання криз і ліквідації їхніх наслідків.

Отже, запропонована організаційна структура за умов якісного правового, фінансового, кадрового та інформаційного забезпечення дозволить домогтися високого рівня національної безпеки в Україні.

На нашу думку, така система дасть змогу своєчасно виявляти загрози інформаційно-психологічній безпеці, мобілізувати ресурси, сили та засоби для захисту державних інтересів, протидії агресії супротивника, оперативно реагувати на виявлені загрози.

В сучасних умовах державотворення України, значною теоретичною проблемою інформаційного права стає відокремлення функцій держави щодо забезпечення інформаційної безпеки. Виділення напрямів забезпечення ІПБ важливе не тільки для чіткого визначення предметного змісту діяльності уповноважених суб'єктів, а й визначення основних векторів формування та розвитку вітчизняного законодавства у цій сфері.

В теорії управління, функції розглядаються як напрями (види) управлінської діяльності, що забезпечують досягнення цілей управління та здійснюються спеціальними прийомами та способами [119]. Функція управління являє собою стійку сукупність завдань (операцій, дій) реалізації процесу управління (його частини) задля досягнення приватних цілей управління, засновану на розподілі управлінської праці в органах управління [122]. Виходячи з даного трактування, в теорії управління, починаючи з класика А. Файоля [165], прийнято виділяти такі функції управління, як планування, організація, координація, контроль. Однак стосовно сфери безпеки таке трактування функцій не підходить, тому що воно позначає стадії управлінського процесу, а не орієнтує на напрямки діяльності суб'єктів забезпечення безпеки. Вийти з цієї ситуації можна за допомогою класифікації

функцій управління на два класи: функції-операції, що є функціями процесу управління, та функції-завдання, виступаючі функціями системи управління [162]. Саме про останні, на наш погляд, має йтися стосовно забезпечення безпеки. Аналіз нормативно-правових механізмів публічного управління сферою інформаційної безпеки дає можливість запропонувати авторську концепцію основних напрямів (функцій) забезпечення ІПБ.

Так при виділенні напрямів забезпечення безпеки недоцільно змішувати діяльність у рамках рішення основних та забезпечувальних завдань. Для визначення основних завдань напряму діяльності державних органів відштовхуються від загроз безпеці та сфер їх прояву (наприклад, протидія пропаганді тероризму або діяльності іноземних спецслужб щодо здійснення деструктивного ІПВ). При цьому в рамках кожного з таких напрямів діяльності необхідне рішення однотипних забезпечувальних завдань у рамках вироблення та реалізації державної політики забезпечення ІПБ (стратегічне планування, правове регулювання, матеріально-технічне забезпечення, підготовка кадрів).

Пропонуємо два переліки: основних напрямів забезпечення ІПБ та основних напрямів діяльності з вироблення та реалізації державної політики забезпечення ІПБ.

Водночас останніми роками у документах стратегічного планування у сфері національної безпеки став застосовуватися дещо інший підхід до визначення системи забезпечення національної безпеки, що виділяє такі її елементи, як сили та засоби забезпечення національної безпеки. Він знайшов відображення у Законі «Про національну безпеку України» 2018 року, де дається визначення сил безпеки та сил оборони, Стратегії національної безпеки 2020 року. Узагальнюючи науковий та правовий аналіз цього питання можна зробити висновок, що під силами забезпечення інформаційної безпеки розуміються державні органи, а також підрозділи та посадові особи державних органів, органів місцевого самоврядування та організацій, уповноважені на виконання завдань із забезпечення інформаційної безпеки, а під засобами правові, організаційні, технічні та інші засоби, що використовують сили

забезпечення інформаційної безпеки.

Відповідно, виходячи з розгляду ІПБ як елемента ІБ, ми повинні зробити висновок про те, що система забезпечення ІПБ є частиною системи (підсистемою) забезпечення ІБ. Водночас цей тезі притаманна деяка частка умовності, оскільки виділення різних систем забезпечення окремих видів безпеки є більшою мірою розумовим конструктом, що «вписує» в неї певні державні органи та інші суб'єкти забезпечення безпеки. Насправді більшість з таких суб'єктів поліфункціональні, що обумовлює їх одночасне «членство» у багатьох системах забезпечення безпеки. Таким чином, система забезпечення ІПБ є підсистемою забезпечення ІБ, що включає сукупність сил забезпечення ІПБ, використовуваних ними засобів та методів, а також правового регулювання відносин у сфері забезпечення ІПБ. У її структурі нами виділяються інституційна (сили), інструментальна (засоби та методи) та нормативна (правове регулювання) підсистеми.

Нормативна підсистема – система правового забезпечення ІПБ – грає особливу роль, оскільки саме правовими нормами регламентується весь процес забезпечення безпеки, включаючи визначення його суб'єктів, їх завдань та функцій, що застосовуються ними, а також засобів та методів діяльності.

З урахуванням викладеного, *систему правового забезпечення інформаційно-психологічної безпеки можна визначити як впорядкований комплекс правових засобів, що використовуються для підтримки стану захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу.*

Сучасна система інформаційної безпеки України та її нормативно-правове забезпечення свідчить про те, що наразі функціонування комплексного механізму реалізації державної політики у сфері інформаційної безпеки здійснюється в рамках реактивного реагування на загрози інформаційного характеру. Це відповідає завданням лише поточної державної політики у згаданій сфері. В розрізі побудови системи захисту інформаційного простору України необхідно проаналізувати чинну Доктрину інформаційної безпеки

України (далі – Доктрина) на предмет завдань та можливостей їх реалізації [102].

На підставі аналізу результатів актуальних наукових досліджень можна зробити висновок про те, що розгляд проблем розробки та реалізації державної політики у сфері інформаційної безпеки України стали предметом досліджень вітчизняних науковців: Г.П. Ситника, О.Г. Осауленка, Р.Р. Марутян, В.І. Гурковського , Л.О. Євдоченко, З.В. Коваля, О.В. Власенка,
О.С. Зозулі, В.В. Антонюка, М.М. Шевченко та ін [5;40;56;67-71;118-119;138]. Незважаючи на значну кількість робіт, в яких розглядаються актуальні проблеми формування та реалізації державної політики у сфері інформаційної безпеки України в сучасних умовах гібридної війни маємо констатувати недостатню кількість наукових праць в яких би містилися конкретні рекомендації щодо удосконалення нормативно-правових механізмів формування та реалізації державної політики у сфері інформаційної безпеки України.

В Доктрині інформаційної безпеки України визначено національні інтереси України в інформаційній сфері, загрози інформаційній безпеці, напрями і пріоритети інформаційної політики Української держави. Правовою основою Доктрини є Конституція України, Закони України, а також міжнародні договори, згода на обов’язковість яких надана Верховною Радою України.

Вище зазначене дозволяє констатувати, що в Доктрині визначено засади формування лише поточної державної політики у сфері інформаційної безпеки, пріоритетом якої є реактивна протидія інформаційній агресії рф [102]. Тобто, в цьому документі розробники знехтували питанням розробки довгострокової державної політики у сфері інформаційної безпеки, пріоритетом якої мала бути проактивна та реактивна протидія широкому спектру загроз інформаційній безпеці. Водночас, у Стратегії інформаційної безпеки України [103] акцентується увага на протидії загрозам інформаційній безпеці, що надходять не лише від росії, а й інших суб’єктів інформаційно-психологічного протиборства.

Відповідно, з метою удосконалення механізму розробки державної політики у сфері інформаційної безпеки розробники чинної редакції Доктрини інформаційної безпеки України мають здійснити диференціацію державної політики у сфері інформаційної безпеки на довгострокову і поточну, із зазначення особливостей їхньої розробки та реалізації. Далі розглянемо питання удосконалення механізмів реалізації державної політики у сфері інформаційної безпеки України.

Для реалізації Доктрини РНБОУ здійснює координацію діяльності органів виконавчої влади щодо забезпечення інформаційної безпеки. Зважаючи на особливі умови і ведення росією проти Української держави інформаційної війни не лише на її території, але й у світі, забезпечення реалізації Доктрини можливе лише за умови належної координації заходів, які здійснюються усіма державними органами. РНБОУ також визначає ключові заходи, відповідно до положень нормативно-правової бази в галузі безпеки і оборони України.

З метою удосконалення комплексного механізму реалізації державної політики у сфері інформаційної безпеки України пропонуємо в нормативно-правових документах держави зі сфери інформаційної безпеки чітко виокремити контури управління інформаційною безпекою – *стратегічне, тактичне, оперативне управління*. Це дозволить здійснювати комплексну реалізацію довгострокової та поточної державної політики у сфері інформаційної безпеки України. Водночас, необхідно суб'єктам забезпечення інформаційної безпеки визначити завдання щодо прогнозування майбутнього характеру загроз інформаційній безпеці, що дозволяє окреслити вимоги до реформування вітчизняної системи забезпечення інформаційної безпеки в контексті еволюції інформаційної війни.

Враховуючи те, що інформаційна війна ведеться в режимі «онлайн», з нашого боку має бути реагування на загрози інформаційного характеру, якщо не проактивним, то щонайменше реактивним. Відповідно, з метою удосконалення інформаційно-аналітичного механізму забезпечення інформаційної безпеки України та механізму державного реагування на загрози

інформаційного характеру пропонуємо розробити та впровадити у вітчизняну практику державного управління інформаційною безпекою:

1) паспорти загроз інформаційній безпеці [53];

2) технології державного реагування на загрози інформаційній безпеці.

Структура паспорту загрози інформаційній безпеці містить три частини:

I. Загальна характеристика загрози інформаційній безпеці:

1.1. Структура загрози. Аналізу мають підлягати також чинники, що породжують загрози інформаційній безпеці.

Зокрема, основними видами загроз інформаційній безпеці Українській державі в сучасних умовах гібридної війни є [2-3]:

руйнування єдиного інформаційного простору Української держави;

руйнування духовного простору Української держави;

надмірна комерціалізація частотного ресурсу та медіаринку;

непрозорість формування інформаційної політики провідних телерадіоканалів та медіа-холдингів, які мають велику частку іноземного капіталу;

примітивізація змістовної частини інформаційного продукту, який нерідко має антиукраїнську спрямованість;

відсутність дієвих інформаційно-комунікативних технологій формування самоідентичності громадян України;

застосування спеціальних інформаційно-комунікативних технологій для деструктивного впливу на психіку людини та маніпулювання суспільною свідомістю;

заміна цінностей національної культури цінностями масової культури;

зміна картини світу людини, її ціннісної свідомості в напрямку вигідному для активної сторони деструктивного впливу;

насадження чужих для українського суспільства цінностей та інтересів;

зміна мотиваційних настанов;

формування нових стереотипів поведінки, які є асоціальними для українського суспільства;

перегляд історії як засіб руйнації духовних цінностей українського народу;

перекодування оточуючого світу, тобто введення нових елементів оточуючого світу та зміна емоційного навантаження існуючих;

обмеження, дозоване подання інформації, або ж масоване подання необхідної інформації;

переобтяження каналів непотрібною, надлишковою інформацією;

подання сигналів, несумісних із внутрішніми символьними системами українського суспільства.

1.2. Об’єкти загрози: об’єкти загрози визначаються відповідно їх спрямованості проти реалізації життєво важливих національних інтересів в інформаційній сфері.

Об’єктами загроз інформаційній безпеці пропонуємо визначити:

конституційні права і свободи людини й громадянина у сфері духовного життя та інформаційної діяльності;

індивідуальна свідомість;

консервативна складова масової свідомості, що є сукупністю:

а) загальних інтересів (інтересів, що поділяються переважною більшістю членів соціальних груп);

б) культурних, духовних та моральних цінностей, що визначають правила поведінки членів групи;

в) готовності до протидії чинникам та діям, що загрожують цим цінностям та інтересам;

динамічна складова масової свідомості, що є сукупністю відображень інформації про соціально значущі події в консервативній складовій масової свідомості.

1.3. Джерела загроз інформаційній безпеці: джерелами загроз визначаються явища, процеси, події та інші чинники, а також суб’єкти, які

створюють небезпеку для інформаційної безпеки.

До зовнішніх джерел вказаних загроз пропонуємо віднести:

недосконаліть міжнародного права, що регулює міжнародні інформаційні відносини в глобалізованому світі, а також недостатню практику застосування права у цій специфічній сфері;

розвідувально-підривна діяльність іноземних спецслужб, іноземних ЗМІ, яка спрямована проти національних інтересів Української держави у інформаційній сфері;

загострення конкуренції у сфері міжнародних інформаційних відносин;

діяльність міжнародних терористичних організацій в напрямку реалізації сценаріїв інформаційного тероризму;

розробку та застосування низкою держав концепцій інформаційної та психотронної війни.

До внутрішніх джерел загроз пропонуємо віднести:

недостатню координацію органів державної влади та органів місцевого самоврядування з формування й реалізації єдиної державної політики у сфері інформаційної безпеки України;

недосконаліть нормативно-правової бази в галузі інформаційної безпеки України, а також недостатню практику застосування інформаційного права у сфері забезпечення інформаційної безпеки;

недостатню економічну та інформаційну потужність держави;

недосконаліть системи освіти та виховання в аспекті формування критичного мислення у населення країни, а також стійкості до деструктивних інформаційно-психологічних впливів;

недостатню кількість кваліфікованих кадрів у сфері інформаційно-психологічної безпеки.

II. Характеристика можливого розвитку загрози інформаційній безпеці:

2.1. Вказуються тривалість та просторовий розмах загроз інформаційного характеру.

В даному випадку коротко- та середньостроковим загрозами можуть

виступати явні загрози і загрози динамічній складовій масової свідомості. Довгостроковими загрозами можуть виступати сугестивні загрози та загрози консервативній складовій масової свідомості.

Вказані загрози можуть застосовуватися в комплексі із загрозами організаційній безпеці [39].

2.2. Тенденції розвитку загроз інформаційній безпеці.

Трансформація масової свідомості та зовнішнього середовища під впливом «агресора» здійснюється в два етапи [95]:

1 етап: робота з динамічною складовою масової свідомості в напрямку дестабілізації суспільно-політичної системи;

2 етап: зміна у консервативній складовій в напрямку модифікації суспільства за сценарієм агресора, й насамкінець закріплення нових елементів масової свідомості.

2.3. Можливі наслідки загрози інформаційно-психологічній безпеці.

Наслідками реалізації явних та сугестивних загроз, загроз консервативній та динамічній складовим масової свідомості є:

1) світоглядний хаос, некритичність мислення і диктат забобонів, що дозволяє здійснювати екзистенційне маніпулювання масовою свідомістю населення країни;

2) комплекс меншовартості народу або ж навіть психологія раба; громадянський інфантилізм; вкрай низький рівень релігійної і етичної культури.

Вітчизняний дослідник В. Зеленін пропонує здійснювати якісну та кількісну оцінку результатів негативного інформаційно-пропагандистського впливу за такими індикаторами, як: оточення, поведінка, здібності, переконання/цінності, ідентичність (див. табл. 3.2.1.). При цьому він констатує, що чим вищий нейрологічний рівень атаки застосовується у інформаційно-пропагандистській війні, тим більш нищівні наслідки це має.

Таблиця 3.2.1.

Рівні оцінки індикаторів стану
інформаційно-психологічної безпеки військових колективів

Якісна оцінка	Індикатор (характеристика / результат негативного інформаційно-пропагандистського впливу)	Кількісна оцінка
Дуже низький (фон, шум)	**Оточення** Суб'єкт негативно висловлюється у спілкуванні з товаришами по службі щодо уставних документів, національного суверенітету розповсюджує занепадницькі настрої тощо. Проте ніяких претензій до виконання ним службових обов'язків з боку керівництва до нього нема.	На цьому рівні інформаційно-пропагандистський тиск є таким, що виводить з ладу не більше 5% особового складу.
Низький (припустимий)	**Поведінка** Суб'єкт починає нехтувати службовими обов'язками, саботувати, діяти всупереч уставу, дискредитувати накази, пояснюючи це тим, що «в державі все неправильно» тощо	На цьому рівні інформаційно-пропагандистська атаках виводить з ладу до 15%
Середній (збитковий)	**Здібності** На цьому рівні суб'єкт вже не може (втрачає здібності) виконувати службові обов'язки. Навіть у разі актуальної небезпеки для свого життя не може застосувати зброю, за першої можливості дезертирує	Цей рівень є свідченням інформаційно-пропагандистської війни, адже понад 45 % особового складу є не боєздатні

Високий (критичний)	**Переконання / цінності** На цьому рівні суб'єкт майже повністю деморалізований. Він активно поширює занепадницькі настрої, починає переконувати товаришів по службі скласти зброю та здатися ворогу. Накази не виконує, порушуючи присягу.	Цей рівень інформаційно-пропагандистської агресії виводить з ладу до 70% особового складу.
Дуже високий (руйнівний)	**Ідентичність** На цьому рівні представник силових структур зраджує Батьківщину, починає ідентифікувати себе з ворогом, відверто переходить на його бік застосовує зброю проти своїх.	Такий рівень інформаційно-пропагандистської навали винищує до 90% особового складу.

Джерело : [24, с. 102]

III. Діяльність суб'єктів забезпечення інформаційної безпеки по реагуванню на загрози:

3.1. Суб'єкти забезпечення інформаційної безпеки.

До суб'єктів забезпечення інформаційної безпеки належать наступні органи: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Збройні Сили України, Служба безпеки України, військові формування, утворені відповідно до законів України.

Зрозуміло, що в залежності від характеру завдань, їх виконання входить до компетенції державних органів різного рівня, які відносяться до різних гілок влади, мають різні сфери діяльності та обсяг владних повноважень. Але враховуючи той факт, що політика інформаційної безпеки як суспільне явище носить комплексний характер, необхідно розглядати діяльність державних органів, спрямовану на виконання конкретних завдань в цій сфері, в рамках єдиного інституціонального механізму, який об'єднується єдиною метою забезпечення належних умов забезпечення інформаційної безпеки України.

3.2. Ресурсне забезпечення діяльності суб'єктів забезпечення інформаційної безпеки.

Організацію ресурсного забезпечення діяльності суб'єктів забезпечення інформаційної безпеки здійснює Секретаріат Кабінету Міністрів України, а також Міністерство культури та інформаційної політики України, Міністерство оборони України, Міністерство внутрішніх справ України, Міністерство освіти та науки України, Міністерство цифрової трансформації України, Міністерство фінансів України.

3.3. Способи і методи реагування на загрози: визначається алгоритм дій суб'єктів забезпечення інформаційної безпеки по реагуванню на загрози інформаційного характеру.

Попередньо зауважимо, що в умовах гібридної війни система забезпечення інформаційної безпеки має забезпечити захист національного інформаційного простору від закордонної пропаганди, нейтралізувати або значно послабити довготривалий вплив іноземних інформаційних дій. Тобто, ця система повинна забезпечити надійний захист від методів інформаційно-психологічних операцій. Враховуючи специфічний характер цих операцій потрібний окремий підхід для протидії їхнім наслідкам, а також спеціальні дії щодо їхньої нейтралізації.

Вказані завдання можна вирішити шляхом розробки та впровадження в державно-управлінську практику технологій реагування на загрози інформаційно-психологічного характеру.

Структура технології містить такі елементи: теоретична концепція, яка відображає закономірності функціонування об'єкту безпеки; об'єкт безпеки і предмет впливу (сторона об'єкт безпеки); алгоритм впливу; технологічні способи і засоби перетворення предмету впливу [138].

Перша складова технології реагування на загрози інформаційно-психологічного характеру – це теоретичні концепції, які відображають закономірності функціонування системи формування та регулювання

духовного потенціалу суспільства в умовах динамічного безпекового середовища.

Друга складова технології реагування на загрози інформаційній безпеці – це:

1) об'єкт управлінського впливу – субстрат загроз інформаційно-психологічній безпеці (див. рис. 1):

особа, її права і свободи;

соціальні організації у взаємовідносинах між собою, духовний потенціал суспільства загалом;

держава, її національно-культурна самобутність, інформаційний суверенітет;

2) головний суб'єкт забезпечення інформаційної безпеки є держава, яка разом із іншими суб'єктами інформаційно-суспільних відносин реалізовує політику в інформаційній сфері суспільства. Ця політика покликана забезпечити духовну єдність українського народу, національну злагоду і мир;

3) предмет управлінського впливу – це процес перетворення і трансформації субстрату загроз інформаційно-психологічній безпеці, а саме: профілактика та протидія виявленим загрозам.

Третя складова технології реагування на загрози інформаційній безпеці – це алгоритм реагування, який передбачає послідовне застосування технологічних способів, методів і засобів реагування з метою мінімізації рівня загроз інформаційно-психологічній безпеці.

Алгоритм реагування на загрози інформаційно-психологічній безпеці містить такі операційні ланцюги:

1) формулювання проблеми забезпечення інформаційно-психологічної безпеки (формулювання проблеми та її оцінка);

2) моніторинг загроз інформаційно-психологічній безпеці;

3) ідентифікація та оцінка рівня загроз інформаційно-психологічній безпеці;

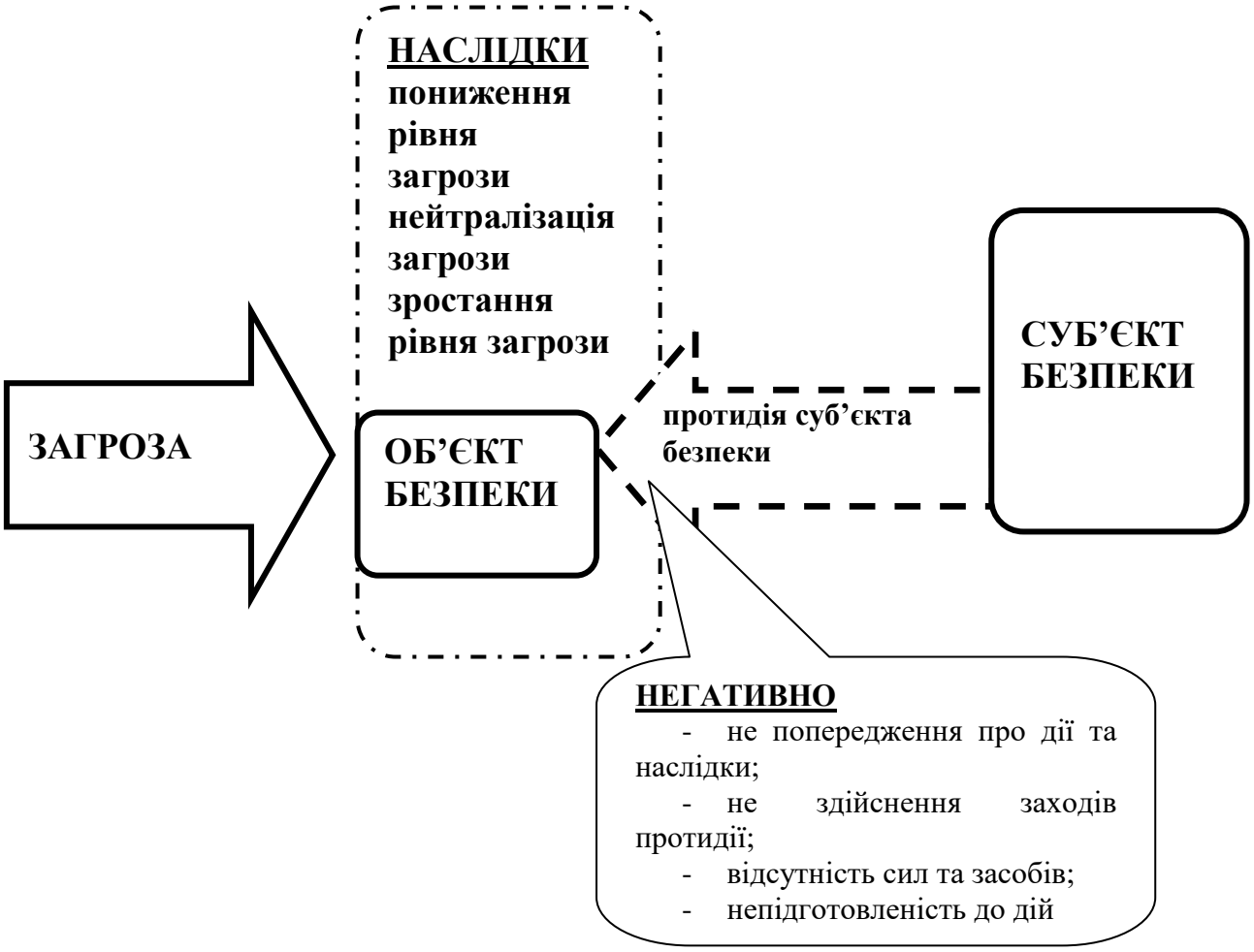

Рис. 1. Схема протидії загрозам об'єкту безпеки

4) розробка варіантів локалізації/нейтралізації загрози інформаційно-психологічній безпеці;

5) оцінка варіантів локалізації/нейтралізації загрози інформаційно-психологічній безпеці;

6) вибір оптимального варіанту локалізації/нейтралізації загрози інформаційно-психологічній безпеці за обраними критеріями ефективності та результативності;

7) прийняття рішення про локалізацію/нейтралізацію загрози інформаційно-психологічній безпеці;

8) підготовка та всебічне забезпечення реалізації державно-управлінського рішення щодо реагування на загрозу інформаційно-психологічній безпеці;

9) управлінський вплив на загрозу (локалізація/нейтралізація загрози);

10) оцінка рівня загрози інформаційно-психологічного характеру після впливу на неї системи забезпечення інформаційної безпеки;

11) вибір оптимального варіанту за обраним критерієм досягнення запланованого результату реагування на загрозу.

Четверта складова технології реагування на загрози інформаційно-психологічній безпеці – це технологічні способи реагування на загрози, а саме правила згідно яких здійснюються заходи щодо реагування на виявлені загрози.

П’ята складова технології реагування на загрози інформаційно-психологічній безпеці – це засіб перетворення предмету (певної сторони об’єкту безпеки), що передбачає застосування відповідних методик реагування на виявлені загрози інформаційно-психологічного характеру.

Шоста складова технології реагування на загрози інформаційно-психологічній безпеці – це контроль досягнутого результату по локалізації/нейтралізації виявленої загрози. Вказана технологія є надійним інструментом у процесі вирішення завдань забезпечення інформаційно-психологічної безпеки.

Таким чином: 1. Визначено порядок денний щодо удосконалення системи творення державної політики у сфері інформаційної безпеки, а саме:

удосконалення механізмів формування і реалізації державної політики у сфері інформаційної безпеки, а також механізмів забезпечення інформаційної безпеки України з урахуванням динамічного безпекового середовища, й державного механізму реагування на загрози інформаційного характеру;

розробка реактивних та проактивних технологій захисту національного інформаційного простору, й зокрема технологій спеціальних інформаційних операцій в інтересах забезпечення національної безпеки України.

2. Запропоновано рекомендації щодо удосконалення механізмів розробки та реалізації державної політики у сфері інформаційної безпеки України, зокрема на сучасному етапі необхідно:

здійснити систематизацію актів законодавства за трьома рівнями: доктринально-стратегічним; тактичним та функціонально-спеціальним;

надати інформаційній безпеці статусу пріоритетного напряму в роботі органів державної влади;

надати прогнозуванню майбутнього інформаційного і безпекового середовища статусу пріоритетного напряму в роботі суб'єктів формування державної політики у сфері інформаційної безпеки;

розширити перелік викликів і загроз інформаційного характеру та конкретизувати положення законів України, що регламентують діяльність суб'єктів забезпечення інформаційної безпеки України;

оптимізувати структуру та функції механізмів формування і реалізації державної політики у сфері інформаційної безпеки України з урахуванням поділу державної політики на довгострокову і поточну;

удосконалити концептуальний підхід до реформування системи забезпечення інформаційної безпеки;

здійснити паспортизації загроз інформаційного характеру;

здійснити технологізацію державного реагування на загрози інформаційній безпеці та ін.

3.3. Інституціоналізація інформаційно-психологічної безпеки в системі інформаційного права України

Сучасні соціальні, політичні та геополітичні процеси, що відбуваються в світі та Україні, процеси широкого проникнення цифрових технологій у всі сфери життя і викликані ними соціальні зміни, гібридна війна росії проти України, негативні інформаційно-психологічні впливи на ОПР зумовлюють необхідність модернізації системи українського законодавства у сфері інформаційної безпеки. Система інформаційного права та інформаційної безпеки має досягти максимальної відповідності в процесах цифровізації, розвитку інформаційного суспільства, протидії інформаційним та смисловим війнам, що є сьогодні викликами та загрозами України. Вважаємо, що таким новим правовим інститутом інформаційного права є правове забезпечення інформаційно-психологічної безпеки. Процес інституціоналізації у праві тісно

пов'язаний із загальними тенденціями розвитку правової системи країни. У юридичній науці домінує розуміння інституціоналізації на підставі інституційної теорії як процесу створення інститутів, а інститут права традиційно сприймається як система норм права, об'єднаних за ознакою однорідності їх предмета» [159]. Інститут, як галузь права, на думку В.Богдановича характеризують загальні системні ознаки функціональності та субстанційності в їх поєднанні [11]. Базовими ознаками інституту права виступають предмет та метод правового регулювання. Предмет характеризує те, що регулює право, а метод – певні прийоми, способи, засоби впливу права на суспільні відносини. Правове регулювання забезпечення інформаційної безпеки є інститутом інформаційного права. Можна виділити ряд ознак правового інституту інформаційної безпеки, включаючи наявність впорядкованої системи інформаційно-правових норм, їх цільову орієнтованість на забезпечення життєво важливих інтересів в інформаційній сфері, виділення особистого, суспільного та державного рівнів інформаційної безпеки.

У виділеного інституту є свій самостійний предмет правового регулювання – комплекс суспільних відносин, пов'язаних із захистом особистості, соціальних груп та суспільства від деструктивного ІПВ. Ця сфера відносин має достатню чітку грань, що відокремлює її від іншого великого блоку відносин у рамках інформаційної безпеки – захисту інформації. Названий предмет правового регулювання має достатню однорідність, оскільки в основі його лежить загальний механізм надання деструктивного ІПВ на індивідуальну психіку та суспільну свідомість, а також захист від нього.

Є характерний метод правового регулювання, що охоплює сукупність способів та засобів впливу права на суспільні відносини. У сфері забезпечення ІПБ домінує імперативний метод правового регулювання, активно застосовуються правові засоби заборон та зобов'язань. Наприклад, законодавством України встановлено правові заборони на поширення певної негативної інформації, що доповнюються запровадженням юридичної відповідальності за їх порушення та наділення державних органів та

інформаційних посередників обов'язками з обмеження поширення такого контенту у певних інформаційних середовищах [97]. Критерії єдності правових норм, нормативної відокремленості та повноти регульованих відносин виконуються лише частково, що свідчить про те, що інститут правового забезпечення ІПБ знаходиться в стадії формування. Водночас уже зараз чітко проглядається міжгалузева природа цього правового інституту, властива її «материнській» підгалузі. Інститут права як системна правова освіта відрізняється високим рівнем інтеграції, що виходить за рамки окремих галузей права, набуваючи міжгалузевого або загальноправового статусу.

Норми інформаційного права відіграють ключову роль у правовому регулюванні цілей, завдань, принципів та напрямів забезпечення ІПБ. Прерогативою інформаційного права є регламентація питань протидії поширенню негативної інформації у ЗМІ та мережі Інтернет. Водночас інформаційно-правове регулювання не вичерпує всієї предметної галузі забезпечення ІПБ. Тому правову основу ІПБ становлять також норми інших галузей права, включаючи конституційне, адміністративне, кримінальне, цивільне. Конституційне право встановлює базові засади державного та громадського устрою, правового статусу особистості, а також систему органів публічної влади в Україні, мають відправне значення всіх сфер забезпечення національної безпеки. Крім того, норми конституційного законодавства у окремих галузях стосуються питань протидії деструктивному ІПВ (наприклад, маніпуляції суспільною свідомістю). Роль адміністративного права проявляється, перш за все, в регламентації правового статусу органів виконавчої влади, що є основними суб'єктами забезпечення ІПБ. Також адміністративне право, так само як і кримінальне право, встановлює юридичну відповідальність за правопорушення, пов'язані з наданням деструктивного ІПВ на особу та соціальні групи. Норми цивільного права регламентують питання захисту честі, гідності та ділової репутації як нематеріальних благ фізичних та юридичних осіб, а також підстави та види цивільної відповідальності в області, що вивчається нами. Тому правовий інститут забезпечення ІПБ має

міжгалузевий характер. За наявності досить різноманітних правових методів та засобів протидії загрозам ІПБ інформаційне законодавство не містить відправних норм, що характеризують базові аспекти забезпечення ІПБ, включаючи понятійний апарат, загрози ІПБ, правові принципи та напрями її забезпечення. Наслідком цього є відсутність системності у правовому регулюванні забезпечення ІПБ. Даний правовий пробіл вимагає усунення.

Висновки до третього розділу.

1. В розділі сформульовано пріоритетні напрями вдосконалення державної політики інформаційної безпеки в умовах протидії гуманітарної експансії рф проти України, дано авторське тлумачення поняття «забезпечення ІПБ» та «правове забезпечення ІПБ», «система правового забезпечення ІПБ», визначені заходи з забезпечення ІПБ, які поділено на 4 групи. Сформульований також авторський перелік національних інтересів в інформаційній сфері. Чітко визначені мета, завдання та напрями забезпечення ІПБ та на основі аналізу нормативно-правових документів України у сфері інформаційної безпеки визначено додаткові завдання з забезпечення ІПБ.

2. Розкрита сутність та структура Паспорту загроз інформаційній безпеці, визначено завдання та функції забезпечення ІПБ.

3. Окреслено основний зміст процесу інституціоналізації інформаційно-психологічної безпеки в системі інформаційного права України та дано рекомендації щодо удосконалення нормативно-правових механізмів державної політики у сфері інформаційної безпеки України.

4. Основні наукові результати розділу опубліковані в працях [54].

ВИСНОВКИ

У дисертаційній роботі узагальнено і вирішено актуальне наукове завдання науки «Публічне управління та адміністрування», яке полягає у обґрунтуванні теоретичних положень і методологічних підходів дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки та на підставі комплексного аналізу міжнародно-правових стандартів у сфері інформаційної безпеки і досвіду зарубіжних країн щодо використання публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки, науково обґрунтовано пропозиції з удосконалення цих механізмів в Україні. Розроблено основні положення Концепції інформаційно-психологічної безпеки України.

1. Теоретичний аналіз проблеми та узагальнення основних наукових підходів щодо дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки дає підстави стверджувати, що у вітчизняній та зарубіжній науці накопичено суттєвий науковий багаж знань з окремих аспектів забезпечення інформаційно-психологічної безпеки. Проте цілісна концепція інформаційно-психологічної безпеки як об'єкта публічно-управлінського регулювання та системне бачення механізмів її забезпечення в гібридної та конвенційної війни, яку веде України проти рф досі відсутні. Аналіз понятійно-категорійного апарату дослідження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки, що міститься у нормативно-правових документах та результатах наукових досліджень із досліджуваної теми свідчить, що реалізація публічно-управлінських механізмів забезпечення інформаційної безпеки України залишається актуальною науковою проблемою, що на сьогодні, незважаючи на значну кількість наукових розробок у цій сфері, характеризується недостатнім ступенем вивчення. В той же час питання формування та реалізації публічно-управлінських механізмів забезпечення інформаційної безпеки України знаходиться на стадії розробки та обговорення в рамках наукового дискурсу.

Проведений аналіз дозволив авторові визначити *публічно-управлінський механізм забезпечення інформаційно-психологічної безпеки* як ефективно функціонуючу систему засобів, заходів та важелів інформаційно-психологічного впливу суб'єкту управління (органів публічної влади та місцевого самоврядування) на об'єкти управління. Проведений же аналіз критичних підходів до трактування безпеки, представлених у науковій літературі, дозволив дійти висновку про оптимальність використання конструкції «стан захищеності» як основи визначення базової категорії «безпеки» та окремих її видів. При цьому саме поняття «стан захищеності» трактується як «сукупність внутрішніх та зовнішніх умов, що запобігають або мінімізують негативний вплив загроз на об'єкти безпеки та забезпечують тим самим можливість існування та збереження даного об'єкту. На основі вищевикладеного автором визначено *інформаційно-психологічну безпеку* як складову частину інформаційної системи безпеки, що є станом захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу. На основі міждисциплінарного підходу досліджено проблему правового забезпечення ІПБ та доведено двоїстість об'єктів ІПБ - до них віднесено як саму людину, групи людей і суспільство в цілому, так і їх психологічні складові – індивідуальну психіку та суспільну свідомість.

2. Досліджено сутність, функції та повноваження публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки в України. Визначено, що ключовою проблемою інформаційної (інформаційно-технічної та інформаційно-психологічної) безпеки України є проблема концептуального, доктринального і законодавчого її забезпечення, формування комплексу нормативно-правових регуляторів даної сфери. Інформаційно-психологічна безпека України не виділена як одна з визначальних у спектрі безпекових складових.

3. Проаналізовано зарубіжний досвід державно-управлінської практики щодо забезпечення інформаційної безпеки та можливості його використання в Україні. Серед релевантних міжнародно-правових норм, що

стосуються забезпечення ІПБ, у межах тематичних груп міжнародних актів досліджено та виділено такі сфери: 1) права людини; 2) ЗМІ та мережі Інтернет; 3) боротьба зі злочинністю та тероризмом в інформаційному просторі; 4) міжнародна інформаційна безпеки. Розроблено таблицю видів негативного контенту у міжнародно-правових актах з описом контенту та посиланням на правове джерело де воно міститься. Розвиток правового регулювання забезпечення ІПБ у рамках правового поля МІБ є дуже значущим, оскільки транскордонний характер багатьох інформаційних загроз зумовлює необхідність тісної міжнародної співпраці для ефективної протидії їм. При цьому ми підтримуємо включення питань забезпечення ІПБ до загального предметного порядку денного МІБ, її ухвалення в рамках ООН заклало б фундамент для міжнародно-правового регулювання у сфері МІБ на глобальному рівні, який можна розвивати на регіональному рівні та (або) за окремими напрямками забезпечення МІБ , включаючи психологічні аспекти (ІПБ). Зроблено висновок, що для України як держави, що зіткнулася із проблемами втягнення в гібридну війну та наявністю населення на тимчасово окупованих територій, досвід країн ЄС щодо гарантування інформаційної безпеки є доцільним для розгляду. Зокрема пропонується використовувати приклад Хорватії, протидія сепаратизму в якій закінчилася успішною реінтеграцією самопроголошеної «республіки». Відповідно, варто використовувати передові методи протидії російській інформаційній агресії , постійно представляти якісний інформаційний продукт на тимчасово окупованих територіях . Доцільним буде також наслідувати досвід Німеччини в переході до принципу «активної оборони » щодо інформаційної безпеки . Постійна діяльність компетентних органів, спрямована на попередження, протидію загрозам в інформаційній сфері , а також застосування активних заходів інформаційного впливу може надати значні переваги в умовах гібридної війни з рф.

4. Розкрито зміст інформаційно-психологічних загроз як головного фактору розгортання «гібридної війни». Визначено 8 характерних рис загроз ІПБ та розроблено матрицю загроз ІПБ, що відображає широкий спектр загроз

ІПБ у політичній, соціальній, культурній та міжнародній сферах. Також загрози ІПБ чітко проглядаються у рамках державної, громадської та воєнної безпеки. На основі складеної матриці основних загроз ІПБ, а також з урахуванням результатів власного наукового дослідження, представлено авторську класифікацію основних загроз ІПБ, що включає в себе поділ цих загроз на групи контентних та комунікаційних загроз. Все це дозволило запропонувати опис актуальних загроз інформаційно-психологічній безпеці людини, суспільству та державі в Україні.

5. Охарактеризовано проблеми та перспективи розвитку системи правового забезпечення інформаційно-психологічної безпеки в Україні. Аналіз стану захищеності інформаційно-психологічного простору України свідчить, що інформаційно-психологічна безпека України не виділена як одна з визначальних у спектрі безпекових складових. Політико-правові механізми державного управління нею чітко не визначені, фрагментовані та неузгоджені, а передовий іноземний досвід не запроваджується. За роки незалежності України так і не було прийнято Закон України «Про інформаційно-психологічну безпеку», де було б чітко визначено суб'єктів державної політики національної безпеки у даній сфері діяльності та політико-правові механізми її реалізації. Запропоновано авторське визначення понять : «політико-правовий механізм», «правове забезпечення ІПБ».

6. Визначено пріоритетні напрями та запропоновано рекомендації щодо вдосконалення публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни, дано авторське тлумачення поняття «забезпечення ІПБ» та «правове забезпечення ІПБ», «система правового забезпечення ІПБ», визначені заходи з забезпечення ІПБ, які поділено на 4 групи. Сформульований авторський перелік національних інтересів в інформаційній сфері. Чітко визначені мета, завдання та напрями забезпечення ІПБ та на основі аналізу нормативно-правових документів України у сфері інформаційної безпеки визначено додаткові завдання з забезпечення ІПБ. Розкрита сутність та структура Паспорту загроз

інформаційній безпеці, визначено завдання та функції забезпечення ІПБ. Окреслено основний зміст процесу інституціоналізації інформаційно-психологічної безпеки в системі інформаційного права України та надано рекомендації щодо удосконалення нормативно-правових механізмів державної політики у сфері інформаційної безпеки України.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Алещенко, В. Інформаційно-психологічна складова безпеки особистості в умовах війни. *Вісник Національного університету оборони України*, 66(2), 2022. С.5–17. URL https://doi.org/10.33099/2617-6858-2022-66-2-5-17

2. Алещенко В.І. Особливості сучасних психологічних операцій Російської Федерації в умовах гібридної війни. “Сучасні інформаційні технології у сфері безпеки та оборони”. Київ. № 3/2019.

3. Алещенко В.І. Феноменологія "гібридної війни" та її особливості у виконанні Російської Федерації: інформаційно-психологічний аспект. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки,* №1(34)/2016. С.6-11.

4. Андрущенко Т.В., Зеленін В.В. Психологія політичної пропаганди : Методичні рекомендації для самостійної роботи студентів. 2-ге видання, виправлене та доповнене. К.: Видавництво «Гнозіс», 2022. 100 с.

5. Антонюк В.В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: автореф. дис... канд. наук держ. упр.: 25.00.02 / НАДУ. К., 2017. 20 с.

6. Арабаджиєв, Д. Ю., Сергієнко, Т. І. Політична маніпуляція та інформаційно-психологічна безпека в політичних відносинах. *Політикус : наук. журнал*. 2020. № 2. С. 36–44. URL http://dspace.pdpu.edu.ua/handle/123456789/9448

7. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 «Право». Львівський державний університет внутрішніх справ. Львів, 2022

8. Біла книга протидії дезінформації / ГО «Інститут інформаційної безпеки». К., 2022. 62 с.URL: https://bit.ly/DisinfoWhiteBook2023,

9. Бірта Г. О., Бургу Ю.Г. Методологія і організація наукових досліджень. [текст] : навч. посіб. К. : «Центр учбової літератури», 2014. 142 с.

10. Богданович В.Ю. Інформаційна безпека та шляхи її забезпечення : навч. посіб. / В.Ю. Богданович ; [у 2 ч. : Основні засади забезпечення інформаційної безпеки]. К. : Вид-во НАУ, 2005. Ч. ІІ. 342 с.

11. Богданович В.Ю. Системний підхід до дослідження проблем національної безпеки держави. URL: http://books.zntu.edu.ua/book_info.pl?id=89181

12. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для Україн безпеки. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350

13. Валевський О. Л., Ребкало В. А. Державне управління як інструмент впровадження реформ в Україні. Аналітика і влада. 2012. № 6. С. 139-144. URL: http://nbuv.gov.ua/UJRN/avlad_2012_6_23

14. Варивода Я.О. Масова свідомість як об’єкт національної безпеки . Людина і політика. 2001. №2. С. 88-96.

15. Василенко В.А. Комунікативно-психологічна культура особистості як складова інформаційно-психологічної безпеки // Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів: матеріали міжнародної науково-практичної, 30 жовтня 2020 року, Державний науково-дослідний інститут МВС України, Київ: ДНДІ МВС України, 2020. С.24-27.

16. Вєдєнєєв Д. Семенюк О. Організаційно-управлінський механізм розбудови та діяльності структур інформаційно-психологічного протиборства збройних сил України (2007–2021 рр.). Право та державне управління. 2022. С.147-152. https://doi.org/10.32840/pdu.2022.3.22

17. Військовий Інтернет. Ньюсленд. 08.11.2009. URL: http://newsland.ru/news/article.htm.

18. Власенко О.В. Механізми державного регулювання захисту громадян від негативних інформаційних впливів: дис. … канд. наук з держ. упр.: спец. 25.00.02. Київ., 2012. 190 с.

19. Воєнні аспекти протидії «гібридній» агресії: досвід України: монографія / авт. кол.; за заг. ред. А. М. Сиротенка. Київ: НУОУ ім. Івана Черняховського, 2020. 176 с.

20. Галузь OSINT в суспільній та державній діяльності. URL: https://bit.ly/OSINTUkraine

21. Глобальна та національна безпека : підручник / авт. кол. : В.І.Абрамов, Г.П.Ситник, В.Ф.Смолянюк; за заг. ред. Г.П.Ситника. – Київ : НАДУ, 2016. – 784;

22. Голод К. Інформаційна безпека США : сучасний стан та уроки для України. *ДВНЗ «Ужгородський національний університет »* / Геополітика україни: історія і сучасність / Збірник наукових праць. Випуск 2(19). 2017. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/22442/1/Інформаційна%20безпека%20США.pdf

23. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Стратегічні пріоритети, № 4 (33), 2014 р. С.5-12.

24. Горбулін В. Як перемогти Росію у війні майбутнього. К.: Брайт Букс, 2021. 248 с.

25. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дис. … канд. наук з держ. упр.: спец. 25.00.02. Київ., 2004. 205 с.

26. Гусаров В. Кремль розпочав нову інформаційну операцію проти України. Українська правда. URL: https://www.pravda.com.ua/news/2014/09/3/7036659/

27. Гусаров В. Протидія інформаційному тиску Кремля: першочергові кроки. «MediaSapiens» URL: http://osvita.mediasapiens.ua/monitoring/advocacy_and_influence/protidiya_informatsiynomu_tisku_kremlya_pershochergovi_kroki/.

28. Дахно О. Адміністративно-правове регулювання протидії інформаційно-психологічним операціям на стратегічному рівні. Науковий вісник Ужгородського Національного Університету, 2022. DOI https://doi.org/10.24144/2307-3322.2021.69.44

29. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення. : монографія / Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. Львів : Сполом, 2020. 418 с.

30. Деркаченко Я. Інформаційно-психологічні операції як сучасний інструмент геополітики. URL: https://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/

31. Дубов Д. Інформаційна безпека в умовах впровадження електронного урядування. Вісник книжкової палати. 2006. № 7. С. 34–38.

32. Дузь-Крятченко О.П.та ін. Основи стратегії національної безпеки та оборони держави: підруч. 3-е вид., перероб. і доп. Київ: НУОУ ім. І. Черняховського, 2015. 620 с.

33. Історія інформаційно-психологічного протиборства : підруч./ Я.М.Жарков та ін.; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.

34. Енциклопедичний словник з державного управління / уклад.: Ю.П. Сурмін, В.Д. Бакуменко, А.М. Михненко та ін.; за ред. Ю.В. Ковбасюка, В.П. Трощинського, Ю.П. Сурміна. К.: НАДУ, 2010. 820 с.

35. Євдоченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: дис. канд. наук з держ. упр.: спец. 25.00.01. Львів., 2011. 225 с.

36. Журавський В.С., Родіонов, І.Б., Жиляєв; Україна на шляху до інформаційного суспільства. За заг. ред. М.З. Згурського. К.: ІВЦ «Видавництво «Політехніка», 2004. 484 с.

37. Запорожець О .Ю. Політика Європейського Союзу в сфері інформаційної безпеки [Електронний ресурс] // Київський національний університет імені Тараса Шевченка / Актуальні проблеми міжнародних відносин. Випуск 87 (Частина II). 2009. URL: http://journals.iir.kiev.ua/index.php/apmv/article/viewFile/1195/1139

38. Затинайко О., Павленко В., Бочарніков В., Свєшніков С. Політика безпеки і воєнно-політичні відносини Угорщини. Наука і оборона. 2014. № 1. С. 11.

39. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни: навч. посіб. Том 1. НЛП – XX століття. 2-е видання, виправлене та доповнене. К.: Вид-во «Люта справа», 2015. 384 с.

40. Зозуля О. С. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства : дис. … канд. наук з держ. упр. : 25.00.01. Київ, 2017. 261 с.

41. Золотухін Д. Головний важель «гібридної» війни – використання «вразливостей» демократії. «Гібридна» війна Росії – виклик і загроза для Європи: Матеріали Центра Разумкова. К., грудень 2016. С. 13 – 15.

42. Історія інформаційно-психологічного протиборства : підруч. / Я.М.Жарков та ін.; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.

43. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька // Humanitarian vision. - 2016. - Vol. 2, Num. 1. - С. 27-32. - Режим доступу: http://nbuv.gov.ua/UJRN/hv_2016_2_1_7

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

45. Інформаційно-психологічна безпека: сучасні тренди: моногр. /Бровко О.О. та ін; за ред. Курбана О.В., Лісневської А.Л. К.: Київ, ун-т ім. Б.Грінченка, 2022. 392 с.

46. Канарський В.С. Аналітичний огляд джерел та наукової літератури з публічного управління інформаційно-психологічною безпекою України. Актуальні питання у сучасній науці (Серія «Державне управління»). Випуск № 6(12) 2023. С. 210-224

47. Канарський В. С. Інформаційні загрози як головний фактор розгортання «гібридної війни». Електронне наукове видання "Публічне адміністрування та національна безпека". 2022. №2. URL: https://doi.org/10.25313/2617-572X-2022-2-7926

48. Канарський В.С. Механізми оптимізації державного управління забезпеченням інформаційної безпеки в Україні. 30 років незалежності України: досягнення, виклики, перспективи : мате ріали міжнар. наук.практ. конф. (Київ, 10 верес. 2021 р.) / за заг. ред. Л. Г. Комахи, О. М. Андрєєвої, В. А. Гошовської. Київ : ННІ ПУДС КНУ, 2021. С.178-179.

49. Канарськiй В. С. Політико-правовий механізм державного управління інформаційно-психологічною безпекою України: сутність, функції та повноваження. Наукові перспективи, Випуск №9(15). 2021. С.99-110.

50. Канарський В.С. Пріоритети державної політики інформаційної безпеки України: Збірник тез наукових доповідей XII Всеукр. наук.-практ. конф. “Актуальні проблеми управління інформаційною безпекою” (Київ: Національна академія СБУ, 26 березня 2021 р.), С.275-276.

51. Канарський В. Пріоритетні напрями вдосконалення державної політики інформаційної безпеки в умовах протидії гуманітарної експансії рф проти України. Глобалізаційні виклики: урядування майбутнього : матеріали міжнар. наук.-практ. конф. (Київ, 7–8 черв. 2022 р.) / за заг. ред. Л. Г. Комахи. Київ : ННІ ПУДС КНУ імені Тараса Шевченка, 2022.С.199-201.

52. Канарський В.С. Пропозиції щодо вдосконалення організаційно-правових механізмів реагування на загрози інформаційно-психологічної безпеки України. Шевченківська весна – 2022: публічне управління та державна служба : матеріали міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених (Київ, 19 квіт. 2022 р.) / за заг. ред. Л. Г. Комахи, О. М. Андрєєвої. Київ : ННІ ПУДС КНУ, 2022 С.103-104.

53. Канарський В. Публічно-управлінські механізми протидії інформаційним загрозам: європейський досвід. Україна 2030: публічне управління для сталого розвитку : матеріали щоріч. міжнар. наук.-практ. конф. (Київ, 2020 р.) : у 3 т. / за заг. ред. А. П. Савкова, М. М. Білинської, О. М. Петроє. Київ : НАДУ, 2020. С.32-33.

54. Канарський В. С. Рекомендації щодо удосконалення нормативно-правових механізмів державної політики у сфері інформаційної безпеки України. Наукові інновації та передові технології (серія «Державне управління»). №10(12), 2022. DOI: https://doi.org/10.52058/2786-5274-2022-10(12)-63-75

55. Катаев Є. Інформаційно-психологічна безпека особистості в умовах сучасного суспільства. Вісник Національного університету оборони України, 2 (39) /2014. С. 215-220.,

56. Коваль З.В. Політико-правові механізми державного управління інформаційно-психологічною безпекою України: дис. … канд. наук з держ. упр.: спец. 25.00.02. Одеса., 2011. 201 с .

57. Колотій Н. Ляльководи свідомості. «Дзеркало тижня» URL: https://dt.ua/TECHNOLOGIES/lyalkovodi-svidomosti-_.html

58. Конституція України. URL: https://www.president.gov.ua/documents/constitution

59. Концепція державної інформаційної політики. Сучасний стан інформаційної сфери, визначення проблем на розв'язання яких спрямована концепція . URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=38772&pf35401=174806

60. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. на здобуття наук. ступеня д-ра юрид. наук / Б.А. Кормич. Харків, 2004. 44 с, с. 16.

61. Кормич Б.А. Суб'єктно-об'єктний склад інформаційної безпеки. Актуальні проблеми політики. 2003. Вип. 8. С. 130–137.

62. Кремлівська агресія проти України: роздуми в контексті війни : монографія / Олександр Степанович Власюк, Сергій Володимирович Кононенко, Нац. ін-т стратег. досліджень. Київ : НІСД, 2017. 302 с.

63. Лазаренко О. А. Інформаційний складник гібридної війни російської федерації проти України: тенденції розвитку. Стратегічні пріоритети. 2015. № 3 (36). С. 124 – 133.

64. Левченко О.В. Нормативно-правове регулювання інформаційної безпеки України: стан та шляхи вирішення проблем. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2014. № 3(40). С. 130-135. URL: http://www.hups.mil.gov.ua/periodic-app/article/4075

65. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. «Інформаційна безпека України в умовах євроінтеграції». Київ, 2006. КНТ Країна, 280 с.

66. Максименко С.Д. Психологічні механізми становлення особистості: експериментально-генетичний метод. Наукові записки Інституту психології ім. Г.С. Костюка АПН України / за ред. академіка С.Д. Максименка. К.: Ніка-Центр, 2010. – Вип. 38. С.18-35

67. Марутян Р. Евфемізми російсько-української війни як інструмент смислової війни. Виклики і загрози дестабілізації суспільно-політичної системи України: матеріали науково-практичного семінару (Київ, 11 травня 2022 р.) К / за ред. Г. П. Ситника, Л. М. Шипілової. – Київ : Навч.-наук. ін-т публ. упр. та держ. служби Київ. нац. ун-ту імені Тараса Шевченка, 2022. С.26-31. URL: http://ipacs.knu.ua/pages/osn/2/news/1948/files/3fadf13a-c17f-46a4-b56f-e3b5f92ec3bd.pdf

68. Марутян Р.Р. Інтелектуально-ресурсне забезпечення державного управління у сфері національної безпеки України : монографія. – Київ : ЦП «Компринт», 2020. – 410 с.Інфодемія як наслідок неефективних стратегічних комунікацій. STRATCOM. Науково-публіцистичне видання. К., 2020. №.1. С.36-40.

69. Марутян Р.Р. Методологія стратегічного планування в умовах глобальних загроз національній безпеці та міжнародній стабільності: монограф. / Абрамов В.І., Запорожець Т.В., Марутян Р.Р. та ін.; за заг. ред. Л.М. Шипілової Київ НАДУ, 2018. 232 с.

70. Марутян Р. Національна стійкість як основний інструмент протистояння у гібридній війні. Національна стійкість України до загроз гібридної війни : матеріали наук.-практ. семінару (Київ, 25 квіт. 2018 р.) / за ред. Ю. В. Мельника, Л. М. Шипілової. Київ : НАДУ, 2018. С. 3–5.

71. Марутян Р. Організаційна зброя у гібридній війні. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 04 квіт. 2019 р.). Київ : Нац. акад. СБУ, 2019. С. 89–91.

72. Мороз О. Боротьба за правду: Як мій дядько переміг брехню. Київ: Yakaboo Publishing,2020? 160 с.

73. Наталія Н., Євгенія В. Секрет успіху США у сфері інформаційної безпеки США. *Міжнародні відносини, суспільні комунікації та регіональні студії. 2018*. URL: https://cutt.ly/8e953lQ

74. Національна безпека: світоглядні та теоретико-методологічні засади: монографія/ за заг.ред. О.П. Дзьобаня. – Харків: Право, 2021. 776.

75. Нік Даєр-Візефорд, Світлана Матвієко. Кібервійна та революція. К.:Критика, 2021, /Авториз. пер. з анг. Андрія Бондаря, 328 с.

76. Обґрунтування концептуальних та організаційно-правових засад розробки паспортів загроз національній безпеці України : навч.-метод. посіб. / [Г.П. Ситник, В.І. Абрамов, М.М. Шевченко та ін.] за заг. ред. Г.П. Ситник К.: НАДУ, 2012. 52 с.

77. Ожеван М. Фронти й тили великих інформаційних війн. Підприємництво в Україні. 2001. № 4–5.

78. Олійник О. В. Інформаційна безпека США. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. Вип. 1. С. 280-288. URL: http://nbuv.gov.ua/UJRN/boz_2012_1_33

79. Основи класифікації складу та напрямів інформаційної безпеки. URL: http://mego.info/матеріал/24-основи-класифікації-складу-та-напрямів-інформаційної-безпеки

80. Основи національної безпеки України. Навчальний посібник. / Смолянюк В .Ф., Деменко О. Ф., Прибутько П. С. К.: Паливода А. В., 2017. 140 с.

81. Остапйовський І.Є. Остапйовська Т.П. Актуальність ідей Анрі Файоля в умовах сьогодення. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://evnuir.vnu.edu.ua/bitstream/123456789/5091/1/Fayol.pdf

82. Парахонський Б.О., Яворська Г.М. Онтологія війни та миру: безпека, стратегія, смисл: монографія. К.: НІСД, 2019, 560 с.

83. Панченко О.А., Кабанцева А.В. Людська психіка в інформаційній небезпеці. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. Том 31 (70) № 3 2020. С. 226–233.

84. Петрик В. М., Остроухов В. В. та ін. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навч. посіб. / В. М. Петрик, В. В. Остроухов; за ред. В. М. Петрика. — К.: Росава, 2006. — 208 с.

85. Перепелиця Г. Ми маємо сконцентруватися на зменшенні власної вразливості та подоланні власних вад. «Гібридна» війна Росії – виклик і загроза для Європи :Матеріали Центра Разумкова. К., грудень 2016. С. 17 – 19.

86. Пилипчук В. Г., Компанцева Л. Ф., Кудінов С. С., Доронін І. М., Дзьобань О. П., Акульшин О. В., Заруба О. Г.; за заг. ред. В. Г. Пилипчука: Становлення і розвиток системи стратегічних комунікацій сектору безпеки і оборони України: монографія – К. : ТОВ «Видавничий дім «АртЕк», 2018. – 272 с

87. Померанцев П. Нічого правдивого й усе можливо. Сходження до сучасної Росії. Видавництво : Yakaboo Publishing2020, 228 с.

88. Померанцев П. Це не пропаганда. Подорож на війну проти реальності. Видавництво : Yakaboo Publishing. 2020, 288 с.

89. Полтораков О. Гібридна війна в контексті асиметричного світоустрою. Гілея: науковий вісник. 2015. Вип. 100. С. 258 – 260.

90. Потій О., Семенченко А., Дубов Д., Бакалинський А., Мялковський Д. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. DOI: 10.18372/2410-7840.23.15434

91. Почепцов Г. Гібридна війна: інформаційна складова. «MediaSapiens». URL: http://osvita.mediasapiens.ua/trends/1411978127/gibridna_viyna_informatsiyna_skladova/.

92. Почепцов Г.Г. Інформаційні війни. Військо України. 2001. № 3–4. С. 20.

93. Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с.

94. Почепцов Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війнах. К.: 2016. Видавництво : Києво-Могилянська академія. 316 с.

95. Практичні аспекти стратегічного планування в умовах глобальних загроз національній безпеці та міжнародній стабільності: навч. посіб. / В. І. Абрамов, А. В. Дацюк, М. М. Шевченко та ін.; за заг. ред. Ю. В. Мельника, Л. М. Шипілової. Київ : НАДУ, 2018. 128 с.

96. Протидія когнітивній війні: інформованість і стійкість. Johns Hopkins University & Imperial College London.NATO Review. URL: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html.

97. Про інформацію. Закон України № 2657-XII від 2 жовтня 1992 року URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

98. Про національну безпеку України: Закон України № 2469-VIII від 21 червня 2018 року. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

99. Про основи національної безпеки України. *Відомості Верховної Ради України (ВВР),* 2003, № 39, ст.351. Закон України від 19 червня 2003 року № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text

100. Про Основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

101. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: Закон України від 9 січня 2007 року № 537-V. URL: http://zakon4.rada.gov.ua/laws/show/537-16

102. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України № 47/2017 від 25 лютого 2017 року. URL: https://www.president.gov.ua/documents/472017-21374

103. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України №685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

104. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України»: Указ Президента України №121/2021 України URL: https://www.president.gov.ua/documents/1212021-37661

105. Про рішення Ради національної безпеки і оборони України від 26 серпня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

106. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: розпорядження Кабінету міністрів України № 386-р від 15 травня 2013 р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text

107. Про телебачення та радіомовлення. Закон України № 3759-XII від 21 грудня 1993 року. URL: https://zakon.rada.gov.ua/laws/show/3759-12#Text

108. Про телекомунікації Закон України № 1280-IV від 18 листопада 2003 року URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text

109. Прохоренко І.Л. Національна безпека та баланс сил у світовій економіці: теорія і практика. Київ, 1993. 185 с.

110. Психологічні аспекти педагогічної практики в світлі наукових поглядів С. Л. Рубінштейна. URL: http://medbib.in.ua/psihologicheskie-aspektyi-pedagogicheskoy-38699.html

111. Психофізіологічне забезпечення професійного самоздійснення фахівця в умовах соціально-економічних перетворень: монографія / О.М. Кокун, В.В. Клименко, О.М. Корніяка [та ін.]; за ред. О.М. Кокуна. К.: Інститут психології імені Г.С. Костюка НАПН України, 2018. – 298 с.

112. Публічне управління та адміністрування у сфері національної безпеки: (системні, політичні та економічні аспекти): словник-довідник / С.П. Завгородня, М.Г. Орел, Г.П. Ситник [уклад.] / за заг.ред. Д.В. Неліпи, Є.О. Романенка, Г.П. Ситника. Київ : Видавець Кравченко Я.О., 2020. 380 с.

113. Пучков О. О. Інформаційна безпека у контексті сьогоднішніх реалій: філософський аспект. Гуманітарний вісник ЗДІА. 2015. № 60. С. 239–245.

114. Радковець Ю. Гібридна війна Росії проти України: уроки та висновки. «Укрінформ» URL: https://www.ukrinform.ua/rubric-politycs/2107122-gibridna-vijna-rosii-proti-ukraini-uroki-ta-visnovki.html.

115. Савченко-Галушко Т. Інформаційні та психологічні операції держави-агресора: як це працює. URL: https://armyinform.com.ua/2021/11/04/informaczijni-ta-psyhologichni-operacziyi-derzhavy-agresorayak-cze-praczyuye/

116. . Сафін О.Д. Індоктринація як інструмент гібридної війни Росії. *Вісник Київського національного університету ім. Тараса Шевченка. Військово-спеціальні науки*, 2017. №2(37). С. 24-27.

117. Северина С.В Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету.* 2016. No 1 (29). URL:: https://cutt.ly/IeVp2U8

118. Ситник Г.П., Орел М.Г. Публічне управління у сфері національної безпеки: підручник / за заг.ред. Г.П.Ситника. Київ : Видавець Кравченко Я.О., 2020, 360 с.

119. Ситник Г.П., Зубчик О.А, Орел М.Г., Штельмашенко А.Д. Політико-правове забезпечення публічного управління та адміністрування: підручник /за ред. Г.П.Ситника. Вінниця: ФОП Кушнір Ю.В.,ВПЦ, 2020. 504 с.

120. Розумний М. Національна доктрина. К.: Видавнича група УКМ-БУКС, 2021. 264 с.

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

122. Соснін О. В. Державна політика в галузі управління інформаційним ре- сурсом України : дис. на здоб. наук. ступеня доктора політ. наук : спец. 23.00.02. / Олександр Васильович Соснін ; Одес. нац. юрид. акад. – О., 2005. – 264 с.

123. Соціальна група // Універсальний словник-енциклопедія. 4-те вид. К. : Тека, 2006.

124. Соціально-правові основи інформаційної безпеки : [навч. посібник / за ред. В.В. Остроухова. К. : Росава, 2007. 496 с.

125. Стратегічні комунікації для безпекових і державних інституцій : практичний посібник / [Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин; за заг. ред. О. Давліканової, Л. Компанцевої]. Київ: Тов «Вістка», 2022. 278 с.

126. Стратегія розвитку штучного інтелекту в Україні: монографія / А. І. Шевченко, С. В. Барановський, О. В. Білокобильський, Є. В. Бодянський, А. Я. Бомба, та ін. [За заг. ред. А. І. Шевченка]. Київ: ІПШІ, 2023. 305 с.

127. Сучасний словник іншомовних слів : близько 20 тис. сл. і словосполучень / НАН України, Ін-т мовознав. ім. О. О. Потебні ; уклад.: О. І. Скопненко, Т. В. Цимбалюк. К. : Довіра, 2006. 789 с.

128. Татенко В. О. Психіка як проблема сучасної психологічної науки (аудіозапис наукової доповіді, 22.06.2017 р.

129. Ткачук Т. Ю. Забезпечення інформаційної безпеки в країнах Центральної Європи. *Юридичний науковий електронний журнал* №5. 2017. – URL: http://lsej.org.ua/5_2017/30.pdf

130. Ткачук Т. Інформаційна безпека держави в національному законодавстві країн ЄС. *Visegrad Journal on Human Rights* / volume 2. 2018. - URL: http://vjhr.sk/archive/2018_1/part_2/24.pdf

131. Толубко В.Б., Жук С.Я., Косевцов В.О. Концептуальні основи інформаційної безпеки України, *Наука і оборона.* № 2. 2004. С.18–22.

132. Трюхан В. «Гібридні» війни Росії – це засіб виживання сучасної російської держави. «Гібридна» війна Росії – виклик і загроза для Європи : Матеріали Центра Разумкова. К., грудень 2016. С. 10 – 12.

133. Турчак А. Реалізація національних механізмів протидії інформаційним загрозам URL: http://www.dridu.dp.ua/vidavnictvo/2019/2019_02(41)/12.pdf

134. Уханова Н.С. Інформаційно-психологічна безпека, особистості суспільства та держави. *Правова інформатика* 3(39). 2013. URL: https://ippi.org.ua/ukhanova-ns-informatsiino-psikhologichna-bezpeka-osobistosti-suspilstva-ta-derzhavi

135. Фесенко В. Якщо Захід і ЄС залишать Україну сам на сам з агресором, це лише розпалить агресивні інстинкти путінської Росії. «Гібридна» війна Росії – виклик і загроза для Європи : Матеріали Центра Разумкова. К., грудень 2016. С. 24 – 25.

136. Хайрулін, О. (2021). Інформаційно-психологічна безпека особистості в контексті мовної гри. *Вісник Національного університету оборони України*, 59(1), 189–208. https://doi.org/10.33099/2617-6858-2021-59-1-189-208.

137. Черненко Т. В. Пріоритети державної інформаційної політики в умовах гібридної війни. Стратегічні пріоритети. Серія «Політика» : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. досліджень. Київ : НІСД, 2015. № 4 (37). С. 83 – 92.

138. Шевченко М.М. Поняття «технологія державного реагування на загрози національній безпеці»: смисловий простір соціально-філософського змісту. Філософія науки: традиції та інновації: наук. журнал / відп. ред. В.О. Цикін. Суми: вид-во СумДПУ імені А.С. Макаренка, 2017. № 2 (16). С. 183-196.

139. Шишацький А. В., Башкиров О. М., Костина О. М. Розвиток інтегрованих систем зв’язку та передачі даних для потреб Збройних Сил. // Науково-технічний журнал “Озброєння та військова техніка”. 2015. № 1(5). С. 35 –40.

140. Що війна робить із медіа, що медіа роблять із нами. «Школа журналістики УКУ» URL: http://journalism.ucu.edu.ua/program-highlights/3550/.

141. «Щодо інформаційно-психологічної складової агресії Російської Федерації проти України (за результатами подій 1-2 березня 2014 року)»: аналітична записка // Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/1476/.

142. Юдін О. К., Богуш В. М. Інформаційна безпека держави: Навчальний посібник. - Харків:2005, Консум. 576с.

143. Andriy Datsyuk, Rena Marutyan, Yuriy Melnyk. Ukraine's national security political and legal support under democratic transition conditions. AD ALTA: Journal of Interdisciplinary Research volume 11, Issue 01. 2021. pp. 187-192. DOI (& full text) | .pdf. URL: www.doi.org/10.33543/1101 (Web of Science).

144. Andrii Datsiuk, Kateryna Nastoiashcha, Rena Marutian Trend of self-organization of the population in conditions of conflictogenic transformations of the world political system: challenges and prospects. AD ALTA: Journal of Interdisciplinary Research open journal. 2022. 12/01-XXV 224-227 pp. URL: http://www.magnanimitas.cz/ADALTA/120125/papers/A_40.pdf

145. Chan H. K., Sun X., Chung S.-H. When should fuzzy analytic hierarchy process be used instead of analytic hierarchy process? Decision Support Systems. 2019. pp. 1–37. DOI: https://doi.org/10.1016/j.dss.2019.113114.

146. Gödri, C. Kardos, A. Pfeiffer, J. Váncza. Data analytics-based decision support workflow for high-mix low-volume production systems. CIRP Annals. Vol. 68. Issu. 1. 2019. pp. 471–474. DOI: https://doi.org/10.1016/j.cirp.2019.04.001.

147. Chen H. Evaluation of Personalized Service Level for Library Information Management Based on Fuzzy Analytic Hierarchy Process. Procedia Computer Science. Vol. 131. 2018. pp. 952–958. DOI: https://doi.org/10.1016/j.procs.2018.04.233.

148. Dudnyk V., Sinenko Yu., Matsyk M., Demchenko Ye., Zhyvotovskyi R., Repilo Iu., Zabolotnyi O., Simonenko A., Pozdniakov P., Shyshatskyi A. Development of a method for training artificial neural networks for intelligent decision support systems. Eastern-European Journal of Enterprise Technologies. Vol. 3. No. 2 (105). 2020. pp. 37–47. DOI: https://doi.org/10.15587/1729-4061.2020.203301.

149. Elizabeth Kennedy Trudeau Комплексний і узгоджений підхід до стратегічної комунікації. URL: https://www.nato.int/docu/review/uk/articles/2023/03/16/kompleksnij-uzgodyoenij-pdhd-do-strategchno-komunkats/index.html

150. Harding L. Data quality in the integration and analysis of data from multiple sources: some research challenges. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Vol. XL-2/W1. 2013. pp. 59–63. DOI: 10.5194/isprsarchives-XL-2-W1-59-2013.

151. Hasebrink, U., Livingstone, S., Haddon, L. And Ólafsson K. Comparing children's online opportunities and risks across Europe. Cross-national comparisons for EU Kids Online. LSE, London: EU Kids Online, 2009.

152. Illegal content //INHOPE. URL: http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegalcontent.aspx (дата обращения: 26.09.2022)]

153. Kharkiv Security 1 Смислова війна РФ проти України інструменти засоби досвід протидії. Юлія Лапутіна. URL: https://www.youtube.com/watch?v=-ea24JCTjzY

154. Online World As Important to Internet Users as Real World?- http://www.digitalcenter.org/pdf/2007-Digital-FutureReport-Press-Release 112906.pdf. – Center for the digital future. США.

155. Orouskhani, M., Orouskhani, Y., Mansouri, M., Teshnehlab, M. A novel cat swarm optimization algorithm for unconstrained optimization problems, International Journal "Imformation Technology and Computer Science", 2013, Vol. 11, pp. 32 − 41.

156. Osman M. S.. A novel big data analytics framework for smart cities. Future Generation Computer Systems. 2019. Vol. 91. pp. 620–633. DOI: https://doi.org/10.1016/j.future.2018.06.046.

157. Pérez-González C. J., Colebrook M., Roda-García J. L., Rosa-Remedios C. B. Developing a data analytics platform to support decision making in emergency and security management. Expert Systems with Applications. 2019. Vol. 120. pp. 167–184. DOI: https://doi.org/10.1016/j.eswa.2018.11.023.

158. Pievtsov, H., Turinskyi, O., Zhyvotovskyi , R., Sova , O., Zvieriev, O., Lanetskii , B., and Shyshatskyi , A. (2020). Development of an advanced method of finding solutions for neuro-fuzzy expert systems of analysis of the radioelectronic situation. EUREKA: Physics and Engineering, No. (4), pp. 78-89. https://doi.org/10.21303/2461-4262.2020.001353.

159. Ramaji J., Memari A. M.. Interpretation of structural analytical models from the coordination view in building information models. Automation in Construction. 2018. Vol. 90. pp. 117–133. DOI: https://doi.org/10.1016/j.autcon.2018.02.025.

160. Rena Marutian, Oleksii Poltorakov, John Callahan, “The Tanks of Post-truth:” Post-truth Hybrid Warfare Operations. Studia Politica. Romanian Political Science Review, vol. XXI, no. 1, 2021. pp.101-120. https://www.studiapolitica.eu/

161. Security // Department of Defense Dictionary of Military and Associated Terms. As of December 2020 // Joint Chiefs of Staff. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (дата звернення: 01.02.2022).].

162. Shyshatskyi, O. Zvieriev, O. Salnikova, Ye. Demchenko, O. Trotsko, Ye. Neroznak. Complex Methods of Processing Different Data in Intellectual Systems for Decision Support System. International Journal of Advanced Trends in Computer Science and Engineering. Vol. 9, No. 4, pp. 5583–5590 DOI: https://doi.org/10.30534/ijatcse/2020/206942020.

163. Sova, O., Shyshatskyi, A., Salnikova, O., Zhuk, O., Trotsko, O., & Hrokholskyi, Y. Development of a method for assessment and forecasting of the radio electronic environment. EUREKA: Physics and Engineering, 2021, No. 4, pp. 30-40. https://doi.org/10.21303/2461-4262.2021.001940.

164. Zuiev P., Zhyvotovskyi R., Zvieriev O., Hatsenko S., Kuprii V., Nakonechnyi O., Adamenko M., Shyshatskyi A., Neroznak Y., Velychko V. Development of complex methodology of processing heterogeneous data in intelligent decision support systems. Eastern-European Journal of Enterprise Technologies. 2020, Vol. 4, No. 9 (106), pp. 14–23. DOI: https://doi.org/10.15587/1729-4061.2020.208554.

165. «Fayol, Henri», «Патронс де Франс» (французькою мовою) , відновлено 2 серпня 2017 р.

166. World Factbook – http://cia.gov – Веб-сайт Центрального розвідувального управління США.

167. Yeromina N., Kurban V., Mykus S., Peredrii O., Voloshchenko O., Kosenko V., Kuzavkov V., Babeliuk O., Derevianko M. and Kovalov H.. The Creation of the Database for Mobile Robots Navigation under the Conditions of Flexible Change of Flight Assignment. International Journal of Emerging Technology and Advanced Engineering. 2021. Vol. 11, Iss. 05., pp. 37. –41. https://doi.org/10.46338/ijetae0521_05.

Додаток А

Прокуратура України
КИЇВСЬКА ОБЛАСНА ПРОКУРАТУРА
б-р. Лесі Українки, 27/2, м. Київ, 01601 факс: (044) 286-16-48
e-mail: prok@kobl.gp.gov.ua, web: kobl.gp.gov.ua
Код ЄДРПОУ 02909996

12.09.2022 № 09/1/1-498 вих.22 На №_____ від _____

ДОВІДКА ПРО ВПРОВАДЖЕННЯ

Результати дисертаційного дослідження аспіранта кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка Канарського Володимира Сергійовича на тему «Публічно-управлінські механізми забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни» на здобуття наукового ступеня доктор філософії за спеціальністю «Публічне управління та адміністрування», мають практичну значимість та використані в роботі відділу нагляду за додержанням законів органами Служби безпеки України та Державної прикордонної служби Київської обласної прокуратури.

Заступник керівника
Київської обласної прокуратури,
кандидат юридичних наук **Олег ТКАЛЕНКО**

Додаток Б

ДОВІДКА

про впровадження результатів дисертаційного дослідження аспіранта кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка Канарського Володимира Сергійовича на тему: «Публічно-управлінські механізми забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни» на здобуття наукового ступеня доктора філософії за спеціальністю «Публічне управління та адміністрування»

У Комітеті з питань гуманітарної та інформаційної політики розглянуто результати дисертації та встановлено можливості застосування авторської концепції публічно-управлінських механізмів забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни у законотворчій діяльності та прийнятті управлінських рішень Верховної Ради України.

Відтак, з метою забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни вважаємо, що висновки і пропозиції Канарського В.С. можуть бути використані Комітетом при підготовці та організації засідань, комітетських слухань, круглих столів щодо питань інформаційної політики.

Автор надав пропозиції щодо вдосконалення організаційно-правових механізмів реагування на загрози інформаційно-психологічної безпеки України.

Теоретичні гіпотези та практичні рекомендації дисертаційної роботи Канарського В.С. на тему «Публічно-управлінські механізми забезпечення інформаційно-психологічної безпеки України в умовах гібридної війни» науково доведені та заслуговують використання у законопроектній роботі Комітету.

Голова Комітету Верховної Ради України
з питань гуманітарної та інформаційної
політики Потураєв М.Р.

Підпис Потураєва М.Р.
підтверджую
Гол. конс. відділу О. Марія Марченко
Управління кадрів
Апарату Верховної Ради України
«08» вересня 2022 р.

Додаток В

ПРОЕКТ

Основні положення

Концепції інформаційно-психологічної безпеки України

І. Загальні положення

1. Ця Концепція є системою поглядів на забезпечення інформаційно-психологічної безпеки як частини інформаційної та національної безпеки України.

2. Цією Концепцією визначаються основні загрози інформаційно-психологічній безпеці України, цілі, завдання, принципи та основні напрямки діяльності уповноважених органів публічної влади, організацій та інших суб'єктів, що беруть участь у забезпеченні інформаційно-психологічної безпеки на основі законодавства України.

3. Правову основу цієї Концепції складають Конституція України, Закон України «Про національну безпеку», Стратегія національної безпеки України, Доктрина інформаційної безпеки України, Стратегія інформаційної безпеки України, інші нормативно-правові акти України, що визначають напрямки застосування інформаційних та комунікаційних технологій в Україні.

4. Ця Концепція є основним документом стратегічного планування, що визначає державну політику у сфері забезпечення інформаційно-психологічної безпеки, а також основою для конструктивної взаємодії у цій сфері органів публічної влади та інститутів громадянського суспільства, громадян України, іноземних громадян та осіб без громадянства.

5. Забезпечення інформаційної безпеки один із стратегічних національних пріоритетів. Інформаційно-психологічна безпека є складовою системи інформаційної безпеки і є станом захищеності особистості, соціальних груп і суспільства від деструктивного інформаційно-психологічного впливу.

6. Україна при забезпеченні інформаційно-психологічної безпеки на довгострокову перспективу виходить із необхідності постійного вдосконалення системи забезпечення інформаційно-психологічної безпеки, а також політичних, організаційних, соціально-економічних, інформаційних, правових та інших заходів:

а) щодо здійснення моніторингу інформаційного простору, виявлення, прогнозування та оцінки загроз інформаційно-психологічній безпеці;

б) щодо розробки та застосування комплексу оперативних та довготривалих заходів з метою запобігання та усунення загроз інформаційно-психологічній безпеці, їх локалізації та нейтралізації наслідків їх прояву;

в) зі створення інформаційного середовища довіри, підвищення рівня цифрової грамотності та формування культури інформаційної безпеки;

г) щодо розвитку приватно-державного партнерства та міжнародного співробітництва в галузі забезпечення інформаційно-психологічної безпеки.

7. Для цілей цієї Концепції використовуються такі основні поняття:

а) забезпечення інформаційно-психологічної безпеки - діяльність з вироблення та реалізації системи правових, організаційних, інформаційних та інших заходів, спрямованих на забезпечення захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу;

б) загроза інформаційно-психологічної безпеки - фактор або сукупність факторів, здатних завдати шкоди інтересам особистості, суспільства і держави за допомогою деструктивного інформаційно-психологічного впливу;

в) деструктивний інформаційно-психологічний вплив - негативний вплив на особистість, соціальні групи та суспільство, шляхом поширення деструктивної інформації або комунікації, а також сигналів від технічних пристроїв, що дистанційно впливають на психіку людини через зорові та слухові сенсорні системи, що створює небезпеку заподіяння шкоди інтересам особистості, суспільства та держави;

г) система забезпечення інформаційно-психологічної безпеки - сукупність сил забезпечення інформаційно-психологічної безпеки, що здійснюють скоординовану та сплановану діяльність, та використовуваних ними засобів забезпечення інформаційно-психологічної безпеки, а також правових норм, що регулюють суспільні відносини у сфері забезпечення інформаційно-психологічної безпеки;

д) сили забезпечення інформаційно-психологічної безпеки - державні органи, а також підрозділи та посадові особи державних органів, органів місцевого самоврядування та організацій, уповноважені на вирішення відповідно до законодавства України завдань щодо забезпечення інформаційно-психологічної безпеки;

е) засоби забезпечення інформаційної безпеки – правові, організаційні, технічні та інші засоби, що використовуються силами забезпечення інформаційно-психологічної безпеки;

ж) правове забезпечення інформаційно-психологічної безпеки - діяльність з розробки та реалізації системи правових засобів, спрямованих на забезпечення захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу.

II. Основні загрози інформаційно-психологічній безпеці

8.Стрімкий розвиток інформаційно-комунікаційних технологій супроводжується зростанням загроз безпеці, пов'язаних з наданням деструктивного інформаційно-психологічного впливу на особистість, соціальні групи та суспільством загалом.

Розширюється використання інформаційно-комунікаційних технологій для втручання у внутрішні справи держав, підриву їх суверенітету та порушення територіальної цілісності, що становить загрозу міжнародному миру та безпеці. Активізується діяльність спеціальних служб рф щодо

проведення інформаційно-психологічних операцій в українському інформаційному просторі.

9. З метою дестабілізації суспільно-політичної ситуації в Україні поширюється недостовірна суспільно значуща інформація, у тому числі свідомо неправдиві інформація з викривлення національної історії та національної пам'яті. Новий потенціал для дезінформації відкривають технології штучного інтелекту, зокрема, що дозволяють створювати високоякісні підробки зображення та голосу людини (діпфейк).

10. Російські засоби масової інформації та журналісти ситематино здійснюють дезінформацію про події російсько-української війни та суспільно-політичне життя в Україні на міжнародній арені, що грубо суперечить міжнародно-правовим стандартам свободи масової інформації та демократії. Українське населення на окупованих рф територіях позбавлене можливості отримувати український національний інформаційний продукт та знаходиться під впливом російських ІПСО.

11. Домінування транснаціональних корпорацій в інтернет-секторі створює ризики збору великого масиву персональних даних про українських користувачів та його застосування для надання таргетованого деструктивного інформаційно-психологічного впливу на окремих людей та соціальні групи. 12. Підходи до модерації контенту, що використовуються даними корпораціями, створюють ризики широкого поширення в мережі Інтернет протиправної інформації, формування спотвореної картини подій, що відбуваються в Україні та світі, нав'язування негативних установок і ціннісних орієнтацій при одночасному блокуванні можливості донесення альтернативних відомостей. При цьому ними систематично ігноруються законні вимоги української влади про видалення або обмеження доступу до протиправного контенту, вживання інших заходів щодо забезпечення інформаційно-психологічної безпеки.

13. Фактор анонімності у цифровому середовищі сприяє широкому поширенню негативного контенту та веденню деструктивних комунікацій, полегшує скоєння злочинів та інших протиправних дій. В особистісному плані відчуття анонімності обумовлює зняття низки психологічних бар'єрів у спілкуванні та поведінці людини в інформаційному просторі, що сприяє виявленню ним своїх деструктивних нахилів та інтересів.

14. Зростають масштаби шахрайств, крадіжок та інших злочинів, скоєних з використанням інформаційно-комунікаційних технологій та прийомів соціальної інженерії. При цьому способи та засоби скоєння таких злочинів стають дедалі витонченішими.

15. Широке поширення в цифровому середовищі набули деструктивні молодіжні субкультури, що містять негативні ідеї, ціннісні та поведінкові настанови та норми. Їхнє просування здійснюється через численні спільноти та канали в соціальних мережах і месенджерах, у тому числі за сприяння спецслужб іноземних держав. Особливу небезпеку становлять деструктивні субкультури, які провокують скоєння масових вбивств та застосування інших актів насильства, а також суїцидів та інших форм аутодеструктивної поведінки підлітків.

16. Негативний вплив на психіку надають різні види мовної агресії та іншої деструктивної комунікації в соціальних мережах та месенджерах, включаючи висміювання (тролінг), цькування в мережі (булінг), доведення до самогубства (булліцид) та ін. Можливості Інтернету також активно використовуються для відмінювання та іншого залучення дітей та молоді до терористичної та екстремістської діяльності, скоєння злочинів, вживання та розповсюдження наркотиків, інших антигромадських дій чи дій, що становлять небезпеку для життя неповнолітнього.

17. Джерелом загроз інформаційно-психологічній безпеці також виступають комерційні компанії, які використовують поєднання просунутих методів маніпуляції свідомістю споживачів та аналізу їхньої індивідуальної мережевої активності для агресивного просування своїх товарів та послуг.

18. Ризики заподіяння шкоди психічному та фізичному здоров'ю громадян несуть численні «мережеві проповідники» та «вчителі», які розповсюджують сумнівні, а іноді й відверто помилкові знання щодо здорового способу життя, профілактики та лікування захворювань, особистісного зростання, вчинення юридично значимих дій тощо. У період пандемії нової коронавірусної інфекції масове поширення спотвореної та фальсифікованої інформації про захворювання, методи його попередження та лікування суттєво знижують ефективність діяльності національних систем охорони здоров'я та біологічної безпеки.

19. Джерелом загроз інформаційно-психологічній безпеці для дітей та інших вразливих категорій населення є комп'ютерні ігри, що містять натуралістичні сцени жорсткого насильства, садизму, порнографії, що навчають споживання наркотиків, виготовлення та застосування в реальному житті зброї та вибухових пристроїв, скоєння терористичних та інших насильств, а також самогубств та інших аутодеструктивних дій. Особливу небезпеку становлять ігри альтернативної реальності, що передбачають виконання небезпечних ігрових завдань в офлайні.

20. Нові горизонти для деструктивного інформаційно-психологічного впливу на людей та соціальні групи відкривають системи віртуальної та доповненої реальності, що використовують різні сенсорні канали та створюють глибокий ефект занурення. Ставка великих технологічних компаній на формований розвиток «метавсесвітів» дозволяє прогнозувати їх швидку появу та активне «занурення» в них населення, що створює комплекс нових ризиків та викликів.

21. Значним чинником уразливості для деструктивного інформаційно-психологічного впливу виступає низький рівень медійної та цифрової грамотності населення та культури інформаційної безпеки. Наголошується на суспільному запиті на посилення інформаційно-просвітницької та освітньої діяльності в даній сфері, особливо серед дітей та інших уразливих верств населення.

III. Національні інтереси в інформаційній сфері

22. Розвиток глобального інформаційного суспільства та процесів цифрової трансформації впливає на всі сфери суспільного життя та міжнародні відносини. Інформаційно-комунікаційні технології стають потужним каталізатором соціального прогресу та одночасно генератором нових викликів та загроз. Інформаційна сфера грає ключову роль забезпеченні реалізації стратегічних національних пріоритетів України.

23. Національними інтересами в інформаційній сфері (у частині забезпечення інформаційно-психологічної безпеки) є:

а) забезпечення та захист конституційних прав і свобод людини та громадянина, включаючи право на свободу, недоторканність приватного життя, захист своєї честі та доброго імені, свободу думки та слова, право на інформацію та свободу масової інформації;

б) формування середовища довіри у цифровому середовищі;

в) забезпечення доступу до інформації, що сприяє розвитку особистості та суспільства;

г) захист особистості, соціальних груп та суспільства загалом від деструктивного інформаційно-психологічного впливу;

д) гарантування психічного здоров'я та благополуччя громадян;

е) збереження традиційних національних цінностей та національної ідентичності українського суспільства, підвищення культурного потенціалу країни;

ж) зміцнення національної згоди, політичної та соціальної стабільності;

з) забезпечення інформаційного суверенітету України;

і) поліпшення іміджу України та підвищення її авторитету на міжнародній арені, посилення політичного та культурного впливу України у світі;

к) сприяння формуванню системи міжнародної інформаційної безпеки, спрямованої на протидію загрозам деструктивного ІПВ на особистість, соціальні групи та суспільство.

24. Реалізація національних інтересів в інформаційній сфері спрямована на формування безпечного середовища обігу достовірної інформації, створення умов для реалізації прав і свобод людини та громадянина, стабільного соціально-економічного розвитку країни та забезпечення її національної безпеки.

IV. Цілі, завдання та принципи забезпечення інформаційно - психологічної безпеки

25. Стратегічною метою забезпечення інформаційно-психологічної безпеки виступає підтримання стану захищеності особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу, що забезпечує гарантовану реалізацію національних інтересів України.

26. Основними об'єктами деструктивного інформаційно-психологічного впливу є:

- особистість, великі та малі соціальні групи, суспільство загалом;

- психіка людини, що включає свідомість і несвідоме, і групові психічні структури, які з групового (суспільного) свідомості людини та колективного несвідомого;

- індивідуальні та групові психічні процеси (сприйняття, пам'ять, мислення, мотивація тощо) та психічні освіти (образи, емоції, цілі, установки, архетипи тощо).

Пріоритетним об'єктом правового захисту від деструктивного інформаційно-психологічного на мікросоціальному рівні виступають діти.

27. Завданнями забезпечення інформаційно-психологічної безпеки є:

а) прогнозування, виявлення, аналіз та оцінка загроз інформаційно-психологічної безпеки;

б) аналіз та оцінка вразливості особистості, соціальних груп та суспільства від деструктивного інформаційно-психологічного впливу;

в) стратегічне планування у сфері забезпечення інформаційно-психологічної безпеки;

г) правове регулювання відносин у сфері забезпечення інформаційно-психологічної безпеки;

д) застосування комплексу оперативних та довготривалих заходів щодо профілактики, попередження, припинення та усунення загроз інформаційно-психологічній безпеці, мінімізації та (або) ліквідації наслідків їх впливу;

е) застосування комплексу оперативних та довготривалих заходів щодо підвищення здатності особистості, соціальних груп та суспільства протистояти деструктивному інформаційно-психологічному впливу;

ж) організація діяльності системи забезпечення інформаційно-психологічної безпеки;

з) кадрове, інформаційне, матеріально-технічне та фінансове забезпечення діяльності суб'єктів забезпечення інформаційно-психологічної безпеки;

і) міжнародне співробітництво в галузі забезпечення інформаційно-психологічної безпеки.

28. Діяльність із забезпечення інформаційно-психологічної безпеки здійснюється на основі наступних принципів:

а) дотримання права і свободи людини і громадянина;

б) гарантування свободи масової інформації та заборона цензури;

в) законність;

г) допустимість обмеження права і свободи людини і громадянина з метою захисту основ конституційного ладу, моральності, здоров'я, правий і законних інтересів інших, забезпечення оборони держави й безпеки держави;

д) суверенітет України у інформаційному просторі;

е) створення умов, що сприяють всебічному духовному, моральному, інтелектуальному та фізичному розвитку дітей, вихованню в них патріотизму, громадянськості та поваги до старших;

ж) охорона історичної пам'яті та захист історичної правди;

з) системність та комплексність застосування правових, організаційних, інформаційних та інших заходів забезпечення інформаційно-психологічної безпеки;

і) пріоритет запобіжних заходів забезпечення інформаційно-психологічної безпеки;

к) приватно-державне партнерство та міжнародне співробітництво у забезпеченні інформаційно-психологічної безпеки.

V. Основні напрямки діяльності із забезпечення громадської безпеки

29. Діяльність щодо забезпечення інформаційно-психологічної безпеки включає:

а) протидія джерелам загроз інформаційно-психологічній безпеці;

б) блокування чи послаблення деструктивного інформаційно-психологічного впливу загроз на об'єкти інформаційно-психологічної безпеки, включаючи ліквідацію (мінімізацію) його наслідків;

в) підвищення життєстійкості об'єктів інформаційно-психологічної безпеки;

г) вплив на фактори зовнішнього інформаційного середовища.

30. Основними напрямками діяльності з вироблення та реалізації державної політики забезпечення інформаційно-психологічної безпеки є:

а) стратегічне планування у сфері забезпечення інформаційно-психологічної безпеки;

б) правове регулювання у сфері забезпечення інформаційно-психологічної безпеки;

в) здійснення державного контролю (нагляду) у сфері забезпечення інформаційно-психологічної безпеки;

г) надання державних послуг у сфері забезпечення інформаційно-психологічної безпеки;

д) координація діяльності суб'єктів забезпечення інформаційно-психологічної безпеки;

е) організація матеріально-технічного, фінансового та інформаційного забезпечення діяльності суб'єктів забезпечення інформаційно-психологічної безпеки;

ж) проведення наукових досліджень у галузі забезпечення інформаційно-психологічної безпеки;

з) підготовка кадрів у сфері забезпечення інформаційно-психологічної безпеки;

і) здійснення міжнародного співробітництва у сфері інформаційно-психологічної безпеки.

31. Основними напрямками діяльності щодо безпосереднього забезпечення інформаційно-психологічної безпеки виступають:

а) прогнозування, виявлення, аналіз та оцінка загроз інформаційно-психологічної безпеки;

б) протидія поширенню негативної інформації у засобах масової інформації та мережі Інтернет;

в) протидія терористичній і екстремістській пропаганді та вербувальній діяльності, розпалюванню національної, расової, релігійної чи соціальної ненависті та ворожнечі;

г) протидія деструктивному інформаційно-психологічному впливу з боку державних органів та спеціальних служб іноземних держав, іноземних та міжнародних організацій;

д) забезпечення інформаційно-психологічної безпеки дітей;

е) захист честі, гідності та ділової репутації громадянина, ділової репутації юридичної особи;

ж) захист органів державної влади, посадових осіб від деструктивного інформаційно-психологічного впливу;

з) протидія фальсифікації вітчизняної та світової історії на шкоду інтересам України;

і) протидія розповсюдженню деструктивних субкультур та інших форм негативного інформаційно-психологічного впливу у духовній сфері;

к) протидія злочинам та адміністративним правопорушенням, пов'язаним з наданням деструктивного інформаційно-психологічного впливу;

л) інформування зарубіжної громадськості про внутрішню та зовнішню політику України, її офіційну позицію щодо соціально значущих подій;

м) ведення контрпропаганди в Україні та закордоном;

н) формування цифрової грамотності громадян та культури інформаційної безпеки.

VI. Організаційні засади забезпечення інформаційно-психологічної безпеки

32. Система забезпечення інформаційно-психологічної безпеки є частиною системи забезпечення інформаційної та національної безпеки України.

Забезпечення інформаційно-психологічної безпеки здійснюється на основі поєднання законодавчої, правозастосовчої, правоохоронної, судової, контрольної та інших форм діяльності державних органів у взаємодії з органами місцевого самоврядування, організаціями та громадянами.

33. Система забезпечення інформаційно-психологічної безпеки будується на основі розмежування повноважень органів законодавчої, виконавчої та судової влади у цій сфері з урахуванням функцій та повноважень органів державної влади, а також органів місцевого самоврядування, що визначаються законодавством України у сфері забезпечення національної безпеки.

34. Склад системи забезпечення інформаційно-психологічної безпеки визначається Президентом України.

35. Організаційну основу системи забезпечення інформаційно-психологічної безпеки становлять: Верховна Рада України, Рада національної безпеки та оборони України, Кабінет міністрів України, органи виконавчої влади, Офіс Генерального прокурора, Національний банк України, міжвідомчі органи, органі, які спеціально створені Президентом України та Кабінетом міністрів України, органи місцевого самоврядування, органи судової влади, які беруть відповідно до законодавства України участь у вирішенні завдань щодо забезпечення інформаційно-психологічної безпеки.

Учасниками системи забезпечення інформаційно-психологічної безпеки є: засоби масової інформації та масових комунікацій, оператори зв'язку, оператори інформаційних систем та інші інформаційні посередники, організації, які здійснюють діяльність зі створення та експлуатації інформаційних систем та мереж зв'язку, розроблення, виробництва та експлуатації засобів забезпечення інформаційної безпеки, надання послуг у галузі забезпечення інформаційної безпеки, організації, що здійснюють освітню діяльність у цій галузі, громадські об'єднання, інші організації та громадяни, які відповідно до законодавства України беруть участь у вирішенні завдань щодо забезпечення інформаційно-психологічної безпеки.

36. З метою прогнозування, моніторингу та контролю ситуації в сфері інформаційно-психологічної безпеки та координації діяльності органів публічної влади та недержавних учасників системи забезпечення інформаційно-психологічної безпеки створюється державна система реагування на інформаційно-психологічні загрози, що є єдиним централізованим комплексом, що включає сили та засоби виявлення, попередження, нейтралізації та ліквідації наслідків впливу інформаційно-психологічних загроз. Положення про державну систему реагування на інформаційно-психологічні загрози затверджується Президентом України.

37. Реалізація цієї Концепції складається на основі галузевих документів стратегічного планування України. З метою актуалізації таких документів Радою національної безпеки та оборони України визначається перелік пріоритетних напрямів забезпечення інформаційно-психологічної безпеки на середньострокову перспективу.

38. Результати моніторингу реалізації цієї Концепції відображаються в щорічній доповіді Секретаря Ради національної безпеки та оборони України про стан національної безпеки та заходи щодо її зміцнення.

Додаток Г

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

1. Канарський В. С. Інформаційні загрози як головний фактор розгортання «гібридної війни». *Електронне наукове видання "Публічне адміністрування та національна безпека"*. 2022. №2. URL: https://doi.org/10.25313/2617-572X-2022-2-7926

2. Канарський В. С. Рекомендації щодо удосконалення нормативно-правових механізмів державної політики у сфері інформаційної безпеки України. *Наукові інновації та передові технології (серія «Державне управління»*). №10(12), 2022. DOI: https://doi.org/10.52058/2786-5274-2022-10(12)-63-75

3. Канарський В. С. Політико-правовий механізм державного управління інформаційно-психологічною безпекою України: сутність, функції та повноваження. *Наукові перспективи*, Випуск №9(15). 2021. С.99-110.

4. Канарський В. Аналітичний огляд джерел та наукової літератури з публічного управління інформаційно-психологічною безпекою України. *Актуальні питання у сучасній науці (Серія «Державне управління»).* Випуск № 6(12) 2023. С. 210-224

Праці, які додатково відображають наукові результати дисертації

1. Канарський В.С. Пріоритети державної політики інформаційної безпеки України: Збірник тез наукових доповідей XII Всеукр. наук.-практ. конф. “Актуальні проблеми управління інформаційною безпекою” (Київ: Національна академія СБУ, 26 березня 2021 р.), С.275-276.

2. Канарський В.С. Механізми оптимізації державного управління забезпеченням інформаційної безпеки в Україні. 30 років незалежності України: досягнення, виклики, перспективи : матеріали міжнар. наук.практ. конф. (Київ, 10 верес. 2021 р.) / за заг. ред. Л. Г. Комахи, О. М. Андрєєвої, В. А. Гошовської. Київ : ННІ ПУДС КНУ, 2021. С.178-179.

3. Канарський В.С. Пропозиції щодо вдосконалення організаційно-правових механізмів реагування на загрози інформаційно-психологічної безпеки України. Шевченківська весна – 2022: публічне управління та державна служба : матеріали

міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених (Київ, 19 квіт. 2022 р.) / за заг. ред. Л. Г. Комахи, О. М. Андрєєвої. Київ : ННІ ПУДС КНУ, 2022 С.103-104.

4. Канарський В. Пріоритетні напрями вдосконалення державної політики інформаційної безпеки в умовах протидії гуманітарної експансії рф проти України. Глобалізаційні виклики: урядування майбутнього : матеріали міжнар. наук.-практ. конф. (Київ, 7–8 черв. 2022 р.) / за заг. ред. Л. Г. Комахи. Київ : ННІ ПУДС КНУ імені Тараса Шевченка, 2022.С.199-201.

5. Канарський В. Публічно-управлінські механізми протидії інформаційним загрозам: європейський досвід. Україна 2030: публічне управління для сталого розвитку : матеріали щоріч. міжнар. наук.-практ. конф. (Київ, 2020 р.) : у 3 т. / за заг. ред. А. П. Савкова, М. М. Білинської, О. М. Петроє. Київ : НАДУ, 2020. С.32-33.