КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА МОН УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ЖИВОТОВА КСЕНІЯ ВІКТОРІВНА

УДК 351.74:004.8:659.2

ДИСЕРТАЦІЯ

МЕХАНІЗМИ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

Спеціальність 281 «Публічне управління та адміністрування»
Галузь знань 28 «Публічне управління та адміністрування»

Подається на здобуття ступеня доктора філософії

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

Науковий керівник – Карпенко Олександр Валентинович,
доктор наук з державного управління, професор

Київ – 2024

АНОТАЦІЯ

Животова К. В. Механізми вироблення державної політики у сфері протидії дезінформації. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування». – Київський національний економічний університет імені Вадима Гетьмана, Київ, 2024.

У дисертаційній роботі здійснено теоретичне обґрунтування механізмів вироблення державної політики у сфері протидії дезінформації та надано практичні рекомендації щодо їх вдосконалення в умовах цифровізації публічного управління.

Наукова новизна одержаних результатів полягає в теоретичному обґрунтуванні механізмів вироблення державної політики у сфері протидії дезінформації та наданні практичних рекомендацій щодо їх вдосконалення в умовах цифровізації публічного управління.

Уперше розроблено модель інституціонального механізму вироблення державної політики у сфері протидії дезінформації на стратегічному, тактичному та операційному рівнях для забезпечення реагування підрозділів органів влади на маніпулятивні та фальсифікативні загрози, що базується на взаємодії суб'єктів публічного управління (стратегічних, регуляторних, комунікативних, гуманітарних, юридичних, наукових) у процесі реалізації комплексу організаційно-функціональних заходів згідно зон їх відповідальності на основі: *факторів* (політичний контекст; інформаційна культура; технологічний розвиток; роль громадянського суспільства; вплив медіа; міжнародна співпраця; фінансові ресурси; стратегічне партнерство); *стратегій* (реалізації заходів захисту; здійснення моніторингу, аналізу та оцінювання ризиків; реагування та здійснення контрдій); *принципів* (комунікативності, захищеності, координованості, доказовості, прозорості,

відкритості, задіяності та адаптивності); *методів/засобів збору та поширення контенту* (моніторингу медіа та соціальних мереж; аналітичних інструментів; експертної оцінки; публічних кампаній; спеціальних комісій та агентств; міжнародного співробітництва; законодавчих ініціатив); *інструментів реагування на загрози* (стратегічне планування; аналітичні дослідження; нормативне регулювання; інформаційний моніторинг; освітні програми; партнерська співпраця; інформаційна мобілізація; координаційні заходи); *співпраці* (формування спеціалізованих робочих груп та комітетів; проведення регулярних нарад; здійснення обміну інформацією; створення спільних програм і проєктів; здійснення кризової координації; розробка спільних стратегій) та *партнерської взаємодії* (залучення партнерських програм з громадянським суспільством та міжнародних проєктів; застосування публічно-приватного партнерства; проведення консультацій з експертами; організація форумів та робочих група); *ресурсів* (фінансових, людських і технічних).

Запропоновано шляхи розвитку інституціонального механізму вироблення державної політики у сфері протидії дезінформації, зокрема:

– поліпшення координації дій між Центром протидії дезінформації при РНБО України і профільними органами державної влади та іншими зацікавленими суб’єктами публічного управління;

– оптимізація використання фінансових, людських і технічних ресурсів із залученням партнерської взаємодії з громадськими організаціями, приватним сектором та міжнародними партнерами для спільної реалізації проектів і програм;

– оновлення нормативно-правової бази з урахуванням сучасних викликів, загроз, ризиків та впливу цифрових технологій у сфері протидії дезінформації;

– забезпечення широкого доступу громадськості до достовірної інформації та підвищення інформаційної грамотності населення.

Удосконалено кваліфікуючі критерії, за якими недостовірна інформація визначається дезінформацією, а саме: недостовірний зміст, який суперечить об’єктивній реальності; навмисно вигадані або спотворені дані з метою введення в оману; цілеспрямоване поширення контенту з метою виникнення певних наслідків; вплив на суспільну свідомість та громадську думку, включаючи здатність спричиняти хаос, дестабілізацію, викликати паніку, підважити довіру до державних інституцій або інших суб’єктів публічного управління.

Також удосконалено практичні підходи щодо застосування державних механізмів протидії швидкому поширенню дезінформації шляхом: забезпечення досягнення балансу між індивідуальними інформаційними свободами та захистом національних інтересів держави, зокрема врегулювання діяльності анонімних онлайн-ресурсів для припинення системного та безкарного поширення недостовірної та маніпулятивної інформації в інтернет-просторі, спрямованої проти національних інтересів України; формування належної правової бази ефективного захисту від загроз в інформаційному просторі; створення інтегрованої системи раннього виявлення загроз за допомогою технологій штучного інтелекту, машинного навчання, аналізу даних та цифрових сервісів; налагодження співпраці та обміну інформацією між різними суб'єктами інформаційної безпеки.

Окрім того, удосконалено методику визначення факторів, що впливають на результативність протидії впливу дезінформації, яка поширюється комунікативними каналами у публічній сфері, що складається з аналізу соціальних мереж; моніторингу засобів масової інформації, опитування та анкетування, а також вивчення поведінки цільових груп; аналізу трафіку інформаційних ресурсів; застосування інструментарію інформаційно-аналітичних систем; інтерв’ювання експертів та представників громадських організацій; дослідження цільової

аудиторії та її взаємодії з медіа-контентом; використання кількісних та якісних методів аналізу даних.

В роботі набув подальшого розвитку алгоритм протидії дезінформації з урахуванням умов розвитку цифрових трансформацій, який складається з п’яти основних етапів: визначення потенційних загроз та вироблення стратегії державної політики протидії дезінформації; захист від поточних загроз шляхом впровадження механізмів фільтрації та перевірки інформації, підвищення інформаційної грамотності та вдосконалення заходів захисту від кібератак; виявлення дезінформаційних інцидентів в режимі реального часу; оперативне та ефективне реагування на такі інциденти; здійснення заходів з відновлення стабільності та оцінка результатів.

Також набув подальшого розвитку понятійно-категорійний апарат науки державного управління у сфері протидії дезінформації, зокрема на основі виокремлених ознак (хибність, зловмисність, цілеспрямованість, наявність стратегічної мети та бажаний наслідок впливу) запропоновано авторське тлумачення дезінформації, під якою у подальших дослідженнях запропоновано розуміти створення та поширення з політичною чи іншою стратегічною метою завідомо хибної чи свідомо модифікованої інформації як істинної для інформаційно-психологічного впливу на об’єкт з метою формування в нього помилкового уявлення про реальність та підштовхування до певних дій чи бездіяльності з метою завдання шкоди інтересам людини, суспільства і держави. Констатовано, що до дезінформації слід відносити як самі хибні відомості, так і процес їх поширення, що може мати різні форми, методи та канали комунікації. Уточнено визначення таких понять, як «поширення дезінформації», «інформаційний ресурс», «канали поширення дезінформації», «спроба впливу на громадську думку», «суб’єкт поширення дезінформації», «об’єкт дезінформації». На основі проведеного аналізу різних підходів до формулювання терміну «інформаційна війна» запропоновано його

узагальнене визначення як процес використання інформаційних технологій та медіа-ресурсів з метою впливу на інформаційну безпеку та соціальну стабільність країни, проти якої така війна ведеться. Обґрунтовано недоцільність його заміни в офіційних документах на термін «спеціальні інформаційні операції», оскільки термін «інформаційна війна» охоплює більш широкий спектр діяльності, пов’язаної з використанням інформаційних засобів і методів для досягнення стратегічної мети. З урахуванням цього рекомендується зберегти термін «інформаційна війна» для загального опису явищ в інформаційному просторі, тоді як термін «спеціальні інформаційні операції» можна використовувати для позначення конкретних дій, обмежених у часі і цілях. Доведено, доцільність подальшого використання зазначених дефініцій у нормативно-правових документах України, які регулюють інформаційну сферу, що дозволить встановити єдині правила і принципи дій для всіх учасників процесу, сприяти ефективній протидії дезінформації, а також стати основою для подальших наукових розробок, спрямованих на удосконалення механізмів вироблення державної політики у сфері протидії дезінформації.

Окрім того, на основі розглянутого плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року в контексті державної політики у сфері протидії дезінформації, що дало змогу виявити ряд недоліків, які полягають у загальності формулювання завдань та недостатній деталізації (конкретизації) заходів, необхідних для досягнення поставлених цілей, визначенні лише узагальнених показників реалізації та не встановленні точних строків (проміжних термінів) щодо окремих етапів їхнього виконання, надано рекомендації щодо вдосконалення плану заходів з реалізації Стратегії інформаційної безпеки в контексті протидії дезінформації, що включають:

– деталізацію загальних завдань шляхом конкретизації дій та заходів, необхідних для досягнення поставлених цілей. Забезпечити

ефективну координацію та співпрацю між різними державними структурами та організаціями, що залучені до виконання Плану заходів;

– розмежування функцій Центру протидії дезінформації при РНБО України, відповідального за стратегічну координацію комунікації урядових структур, і Міністерства культури та інформаційної політики України як центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері для здійснення ефективної координації та співпраці між різними суб'єктами публічного управління, що залучені до виконання Плану заходів;

– розроблення протоколів обміну інформацією та узгодження спільних дій і заходів, спрямованих на протидію інформаційним загрозам;

– встановлення показників успішності, які дозволять оцінити ефективність проведених заходів та виявити потребу у доопрацюваннях;

– впровадження механізмів постійного моніторингу, контролю та оцінювання результативності проведених заходів у сфері протидії дезінформації, що дозволить своєчасно виявляти потребу у внесенні змін, визначати успішні практики та проблемні аспекти, які потребують додаткової уваги;

– унормування (розроблення та затвердження) алгоритму протидії дезінформації в умовах розвитку цифрового суспільства з конкретизацією необхідних заходів, що сприятиме забезпеченню державних структур сучасними технологіями та аналітичними інструментами аналізу інформаційних загроз та запобігання їхнього впливу.

Також, на основі проведеного аналізу концептуальних та практичних підходів в США та ЄС щодо розв'язання проблеми протидії дезінформації та з урахуванням сучасних умов й потенціалу цифрового розвитку України розроблено рекомендації щодо удосконалення нормативно-правового забезпечення у сфері протидії дезінформації шляхом необхідності створення окремого законопроекту, в якому регулюватимуться процеси

виявлення та запобігання її поширенню, а також передбачається: розширення повноважень та зміцнення матеріально-технічної бази Центру протидії дезінформації при РНБО України як керівного ядра інституціонального механізму вироблення державної політики у сфері протидії дезінформації; встановлення адміністративної та кримінальної відповідальності за створення та поширення дезінформації; запровадження інституту уповноваженого з питань інформації. Окрім цього рекомендовано нормативно врегулювати запровадження навчальних модулів, курсів та програм з опануваннях нових знань, умінь та навичок з критичного мислення, медіаграмотності та цифрової гігієни. Ці рекомендації спрямовані на вдосконалення державного управління у сфері протидії дезінформації через оновлення законодавства, що допоможе підвищити скоординованість та ефективність дій усіх зацікавлених сторін та забезпечити ефективне використання ресурсів, сприятиме покращенню захисту громадянських прав та свобод, а також зміцненню демократичних принципів функціонування інформаційного середовища.

На основі обґрунтування необхідності застосування цифрових інструментів протидії дезінформації та доведення ефективності створення єдиної системи раннього виявлення дезінформації та запобігання її поширенню, рекомендовано органам державної влади у подальшому здійснювати такі практичні заходи як:

– *Міністерству культури та інформаційної політики України*: забезпечити розробку та реалізацію цілісної й координованої програми розвитку цифрових каналів управління стратегічними комунікаціями для оперативного забезпечення населення достовірною інформацією в достатньому обсязі, а також для налагодження взаємодії з міжнародними партнерами у сфері захисту національних інтересів в інформаційному просторі;

– *Центру протидії дезінформації при РНБО України*: розвивати партнерські відносини з онлайн-медіа та провайдерами цифрових

платформ з метою виявлення ними дезінформаційного контенту та його блокування;

– *Міністерству цифрової трансформації України*: створити та постійно оновлювати репозитарій цифрових інструментів (програмного забезпечення) з урахуванням потреб технологічного розвитку та актуальних методів поширення дезінформації, а також сформувати державну цифрову платформ для обміну даними між органами публічної влади, задіяними у боротьбі з поширенням дезінформації; забезпечити співпрацю з технологічними компаніями, стартапами та інноваційними організаціями, що спеціалізуються на розробці алгоритмічних фільтрів та інших інструментів для виявлення та протидії дезінформації, що сприятиме появі нових технологій та інструментів у цій сфері;

– *Міністерству освіти і науки України, вищим навчальним закладам*: запровадити освітньо-професійні програми другого (магістерського) рівня освіти за спеціальністю 281 «Публічне управління та адміністрування» для опанування цифрових навичок з управління стратегічними комунікаціями, розробити та постійно проводити короткострокові курси підвищення кваліфікації та тренінги з питань протидії дезінформації для державних службовців та посадових осіб місцевого самоврядування.

Запропоновано органам влади на національному, регіональному та місцевому рівнях активно використовувати цифрові інструменти збору, аналізу та візуалізації даних щодо захисту інформаційного простору України, включаючи використання алгоритмів машинного навчання та штучного інтелекту з метою автоматизованого виявлення, класифікації та аналізу дезінформації.

Практичне значення отриманих результатів дисертаційного дослідження полягає у виробленні пропозицій щодо вдосконалення механізмів вироблення державної політики у сфері протидії дезінформації в умовах цифровізації публічного управління.

Ключові слова: дезінформація, інформаційна політика, державна політика, публічне управління, цифрові комунікації, кібербезпека, комунікативна діяльність, медіапростір, державні комунікації, засоби масової інформації, цифрові трансформації, цифрові технології, міжнародна співпраця.

ABSTRACT

Zhyvotova K.V. Mechanisms of Public Policymaking for Countering Desinformation. – Qualification scientific work, manuscript.

Thesis for the Academic Degree of Doctor of Philosophy in specialty 281 “Public management and administration”. – Kyiv National Economic University named after Vadym Hetman, Kyiv, 2024.

In the dissertation, a theoretical justification of the mechanisms for developing state policy in the field of countering disinformation and offers practical recommendations for their improvement in the context of digitalization of public administration.

The scientific novelty of the obtained results lies in the theoretical substantiation of the mechanisms for developing state policy in the field of countering disinformation and providing practical recommendations for their improvement in the context of the digitalization of public administration.

For the first time, a model of the institutional mechanism for developing state policy in the field of countering disinformation at the strategic, tactical, and operational levels has been developed. This model aims to ensure the response of government bodies to manipulative and falsified threats and is based on the interaction of public administration entities (strategic, regulatory, communicative, humanitarian, legal, scientific) in the implementation of a complex set of organizational and functional measures according to their areas of responsibility. This is based on: *factors:* political context, information culture, technological development, role of civil society, media influence, international cooperation,

financial resources, strategic partnership; *strategies:* implementation of protective measures, monitoring, analysis, and risk assessment, response and counteraction*; principles:* communicativeness, security, coordination, evidence-based approach, transparency, openness, engagement, and adaptability; *methods/means of content* collection and dissemination: media and social media monitoring, analytical tools, expert evaluation, public campaigns, special commissions and agencies, international cooperation, legislative initiatives; *tools for responding to threats*: strategic planning, analytical research, regulatory control, information monitoring, educational programs, partnership cooperation, information mobilization, coordination measures; *cooperation:* formation of specialized working groups and committees, holding regular meetings, information exchange, creation of joint programs and projects, crisis coordination, development of joint strategies; *partnership interaction:* engaging partnership programs with civil society and international projects, utilizing public-private partnerships, consulting with experts, organizing forums and working groups; *resources:* financial, human, and technical resources.

Proposed are the pathways for the development of the institutional mechanism for developing state policy in the field of countering disinformation, including: improving the coordination of actions between the Center for Countering Disinformation under the National Security and Defense Council of Ukraine and the relevant state authorities and other interested public administration entities; optimizing the use of financial, human, and technical resources by engaging in partnership interactions with civil society organizations, the private sector, and international partners for the joint implementation of projects and programs; updating the regulatory framework to take into account contemporary challenges, threats, risks, and the impact of digital technologies in the field of countering disinformation; ensuring broad public access to reliable information and enhancing the information literacy of the population.

The qualifying criteria for identifying false information as disinformation have been improved. These criteria include: inaccurate content that

contradicts objective reality; intentionally fabricated or distorted data aimed at misleading; deliberate dissemination of content with the intent to produce specific outcomes; influence on public consciousness and opinion, including the ability to cause chaos, destabilization, panic, and undermine trust in state institutions or other public administration entities.

Practical approaches to the application of state mechanisms to counter the rapid spread of disinformation have also been improved by: ensuring a balance between individual informational freedoms and the protection of the national interests of the state, including regulating the activities of anonymous online resources to stop the systematic and unpunished dissemination of false and manipulative information in the internet space aimed against the national interests of Ukraine; forming an appropriate legal framework for effective protection against threats in the information space; creating an integrated early threat detection system using artificial intelligence, machine learning, data analysis, and digital services; establishing cooperation and information exchange between various information security entities.

Additionally, the methodology for determining the factors influencing the effectiveness of countering disinformation spread through communication channels in the public sphere has been improved. This methodology comprises the analysis of social networks, monitoring of mass media, surveys and questionnaires, as well as the study of target group behavior. It includes the analysis of information resource traffic, the application of information-analytical system tools, interviews with experts and representatives of public organizations, research on the target audience and its interaction with media content, and the use of both quantitative and qualitative data analysis methods.

The work has further developed an algorithm for countering disinformation, taking into account the conditions of digital transformations. The algorithm consists of five main stages: identifying potential threats and formulating a strategy for state policy to counter disinformation; protecting against current threats by implementing mechanisms for information filtration and verification,

enhancing information literacy, and improving measures to protect against cyberattacks; detecting disinformation incidents in real-time mode; prompt and effective response to such incidents; implementing measures to restore stability and evaluating the results.

Furthermore, the conceptual-categorical apparatus of the science of public administration in the sphere of countering disinformation has also undergone further development. In particular, based on the identified features (fallaciousness, maliciousness, purposefulness, presence of a strategic goal, and desired outcome of influence), an authorial interpretation of disinformation has been proposed. In subsequent research, disinformation is suggested to be understood as the creation and dissemination, with a political or other strategic purpose, of knowingly false or consciously modified information presented as true, for the purpose of informational-psychological influence on the target, aiming to shape a distorted perception of reality and induce specific actions or inaction detrimental to the interests of individuals, society, and the state. It is noted that disinformation should encompass both false information itself and the process of its dissemination, which can take various forms, methods, and communication channels. Definitions of such concepts as "dissemination of disinformation," "information resource," "channels of disinformation dissemination," "attempt to influence public opinion," "disseminator of disinformation," and "target of disinformation" are clarified. Based on the analysis of various approaches to formulating the term "information warfare," a generalized definition is proposed as the process of using information technologies and media resources to influence the information security and social stability of the country against which such warfare is conducted. The impracticality of replacing it with the term "special informational operations" in official documents is substantiated, as the term "information warfare" encompasses a broader spectrum of activities related to the use of informational means and methods to achieve strategic goals. Considering this, it is recommended to retain the term "information warfare" for the general description of phenomena in the information space, while the term "special

informational operations" can be used to denote specific actions limited in time and objectives. The expediency of further using these definitions in regulatory documents of Ukraine, which regulate the information sphere, is proven. This will establish uniform rules and principles of action for all participants in the process, promote effective counteraction to disinformation, and serve as the basis for further scientific developments aimed at improving the mechanisms of formulating state policy in countering disinformation.

In addition, based on the reviewed action plan for implementing the Information Security Strategy for the period up to 2025 in the context of state policy in countering disinformation, which has revealed several shortcomings such as the general formulation of tasks, insufficient detailing (specification) of measures necessary to achieve the set goals, determination of only generalized indicators of implementation, and lack of precise deadlines (intermediate terms) for specific stages of their execution, recommendations have been provided to improve the action plan for implementing the Information Security Strategy in the context of countering disinformation, including:

– detailing the general tasks by specifying actions and measures necessary to achieve the set goals. Ensure effective coordination and cooperation between various government structures and organizations involved in implementing the Action Plan;

– delineating the functions of the Disinformation Counteraction Center under the National Security and Defense Council of Ukraine, responsible for strategic coordination of communication among government structures, and the Ministry of Culture and Information Policy of Ukraine as the central executive authority responsible for shaping and implementing state policy in the information sphere, to ensure effective coordination and cooperation among various public administration entities involved in implementing the Action Plan;

– developing protocols for information exchange and coordinating joint actions and measures aimed at countering information threats;

– establishing performance indicators to assess the effectiveness of the measures taken and identify the need for adjustments;

– implementing mechanisms for continuous monitoring, control, and evaluation of the effectiveness of measures in countering disinformation, enabling timely identification of the need for changes, identification of successful practices, and problematic aspects requiring additional attention;

– standardizing (developing and approving) a disinformation counteraction algorithm in the context of digital society development, with a specification of necessary measures, to provide government structures with modern technologies and analytical tools for analyzing information threats and preventing their impact.

Additionally, based on the analysis of conceptual and practical approaches in the USA and EU regarding the solution to the problem of countering disinformation, and considering the current conditions and the potential of digital development in Ukraine, recommendations have been developed to enhance the regulatory framework in the field of countering disinformation. This involves the necessity of creating a separate legislative bill to regulate the processes of detection and prevention of its dissemination. Furthermore, it includes the following provisions: expansion of powers and strengthening of the material-technical base of the Disinformation Counteraction Center under the National Security and Defense Council of Ukraine as the leading nucleus of the institutional mechanism for formulating state policy in countering disinformation; establishment of administrative and criminal liability for the creation and dissemination of disinformation; introduction of the institution of an authorized person for information matters. Additionally, it is recommended to regulate the implementation of educational modules, courses, and programs for acquiring new knowledge, skills, and abilities in critical thinking, media literacy, and digital hygiene. These recommendations aim to improve state governance in countering disinformation through legislative updates, which will enhance coordination and effectiveness of actions among all stakeholders, ensure efficient resource

utilization, contribute to the improvement of protection of civil rights and freedoms, and strengthen democratic principles in the functioning of the information environment.

Based on the justification for the necessity of applying digital tools to counter disinformation and demonstrating the effectiveness of creating a unified system for early detection of disinformation and prevention of its dissemination, it is recommended that government authorities implement the following practical measures:

– *Ministry of Culture and Information Policy of Ukraine:* Ensure the development and implementation of a comprehensive and coordinated program for the development of digital channels for strategic communications management to promptly provide the population with reliable information in sufficient volume, as well as to establish cooperation with international partners in protecting national interests in the information space.

– *Disinformation Counteraction Center under the National Security and Defense Council of Ukraine:* Develop partnerships with online media and digital platform providers to identify disinformation content and block it.

– *Ministry of Digital Transformation of Ukraine:* Create and continuously update a repository of digital tools (software) considering the needs of technological development and current methods of disseminating disinformation. Form a state digital platform for data exchange between public authorities involved in combating disinformation. Ensure cooperation with technology companies, startups, and innovative organizations specializing in the development of algorithmic filters and other tools for detecting and countering disinformation, which will contribute to the emergence of new technologies and tools in this field.

– *Ministry of Education and Science of Ukraine,* higher education institutions: Introduce educational-professional programs at the second (master's) level of education in the specialty 281 " Public management and administration" to

master digital skills in strategic communications management. Develop and regularly conduct short-term qualification enhancement courses and training sessions on countering disinformation for civil servants and officials of local self-government.

The practical significance of the obtained results of the dissertation research lies in the development of proposals for improving mechanisms of Public Policymaking for Countering Desinformation in the context of digitalization of public administration.

Key words: disinformation, information policy, state policy, public administration, digital communications, cybersecurity, communicative activity, media space, government communications, mass media, digital transformations, digital technologies, international cooperation.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових фахових виданнях України

1. **Животова К. В.** Особливості нормативно-правового регулювання сфери інформаційної безпеки: проблемні питання та термінологічні колізії в Україні. *Демократичне врядування.* 2021. №2 (28). URL: https://science.lpnu.ua/uk/dg/vsi-vypusky/vypusk-228-2021/osoblyvosti-normatyvno-pravovogo-regulyuvannya-sfery-informaciynoyi *(0,45 д.а.)*.

2. Карпенко О., **Животова К. В.** Концептуальні підходи до формування інформаційних механізмів запобігання та розв'язання міжнаціональних конфліктів. *Аспекти публічного управління*. 2022. № 10(6). С. 14-18. DOI: https://doi.org/10.15421/152238. *(0,43 д.а., особисто автору 0,25 д.а., проаналізовано концептуальні підходи до розуміння інформаційних механізмів, які базуються на використанні різноманітних теорій, концепцій та моделей, таких як теорії медіа, комунікації, масової інформації, політичної комунікації, комунікації в конфліктах тощо).*

3. **Животова К. В.** Механізми протидії дезінформації в сучасному інформаційному середовищі: економічний аспект. *Стратегія економічного розвитку України.* № 52. С. 5-16. URL: https://doi.org/10.33111/sedu.2023.52.005.016 *(0,62 д.а.)*.

В інших виданнях

1. **Животова К. В.** Інфодемія «Пандемія CoVID-19»: проблеми та перспективи організації реагування на поширення дезінформації. *Соціогуманітарний вимір сучасних трансформацій*. Збірник матеріалів Всеукраїнської науково-практичної конференції (м. Чернігів, 29 жовтня 2021 р.). Науково-освітній інноваційний центр суспільних трансформацій, м.Чернігів. Суми: ТОВ НВП «Росток А. В.Т.». 2021. 96 с. С. 12-14 URL: https://reicst.com.ua/asp/article/view/conf_gum_2021_03 *(0,13 д.а.)*.

2. **Животова К. В**., Пискун І. В. Інформаційна оборона органів влади як складова національної безпеки України. *Інформаційно телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання.* Матеріали науково-практичної конференції (м. Київ, 24-25 листопада 2021 р.). К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 316 с. С .22. *(0,2 д.а.)*

3. **Животова К. В.**, Трофименко В. М. Боротьба з кіберзлочинністю в умовах дії воєнного стану: аналіз нових законодавчих норм. *Кібербезпека державних інституцій та подолання кризових станів:* Матеріали І Міжнародної науково-практичної конференції. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2022. 321 с. С. 294-295. *(0,15 д.а.)*.

4. **Животова К.В.** Особливості використання цифрових інструментів в інформаційному протиборстві. *Кібербезпека державних інституцій та подолання кризових станів.* Матеріали ІІ Міжнародної науково-практичної конференції в 2 т. Том 2. Особливості діяльності органів державної влади в умовах кризи зб. Тез наук.доп. (Київ – Вроцлав. Травень 2023). [Електронне видання]. Київ : «Офіс цифрового врядування», 2023. Т.2. 148 с. С. 36-37. *(0,15 д.а.)*.

5. **Животова К. В.** Дезінформаційні кампанії РФ як спроба зірвати поставки зброї ВСУ та шляхи протидії з боку України. *Політичні технології пропаганди та контрпропаганди у російсько-українській війні* : зб. матеріалів Круглого столу з міжнар. участю, до річниці повномасштаб. вторгнення, м. Київ, 21 лютого 2023 р. / М-во освіти і науки України, Ком. з питань свободи слова Верховної Ради України [та ін.] ; [орг. ком.: Гапоненко В. А. та ін.]. Київ : КНЕУ, 2023. С. 133–136. URL: https://ir.kneu.edu.ua:443/handle/2010/40436 *(0,18 д.а.)*.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному контексті геополітичних подій і військових конфліктів дослідження феномену дезінформації стає важливим напрямом наукових досліджень, оскільки становить суттєву загрозу національним інтересам держави. Дезінформація в умовах збройної агресії проти України використовується як базова технологія реалізації стратегії інформаційної війни, що робить актуальним проблематику результативного застосування інструментів протидії інфільтрації фейків та негативним впливам на масову відомість. Необхідність ефективної протидії поширенню дезінформації спонукає до вдосконалення наявних механізмів вироблення належної державної політики та пошуку нових парадигм організації публічного управління у цій сфері.

Проблематика протидії дезінформації привертає увагу багатьох зарубіжних вчених. Перші спроби досліджень впливу дезінформації на суспільство було здійснено у працях У. Ліппмана [307] та М. Маклуена [312], які аналізували вплив ЗМІ на формування громадської думки та сприйняття політичних рішень, а також потенційну небезпеку інформації, що продукується масмедіа. Проблематика взаємодії мережевих систем досліджувалася М. Кастельсом [258] та Е. Тоффлером [335], які акцентували значущість їх впливу на організацію та функціонування суспільства. Просуваючи ідею впровадження децентралізованих комп'ютерних мереж, було передбачено появу Інтернету та нових цифрових медіа, а також визначено їх основні характеристики: інтерактивність, мобільність, поширення та глобалізація.

В українській та зарубіжній дослідницькій літературі проблему дезінформації активно досліджують О. Баришполець [3], П. Беднар [253], К. Бредемайер [254], К. Вордл [345], В. Горбулін [21], А. Додонов [40], О. Колісник [94], О. Литвиненко [111], В. Ліпкан [114], М. Ожеван [144],

Т. Попова [157], Г. Почепцов [161], М. Слюсаревський [198], М. Туджмант та Н. Мікеліч [338], Д. Фелліс [286], Д. Фетцер [288], Л.Флоріді [289], Х. Фокс [291], Г. Франке [292], І. Ципердюк [239], Г. Шиллер [328], В. Шлапаченко [243], Е. Шостром [329], Б. Шталь [332] та інші. Так, психологічні аспекти масової свідомості, методи та стратегії, які можуть використовуватися для маніпулювання масовою свідомістю та формування громадської думки, розглядають В. Беспека [5], Н. Ємець [48], О. Золотар [74], Л. Орбан-Лембрик [146], Г. Падалка [149]. Натомість, Ю. Половинчак [156], М. Праута [165], О. Пригорницька [166], О. Кононенко [97] та інші зосереджуються на вивченні механізмів маніпуляції та використанні інформації для мобілізації мас і контролю над ними.

Питання глобальної та національної безпеки вивчають В. Абрамов [18], Н. Волошина [14], Ю. Гладун [17], О. Горбатюк [20], Г. Ситник [191], О. Левченко [109], А. Нашинець-Наумова [141], Н. Нижник [142], Т. Ткачук [208], А. Турчак [209], П. Шевчук [241] та інші. Їхні дослідження сприяють розумінню сучасних викликів та розробленню ефективних стратегій, спрямованих на забезпечення стабільності та безпеки на національному та міжнародному рівнях. Крім того, група авторів на чолі з О. Резніковою [180] активно працює над створенням національної системи оцінювання ризиків і загроз, яка має на меті забезпечити вчасне реагування на кризові ситуації, ефективне управління ними та зменшення їх негативних наслідків.

Для глибшого розуміння проблематики вироблення нових підходів та методів протидії дезінформації важливим є ознайомлення зі спеціалізованою літературою, присвяченою сучасним інформаційним технологіям. Роботи О. Карпенка [84], П. Шпиги [244], А. Завади [56], К. Островської [147], Є. Івохіна [76] та інших українських дослідників дають можливість отримати уявлення про окремі цифрові інструменти, які можуть бути успішно застосовані для виявлення та протидії дезінформації. Ці наукові праці

охоплюють широкий спектр тем, включаючи аналіз соціальних мереж, машинне навчання, штучний інтелект, обробку природної мови та інші сучасні технології.

Аналіз стану розробленості зазначеної проблематики свідчить про значущість ролі ефективності та результативності вироблення (формування та реалізації) державної політики у сфері протидії дезінформації. Проте, незважаючи на докладені зусилля, наявні методи, інструменти, засоби та технології у цій сфері є традиційними або недостатньо пристосованими до нових викликів інформаційного середовища. Потреба у вирішенні зазначених проблемних питань на науковому та практичному рівнях зумовила вибір теми дослідження.

Актуальність теми дослідження визначається недостатністю теоретичного обґрунтування механізмів вироблення державної політики у сфері протидії дезінформації та відсутністю розроблених практичних рекомендацій щодо їх удосконалення в умовах цифровізації публічного управління, що не було вирішено на рівні наукового завдання в окремій дисертаційній роботі у галузі науки державного управління.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно з комплексним науковим проєктом «Державне управління та місцеве самоврядування» (№ ДР 0199U002827) науково-дослідної роботи Національної академії державного управління при Президентові України «Сервісна діяльність органів публічної влади в умовах розвитку цифрового суспільства» (№ ДР 0119U101449), де автором узагальнено зарубіжний досвід цифрових трансформацій задля протидії дезінформаційним впливам на масову свідомість.

Мета і завдання дослідження. Метою дисертаційної роботи є теоретичне обґрунтування механізмів вироблення державної політики у сфері протидії дезінформації та надання практичних рекомендацій щодо їх вдосконалення в умовах цифровізації публічного управління.

Для досягнення мети поставлені такі *завдання*:

– визначити основні дефініції понятійно-категорійного апарату науки державного управління у сфері протидії дезінформації;

– встановити фактори, що впливають на швидкість поширення дезінформації комунікативними каналами у публічній сфері та розробити алгоритм протидії дезінформації з урахуванням розвитку цифрових трансформацій;

– розробити модель інституціонального механізму вироблення державної політики у сфері протидії дезінформації та запропонувати шляхи його розвитку;

– розглянути план заходів з реалізації Стратегії інформаційної безпеки в контексті державної політики у сфері протидії дезінформації та надати рекомендації щодо його удосконалення;

– здійснити порівняльний аналіз концептуальних та практичних підходів зарубіжних країн до розв’язання проблеми протидії дезінформації, на основі якого розробити рекомендації щодо удосконалення відповідного нормативно-правового забезпечення з урахуванням сучасних умов й потенціалу цифрового розвитку України;

– обґрунтувати необхідність застосування цифрових інструментів протидії дезінформації та розробити практичні рекомендації щодо їх подальшого використання.

Об’єкт дослідження – державна політика у сфері протидії дезінформації.

Предметом дослідження – механізми вироблення державної політики у сфері протидії дезінформації.

Методи дослідження. Для досягнення поставленої мети та вирішення завдань дисертаційної роботи було застосовано широкий інструментарій наукових методів. Зокрема використано метод узагальнення та систематизації теоретичних джерел і нормативно-

правових документів, що дало змогу отримати базові теоретико-методологічні положення стосовно визначення спектру необхідних механізмів вироблення державної політики у сфері протидії дезінформації. Для з'ясування рівня ефективності застосування нормативно-правового забезпечення для формування інституційної моделі був здійснений аналіз державних програм, стратегій, законодавчих актів, що регулюють процеси формування державної політики та протидії дезінформації. Соціологічний підхід дозволив виявити соціальні тенденції і тренди, що стосуються дезінформації. Порівняльний метод дослідження був використаний для зіставлення механізмів державної політики, які проводять різні країни, що допомогло виявити спільні та відмінні риси їх виробленні, а також з'ясувати, які підходи є найбільш дієвими. Антропологічний підхід, що базується на вивченні людських поведінкових практик, дозволив, зокрема, дослідити, як переконання, цінності, норми та практики різних груп і спільнот впливають на процеси поширення дезінформації. Психологічний метод допоміг зрозуміти психологічні процеси, що лежать в основі створення та розповсюдження дезінформації, та визначити психологічні особливості та мотивації різних груп населення, що можуть бути вразливі до дезінформації. Використання біхевіористського методу дослідження дозволило отримати необхідні данні про результативність різних заходів з протидії дезінформації, що може стати важливим елементом у реалізації державної політики в цій сфері. Нормативно-ціннісний метод дослідження застосовувався у процесі аналізу норм, правил та соціальних установок, які впливають на вироблення державної політики у сфері протидії дезінформації, дозволив вивчити ціннісні орієнтації різних соціальних груп, їхніх поглядів на проблему дезінформації і шляхів її протидії. Використання загальнонаукових та спеціальних методів дослідження допомогло отримати комплексний погляд на проблему і розробити ефективні підходи до механізмів протидії дезінформації з урахуванням різних аспектів, таких як теоретичні основи, нормативно-правове

забезпечення, соціальні тенденції, психологічні процеси та ціннісні орієнтації.

Наукова новизна одержаних результатів полягає в теоретичному обґрунтуванні механізмів вироблення державної політики у сфері протидії дезінформації та наданні практичних рекомендацій щодо їх вдосконалення в умовах цифровізації публічного управління.

Уперше: розроблено модель інституціонального механізму вироблення державної політики у сфері протидії дезінформації на стратегічному, тактичному та операційному рівнях для забезпечення реагування підрозділів органів влади на маніпулятивні та фальсифікативні загрози, що базується на взаємодії суб'єктів публічного управління (стратегічних, регуляторних, комунікативних, гуманітарних; юридичних, наукових) у процесі реалізації комплексу організаційно-функціональних заходів згідно зон їх відповідальності на основі: *факторів* (політичний контекст; інформаційна культура; технологічний розвиток; роль громадянського суспільства; вплив медіа; міжнародна співпраця; фінансові ресурси; стратегічне партнерство); *стратегій* (реалізації заходів захисту; здійснення моніторингу, аналізу та оцінювання ризиків; реагування та здійснення контрдій); *принципів* (комунікативності, захищеності, координованості, доказовості, прозорості, відкритості, задіяності та адаптивності); *методів/засобів збору та поширення контенту* (моніторингу медіа та соціальних мереж; аналітичних інструментів; експертної оцінки; публічних кампаній; спеціальних комісій та агентств; міжнародного співробітництва; законодавчих ініціатив); *інструментів реагування на загрози* (стратегічне планування; аналітичні дослідження; нормативне регулювання; інформаційний моніторинг; освітні програми; партнерська співпраця; інформаційна мобілізація; координаційні заходи); *співпраці* (формування спеціалізованих робочих груп та комітетів; проведення регулярних нарад; здійснення обміну інформацією; створення

спільних програм і проєктів; здійснення кризової координації; розробка спільних стратегій) та *партнерської взаємодії* (залучення партнерських програм з громадянським суспільством та міжнародних проєктів; застосування публічно-приватного партнерства; проведення консультацій з експертами; організація форумів та робочих група); *ресурсів* (фінансових, людських і технічних).

удосконалено:

– кваліфікуючі критерії, за якими недостовірна інформація визначається дезінформацією, а саме: недостовірний зміст, який суперечить об’єктивній реальності; навмисно вигадані або спотворені дані з метою введення в оману; цілеспрямоване поширення контенту з метою виникнення певних наслідків; вплив на суспільну свідомість та громадську думку, включаючи здатність спричиняти хаос, дестабілізацію, викликати паніку, підважити довіру до державних інституцій або інших суб’єктів публічного управління;

– практичні підходи щодо застосування державних механізмів протидії швидкому поширенню дезінформації шляхом: забезпечення досягнення балансу між індивідуальними інформаційними свободами та захистом національних інтересів держави, зокрема врегулювання діяльності анонімних онлайн-ресурсів для припинення системного та безкарного поширення недостовірної та маніпулятивної інформації в інтернет-просторі, спрямованої проти національних інтересів України; формування належної правової бази ефективного захисту від загроз в інформаційному просторі; створення інтегрованої системи раннього виявлення загроз за допомогою технологій штучного інтелекту, машинного навчання, аналізу даних та цифрових сервісів; налагодження співпраці та обміну інформацією між різними суб'єктами інформаційної безпеки;

– методику визначення факторів, що впливають на результативність протидії впливу дезінформації, яка поширюється комунікативними

каналами у публічній сфері, що складається з аналізу соціальних мереж; моніторингу засобів масової інформації, опитування та анкетування, а також вивчення поведінки цільових груп; аналізу трафіку інформаційних ресурсів; застосування інструментарію інформаційно-аналітичних систем; інтерв'ювання експертів та представників громадських організацій; дослідження цільової аудиторії та її взаємодії з медіа-контентом; використання кількісних та якісних методів аналізу даних;

набули подальшого розвитку:

– алгоритм протидії дезінформації з урахуванням умов розвитку цифрових трансформацій, який складається з п'яти основних етапів: визначення потенційних загроз та вироблення стратегії державної політики протидії дезінформації; захист від поточних загроз шляхом впровадження механізмів фільтрації та перевірки інформації, підвищення інформаційної грамотності та вдосконалення заходів захисту від кібератак; виявлення дезінформаційних інцидентів в режимі реального часу; оперативне та ефективне реагування на такі інциденти; здійснення заходів з відновлення стабільності та оцінка результатів;

– понятійно-категорійний апарат науки державного управління у сфері протидії дезінформації шляхом деталізованого аналізу та уточнення поняття «дезінформація» як базової категорії в проблематиці вироблення механізмів державної політики у сфері протидії дезінформації, яке враховує якісні та кількісні характеристики недостовірної інформації, включаючи її походження, наміри та наслідки, та поняття «інформаційна війна» як процесу використання інформаційних технологій та медіа-ресурсів з метою впливу на інформаційну безпеку та соціальну стабільність країни, проти якої така війна ведеться, а також обґрунтовано доцільність подальшого використання цих дефініцій у нормативно-правових актах України. Уточнено визначення таких понять, як «поширення дезінформації», «інформаційний ресурс», «канали поширення

дезінформації», «спроба впливу на громадську думку», «суб'єкт поширення дезінформації», «об'єкт дезінформації».

Практичне значення одержаних результатів полягає у виробленні пропозицій щодо вдосконалення механізмів вироблення державної політики у сфері протидії дезінформації. Основні положення, висновки та рекомендації використано:

– у діяльності Державного комітету телебачення і радіомовлення України. Враховано науково обґрунтовані пропозиції щодо оптимізації механізмів вироблення та реалізації державної політики у сфері протидії дезінформації, що відображено у створенні нових інструментів моніторингу та аналізу інформаційного простору, а також у виробленні Плану заходів уряду з реалізації Стратегії інформаційної безпеки на період до 2025 року (заходів, спрямованих на розвиток співпраці між органами влади, громадськістю та ЗМІ з метою побудови ефективної стратегії протидії дезінформації для забезпечення інформаційної безпеки України). Рекомендації, що містяться в дисертації, також було використано у процесі розробки «Закону про медіа», який набув чинності 31 березня 2023 року, що сприяло підвищенню ефективності системи регулювання медіа простору з урахуванням важливості боротьби з дезінформацією та забезпеченням інформаційної безпеки суспільства (довідка №724/28/3-1 від 12.03.2024);

– в навчальному процесі кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана при підготовці та викладанні навчальних дисциплін «Цифрові комунікації та зв'язки з громадськістю в публічному управлінні», «Інформаційні війни та цифрова культура» та «Цифрові виборчі технології», зокрема запропоновано науково обґрунтовані підходи щодо формування державних механізмів протидії дезінформації в умовах інформаційної війни, зокрема у запровадженні

інноваційних складових програми підвищення медіаграмотності населення України (довідка № 01/13-421 від 23.04.2024).

Особистий внесок здобувача. Дисертація є самостійною науковою працею, яка містить ідеї, висновки і пропозиції, які характеризуються науковою новизною і належать особисто авторці. У наукових працях, опублікованих у співавторстві, використано тільки ті розробки, напрацювання та положення, які є результатом особистих досліджень авторки.

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи оприлюднено авторкою на науково-практичних конференціях за міжнародною участю, а саме: «Соціогуманітарний вимір сучасних трансформацій» (Чернігів, 2021), «Інформаційно телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання» (Київ, 2021), «Кібербезпека державних інституцій та подолання кризових станів» (Київ, 2022), «Кібербезпека державних інституцій та подолання кризових станів» (Київ – Вроцлав, 2023), «Політичні технології пропаганди та контрпропаганди у російсько-українській війні» (Київ, 2023).

Публікації. За результатами дослідження автором опубліковано самостійно й у співавторстві 8 наукових праць загальним обсягом 2,31 д. а. (особисто автору належать *2,13 д. а.),* з них: 3 – у наукових фахових виданнях України, 6 – в інших виданнях.

Структура та обсяг дисертації. Специфіка проблем, що стали предметом дисертаційного дослідження, зумовила його логіку та структуру. Робота складається із вступу, трьох розділів, поділених на підрозділи, висновків, списку використаних джерел і додатків. Загальний обсяг дисертаційної роботи становить 255 сторінок друкованого тексту, з них основний текст – 195 сторінок. Робота містить 6 таблиць на 12 сторінках, 7 рисунків на 7 сторінках, 3 додатки на 5 сторінках, список використаних джерел на 36 сторінках. Список використаних джерел налічує 347 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

1.1. Механізми вироблення державної політики у сфері протидії дезінформації як предмет наукових досліджень

Механізми вироблення державної політики у сфері протидії дезінформації є актуальною науково-практичною проблемою, яка належить до сфери державного управління та вимагає інтегрованого підходу, що поєднує політичні, соціологічні, комунікаційні, психологічні, правові, технологічні аспекти. Це стає особливо важливим у контексті активних дій Російської Федерації, спрямованих на спотворення інформаційного простору, маніпулювання громадською думкою та створення хаосу і невпевненості в суспільстві, що базуються на використанні дезінформації як ключової технології інформаційної війни. Її негативний вплив вимагає адекватного реагування з боку держави та розроблення комплексних стратегій і механізмів, спрямованих на аналіз, контроль та протидію поширенню недостовірної і маніпулятивної інформації.

Для розуміння складних взаємозв'язків, процесів та інструментів, які використовуються у виробленні ефективної державної політики у сфері протидії дезінформації важливо вивчити роль та взаємодію різних акторів, задіяних у цьому процесі, а також проаналізувати досвід інших країн та виявити успішні практики, які можуть бути використані в українському контексті. Зокрема, наукові праці зарубіжних дослідників Г. Колбеча [93], Е. Янґа [246], Л. Пала [151], М. Крафта і Р. Скотта [104], Ж. Андерсона [250] та вітчизняних науковців В. Тертички [204], В.Купрія [108], І. Кресіної [105], В. Ребкала [177], О. Дем’янчука [30], Ю. Палагнюк [153], О. Пухкала [170] стали цінним джерелом для розуміння природи державної політики.

Для більш глибокого осмислення механізмів її вироблення додаткову інформацію надають теоретичні дослідження та розвідки О. Карпенка [83], Ю. Ковбасюка [89], В. Бакуменка [1]. Зокрема, О. Карпенко розглядає механізми вироблення державної політики в Україні як складну систему управління, яка включає в себе різноманітні інституції та групи національного інтересу та потребує ефективного взаємодії між ними для досягнення стратегічної мети [83].

Теоретично-методологічні основи механізмів забезпечення інформаційної безпеки розглядають у своїх публікаціях В. Шемчук [242], О. Радченко [176], О. Кілієвич [86], П. Садковий [187], Л. Козлова [92], В. Гурковський [25], О. Зозуля [72]. Кожен із згаданих науковців спеціалізується на своєму конкретному напрямі, проте всі вони акцентують увагу на проблемах забезпечення інформаційної безпеки в кризових умовах. Наприклад, В. Гурковський [25] розглядає організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки, тоді як О. Зозуля [72] аналізує питання державного управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства.

На значущості розвитку інформаційної складової державної політики зосереджують увагу С. Соловйов [200], В. Тарасюк [201], В. Дрешпак [44], С. Чукут [164], К. Захаренко [67] та автори навчального посібника «Інформаційна безпека України в умовах євроінтеграції» В. Ліпкан, Ю. Максименко і В Желіховський [114]. Їхні наукові праці спрямовані на розуміння ролі інформації у формуванні та реалізації державної політики, а також на виробленні стратегій інформаційної безпеки і оборони та комунікаційних стратегій для державних органів.

Крім того, важливими є дослідження, що охоплюють загальну структуру інституційної моделі державної політики та рольову модель державного апарату в контексті формування політики протидії дезінформації. Зокрема, такі вчені, як Т. Дай [26], Дж. Аї [251],

О. Данильян [27], О. Дем’янчук [30] зосереджуються на вивченні формальних та неформальних правил, процедур та механізмів, які впливають на процес прийняття та реалізації політичних рішень. Також вони аналізують фактори, що забезпечують ефективність інституційної моделі державної політики.

Питання права з акцентом на проблематиці нормативно-правового забезпечення сектору інформаційної безпеки досліджують Т. Ткачук [208], А. Нашинець-Наумова [141], О. Верголяс [12], Б Кормич [102], П. Рабінович [171], І Доронін [42], А. Берлач [4], С. Пирожков [155], Н. Нижник [142], Г. Ситник [191], К. Бєляков [6], В. Фурашев [233], О. Золотар [77]. Зокрема, О. Верголяс [12] досліджує правове забезпечення спеціальних інформаційних операцій. Т. Ткачук [208] зосереджує увагу на євроінтеграційному аспекті правового забезпечення інформаційної безпеки, тоді як Золотар розглядає інформаційне право перш за все в контексті інформаційної безпеки людини. Правовим аспектам забезпечення національної безпеки України в інформаційну епоху присвятив своє дисертаційне дослідження І. Доронін [42].

Для розуміння принципів протидії дезінформації та виявлення ефективних підходів до зазначеної проблеми важливо вивчити джерела, які досліджують механізми протидії дезінформації у різних країнах та міжнародних організаціях. Наприклад, В. Хакімова [234] аналізує здобутки та проблеми в діяльності East StratCom Task Force, М. Гребенюк [23] вивчає досвід ЄС щодо протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів, О. Звоздецька [70] досліджує інституційні механізми протидії дезінформації в Європейському Союзі, Н. Ротар [185] зосереджує увагу на проблемі формування політики захисту електоральної моделі політичної участі від дезінформаційних впливів.

Цінним джерелом інформації також є офіційні документи ЕС, спрямовані на протидію дезінформації, такі як Директива ЄС про протидію дезінформації, Спільна рамкова програма з протидії гібридним загрозам,

Декларація про інформаційну безпеку та боротьбу з дезінформацією, Кодекс поведінки ЄС щодо дезінформації (2018) та оновлений Кодекс поведінки щодо дезінформації (2022), Закон про цифрові послуги тощо.

Варто зауважити, що перша спроба наукового обґрунтування впливу дезінформації на суспільство була здійсненаУ. Ліппманом [307]. У своїй праці "Громадська думка", яка була опублікована у 1922 році, Ліппман розглядав вплив ЗМІ, таких як газети, радіо та інші засоби комунікації, на сприйняття суспільством подій, політичних рішень і формування громадської думки. Він наголошував на необхідності критичного мислення та активній ролі громадян у сприйнятті інформації. Крім того, Ліппман підкреслював роль державних структур у формуванні політики, яка враховує вплив масової комунікації на суспільство.

Зазначимо, що тривалий час феномен дезінформації розглядався в контексті спеціальних інформаційних операцій, які проводив СРСР стосовно умовного Заходу. У 1969 році Г. Шиллер [328] у своїй праці "Масова комунікація та американська еліта" говорить про використання дезінформації в СРСР для контролю над масами. З українського боку історію інформаційного протистояння від початку холодної війни до наших днів досліджує група фахівців з Національного інституту стратегічних досліджень у складі Д. В. Дубова, А.В. Баровської, Т. О. Ісакової, І. О. Коваля та В. П. Горбуліна, які є авторами аналітичної доповіді «Активні заходи» СРСР проти США: пролог до гібридної війни» [45]. Крім того, дослідники В. Беспека [5], К. Мануїлова [118], І. Ципердюк [239] аналізують аналогії між американо-російським інформаційним протистоянням у роки холодної війни минулого сторіччя та сучасними тенденціями в цьому напрямі.

Після закінчення холодної війни термін «дезінформація» почав широко використовуватися у США та інших країнах для позначення різних видів маніпуляції та поширення хибної інформації. Зокрема, це питання активно досліджували К. Девіс і Л.Біттман [262], Р.Шульц і Р.

Годсон [330]. В сучасній дослідницькій літературі проблему дезінформації розглядають хорватські вчені М. Туджман та Н. Мікеліч [262], американські дослідники Д. Фетцер [288], Л.Флоріді [290], К. Вордл [345], Б. Шталь [332], П. Беднар [353], Д. Фелліс [286], К. Фокс [291], Х.Елкот та М. Генцкоу [248], а також вітчизняні науковці Т. Попова та В. Ліпкан [157], О. Баришполець [3], Г. Почепцов [161], В. Горбулін [21] та інші.

На маніпуляційній складовій дезінформації наголошують зарубіжні науковці К. Бредемайер [254], Г. Франке [292], Г. Шиллер [328], Е. Шостром [329], а також вітчизняні дослідники О. Данильян та О. Дзьобань [27], М. Слюсаревський [195], А. Додонов у співавторстві з Д. Ланде та В. Циганком [40], М. Ожеван [144], О. Колісник [94], В. Шлапаченко [243].

Психологічний аспект дезінформації як різновид обману у своїх дослідженнях розглядають Чарльз В. Форд [240], А. Фрай [344], Ю. Харарі [235]. Так, Ч. Форд [240] у своїх дослідженнях зосереджується на психологічних механізмах, які використовуються для створення та поширення дезінформації. Він досліджує психологічні фактори, які сприяють сприйняттю неправдивої інформації та впливають на формування переконань та поведінки людей. А. Фрай [344] розглядає психологічний вимір дезінформації в контексті соціальних мереж та масових комунікацій. Він досліджує, як психологічні чинники, такі як емоції, стереотипи, приналежність до групи та інші фактори, що впливають на розповсюдження дезінформації через цифрові платформи та сприяють формуванню поглядів та установок у суспільстві. Ю. Харарі [235] звертає увагу на психологічний вплив дезінформації на індивіда та суспільство. Він розглядає механізми, за допомогою яких дезінформація впливає на формування світогляду, виявлення реальності та прийняття рішень людьми, а також досліджує психологічні стратегії протидії дезінформації та розвитку медійної грамотності серед населення.

На різні когнітивні спотворення, такі як підтверджувальний упереджений погляд, ефект соціального прийняття, ефект доступності, що впливають на сприйняття інформації та прийняття рішень, звертають увагу Р. Нойман [319], П. Сінгер [190] та інші науковці, які досліджують те, як ці спотворення можуть бути використані для маніпуляції та поширення дезінформації.

Також важливо вивчити підхід до недостовірної і повністю вигаданої інформації відомого французького філософа Ж. Бодріяра [8], який для позначення того, чого насправді немає, використав поняття симулякрів. Відповідно до його філософських роздумів, сучасне суспільство ступило в епоху глибокої симуляції, де реальність і симулякри, створені шляхом імітації реальності через засоби масової комунікації, стають нерозрізненими. Таким чином, філософ стверджує, що інформація, яка надходить до нас через різні канали, може бути неправдивою, зміненою або навіть вигаданою. Він розглядає цей процес як результат активної маніпуляції та контролю, де виробництво симуляків замінює реальність.

Та зауважимо, що серед перших, хто звернув увагу на потенційну небезпеку інформації, яку виробляють і поширюють ЗМІ, був канадський філософ М. Маклуен [312], який зазначав, що засоби масової комунікації мають величезний вплив на сприйняття людьми реальності та нашу здатність розуміти світ.

Відомий американський інформатик Н. Вінер [347] та німецький філософ Г. Маркузе [309] також висловлювали стурбованість щодо проблем інформаційної безпеки та звертали увагу на те, що технічний прогрес може стати джерелом маніпулювання людьми. Як зазначає Джеймс Кац [303], співробітник Центру досліджень мобільного зв'язку Бостонського університету, «натовпи є мудрими, але не надто мудрими», що може зробити їх привабливими для суб'єктів, які хочуть маніпулювати на впливати на інформаційне середовище, щоб масово поширювати будь-яку інформацію, навіть якщо вона є некоректною.

Окрему увагу філософи звертали на проблему широкого використання мережевих систем. Так, американський дослідник З. Бжезинський [255] стверджував, що сучасне суспільство, яке формується під впливом техніки та електроніки, переживає руйнацію традиційних відносин, коли, з одного боку, відбувається фрагментація життя людини, а з іншого, – формується її цілісний глобальний світогляд.

Іспанський соціолог М. Кастельс [259] у своїй концепції «суспільства мережевих структур» характеризує його як суспільство, де провідну роль відіграють різноманітні мережеві форми взаємодії, які впливають на організацію та функціонування суспільства, провідною ознакою якого стає «домінування соціальної морфології над соціальною дією».

У свою чергу Е. Тоффлер [335], просуваючи ідею впровадження децентралізованих комп'ютерних мереж, в яких контроль та управління розподілені між багатьма користувачами, передрік появу Інтернету. Також Тоффлер передбачив появу нових медіа та назвав їх особливості: інтерактивність, мобільність, широке поширення і глобалізація.

Вплив дезінформації на масову свідомість на сучасному етапі розвитку суспільства розглядають українські науковці Н. Ємець [48], Л. Орбан-Лембрик [146], Г. Падалка [149], які досліджують психологічні аспекти масової свідомості, маніпуляційні методи та стратегії, що можуть використовуватись для маніпулювання масами та формування громадської думки, вигідної маніпулятору.

Вітчизняні дослідники Ю. Половинчак [156], Г. Назаренко [133], М. Кононенко [97] та інші вивчають роль нових медіа у формуванні громадської думки, досліджують механізми маніпуляції і використання інформації для мобілізації мас та контролю над ними. Їхні наукові праці спрямовані на аналіз впливу нових медіа та розроблення стратегій для забезпечення інформаційної безпеки в умовах інформаційного суспільства.

На дезінформації як нелінійному ефекті взаємодії інформаційних тематичних потоків зосереджує увагу С. Брайчевський [9], доводячи, що

результат дезінформації не є простим сумуванням окремих інформаційних елементів. Замість цього, на думку вченого, взаємодія різних тематичних потоків створює нову, складну інформацію, яка може мати непередбачувані наслідки та впливати на сприйняття та реакцію громадськості.

У контексті дослідження загроз, пов’язаних з дезінформацією, значну роль у виробленні теоретичних концепцій також відіграють науковці, що вивчають феномен інформаційної війни. Серед важливих джерел у цьому напрямі варто зазначити праці таких вчених, як П. Баран [2], А. Сігал [331], А. Даллес [Цит. 116], які були серед перших, хто зосередив свою увагу на цій темі. Зокрема, колишній директор ЦРУ Ален Даллес використав термін «інформаційна війна» у своїй книзі «Таємна капітуляція», яка була опублікована у 1967 році. Однак, більшість дослідників пов’язує походження цього терміну з аналітичною доповіддю компанії Boeing під назвою «Системи озброєння та інформаційна війна», яка була представлена у 1976 році військовим аналітиком Т. Роном [326].

Проте справжній прорив у дослідженнях теми інформаційної війни відбувся лише в 1990-х роках, коли концепцію інформаційної війни та виклики, які вона ставить перед сучасною безпекою, досліджували Ф. Хоффман [299], Г. Еллісон [299], Г. Шиллер [328].

Технічним аспектам інформаційної війни, таких як хакерство, конфіденційність інформації, комп’ютерні віруси тощо присвятили свої дослідження Д. Гартлі [297], М. Кеннеді [304], М. Лібіцкі [306]. Наприклад, М. Лібіцкі [306] у своїй роботі визначив інформаційну війну як "систематичне використання інформаційних технологій та засобів з метою досягнення політичних, економічних або військових цілей, шляхом маніпуляції, контролю або знищення інформації, що належить іншій стороні». Враховуючи такий розвиток подій, М. Кеннеді [304] висловив необхідність вироблення міжнародних норм, які регулювали б використання сучасних технологій у сфері інформаційної війни.

В українському науковому контексті сутність інформаційної війни та вплив дезінформації на суспільство розкривають вітчизняні науковці В. Ліпкан [112], П. Шевчук [241], Є. Магда [116], О.Копан та В.Мельник [100], Г. Почепцов [161]. Зокрема, Г. Почепцов протягом кількох десятиріч активно досліджує тему безпеки комунікацій і дезінформації та є автором багатьох книг і статей, присвячених різним аспектам інформаційної війни. У своїх працях, зокрема в книзі "Стратегічний аналіз для політики, бізнесу та військової справи" [163] науковець досліджує сутність інформаційної війни, її вплив на політику та суспільство, а також надає рекомендації щодо стратегій управління цим явищем.

Питання глобальної та національної безпеки вивчають українські науковці, зокрема група авторів Г. Ситник, В. Абрамов і В. Смолянюк [18], а також О. Левченко у співавторстві з В. Троцьком та І. Василенко [110], М. Ситник [193], В. Петрик [154] та інші. Їхні дослідження сприяють розумінню сучасних викликів та розробленню ефективних стратегій та політик, спрямованих на забезпечення стабільності та безпеки на національному та міжнародному рівнях. У свою чергу, автори «Зеленої книги протидії дезінформації» С. Балан, Д. Золотухін, О. Романюк та інші [71] пропонують власну концепцію протидії дезінформації в Україні. Ця концепція базується на комплексному підході та включає переважно стратегії і заходи, які були розроблені в попередні роки, та які, на думку авторів, необхідно імплементувати в сучасну державну політику протидії дезінформації.

Натомість, українські дослідники О. Резнікова, К. Войтовський, А. Лепіхов [180] працюють над створенням національної системи оцінювання ризиків і загроз, яка покликана забезпечити вчасне реагування на кризові ситуації, ефективне управління ними та зменшення їх негативних наслідків. Ця система включає методи аналізу, прогнозування та оцінки ризиків, вироблення стратегій превентивних заходів,

впровадження механізмів реагування та координації, а також залучення до спільних дій різних зацікавлених сторін з боку державних структур, неурядових організацій та представників наукової спільноти.

Також питаннями пошуку ефективних інструментів оцінки ризиків і загроз як методів державного управління забезпеченням національної безпеки займаються вітчизняні науковці Ю. Гладун та А. Ліпенцев [17], Н. Ткачук [207], а також група дослідників В. Богданович, А. Семенченко і М. Єжеєв [7]. Зауважимо, що ідею розроблення паспорту загрози як дієвий інструмент раннього виявлення загроз національній безпеці України вперше висунули науковці Національної академії державного управління при Президентові України Г.Ситник, В. Абрамов, В. Мандрагеля, М. Шевченко та Л. Шипілова [192] у 2012 році. В останні роки цю тему розвинули М. Опанасенко та Т. Дзюба [145].

Для глибшого розуміння проблематики вироблення нових підходів та методів протидії дезінформації важливим є ознайомлення зі спеціалізованою літературою, присвяченою сучасним інформаційним технологіям. Роботи О. Карпенка [83], П. Шпиги [244], А. Завади [56], К. Островської [147], Є. Івохіна [76] та інших українських дослідників допомагають отримати чітке уявлення про новітні цифрові інструменти, що можуть бути успішно застосовані для виявлення та протидії дезінформації. Ці наукові праці охоплюють широкий спектр тем, включаючи аналіз соціальних мереж, машинне навчання, штучний інтелект, обробку природної мови та інші сучасні технології.

Узагальнюючи вищезазначене, можнастверджувати, що дослідження концептуальних підходів до аналізу механізмів вироблення державної політики у сфері протидії дезінформації є основою для подальшого осмислення цієї теми. Використання наукових джерел, присвячених цій проблематиці, сприяло порівнянню теоретичних концепцій з емпіричними даними, що дозволило розкрити різні аспекти та підходи до формування державної політики у сфері протидії дезінформації. Такий підхід сприяє

глибшому розумінню сутності проблеми та виробленню ефективних стратегій та політик у цій сфері.

1.2. Історична динаміка та сучасні тенденції становлення та розбудови механізмів вироблення державної політики у сфері протидії дезінформації: правовий аспект

Комплексне дослідження історичного процесу становлення та розвитку системи нормативно-правової регламентації забезпечення інформаційної безпеки України дозволяє простежити взаємозв'язок між загальними підходами до вироблення державної політикита основними тенденціями розвитку відповідного правового поля. Виявлення таких взаємозв'язків допоможе сформувати пропозиції щодо розвитку механізмів вироблення державної політики у сфері протидії дезінформації.

Точкою відліку створення системи захисту інформаційної безпеки незалежної України можна вважати Розпорядження Президента України №117 від 3 липня 1992 року про затвердження Тимчасового положення про Раду національної безпеки України [206], згідно з яким РНБУ визначалася якорган консультативного та дорадчого характеру, що діє в системі державної виконавчої влади при Президенті України, основним завданням якого є розроблення пропозицій та проектів рішень для Президента України, спрямованих на захист національних інтересів та забезпечення національної безпеки України [206]. Проте, за два роки було затверджено нове положення, відповідно до якого Рада національної безпеки визначалася як колегіальний орган, що функціонує при Президентові України та відповідає за організаційно-координаційну діяльність у сфері забезпечення національної безпеки [210].

Зауважимо, що свою сучасну назву Рада національної безпеки і оборони України (РНБОУ) отримала у 1996 році [213] після прийняття Конституції України, а на середину 2023 року діє поточна редакція Указу

Президента «Про Раду національної безпеки і оборони України» від 8 лютого 2005 року [213].

Також згідно зі ст. 107 Конституції України у жовтні 1996 року було утворено Апарат РНБО [212], останні зміни до Положення про який були затверджені Указом Президента України №251/2012 від 6 квітня 2012 року [216]. Свою діяльність з протидії дезінформації РНБО здійснює, зокрема, через спеціальний орган – Центр протидії дезінформації, який було створено у 2020 році [228].

Повертаючись до історичних витоків сучасної нормативно-правової бази, зазначимо, що 1992 року був ухвалений один з найважливіших документівв цьому напрямі – «Закон про інформацію» [58], який містив кілька ключових положень:

–до основних напрямів державної інформаційної політики належить забезпечення інформаційної безпеки України;

– кожен має право на інформацію, її вільне одержання, зберігання, використання та поширення, але реалізація такого права не повинна порушувати законні інтереси інших осіб;

– інформація є відкритою, водночас право на інформацію може бути обмежене у випадках, передбачених законом;

– держава зобов’язана забезпечувати доступ до інформації про свою діяльність;

– журналісти мають право на свободу джерела інформації;

– інформація не може бути використана проти волі її власника, крім випадків, передбачених законом;

– закон захищає право на конфіденційність.

Слід зауважити, що незважаючи на спрямовану проти України багаторічну збройну та інформаційно-психологічну агресію з боку Російської Федерації, в закон «Про інформацію», так і не було внесено норм щодо захисту вітчизняного інформаційного простору в умовах війни.

Проте, повертаючись до перших років незалежності України, необхідно відзначити, що одним із кроків на шляху нашої держави до демократичного суспільства та формування незалежних ЗМІ стало ухвалення у листопаді 1992 року Закону «Про друковані засоби масової інформації (пресу) в Україні» [65].

У 1994 році було створене Міністерство у справах преси та інформації України [211], завданням якого стало забезпечення розвитку засобів масової інформації, а також контроль за дотриманням законодавства в умовах реформування української інформаційної системи.

Ше за два роки, влітку 1996 року була прийнята Конституція України [98], яка, серед іншого, встановила права та свободи громадян в інформаційній сфері, а також забезпечила законодавчу базу для розвитку інформаційного права та інформаційної безпеки. Зокрема, Конституція України гарантує свободу слова та думки, право на інформацію, а також право на захист персональних даних. Крім того, Основний закон встановлює принципи відкритості та прозорості державної влади та забезпечує право громадян на доступ до інформації про діяльність державних органів та органів місцевого самоврядування.

Зазначимо, що однією з ключових є 17 стаття Основного Закону, яку часто цитують: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [98]. Проте, потрібно зауважити, що наразі невідомо, що мав на увазі законодавець, вводячи поняття «інформаційна безпека». Зокрема, у 1997 році Конституційним судом було винесено рішення про те, що в Україні поняття «інформаційна безпека» законодавчо не визначене [181]. Тому кожен вкладає свій зміст в положення зазначеної статті.

Натомість, у січні 1997 року було прийнято Концепцію національної безпеки України [158], яка діяла до прийняття Закону України «Про основи національної безпеки України» у 2003 році [63]. В Концепції було

заявлено про загрозу інформаційної експансії з боку іноземних держав та визначено основні напрями державної політики у цій сфері. «У такий спосіб підкреслювався перспективний характер загальних положень Концепції щодо формування необхідної законодавчої бази у сфері національної безпеки України» [67].

Концепцією було визначено загальні заходи забезпечення національної безпеки та стабільності України, а також передбачено інтеграцію зі світовими структурами безпеки, підвищення міжнародного співробітництва та дотримання міжнародних стандартів у цій сфері. Крім того, Концепція визначила ролі різних галузей влади у забезпеченні національної безпеки та створенні сприятливих умов для їхнього співробітництва. Однак, такий широкий підхід зумовив наукову дискусію щодо тлумачення терміну«національні інтереси», а також переліку таких інтересів та їх систематизації [101; 142, С. 97; 155; 193], і ця дискусія тривала до 2018 року, коли було прийнято Закон «Про національну безпеку України» [62].

Водночас, у 1998 році на урядовому рівні було створено Комісію з питань інформаційної безпеки [214], яка працювала до 2000 року як дорадчий орган. До основних завдань Комісії було віднесено розроблення концептуальних засад та проектів рішень з питань забезпечення інформаційної безпеки України, підготовку пропозицій щодо організації та координації діяльності міністерств, інших центральних органів виконавчої влади у сфері забезпечення інформаційної безпеки, контроль за її здійсненням тощо [164]. Основними здобутками роботи Комісії стали «перші концептуальні обгрунтування категоріально-понятійного апарату інформаційної та інформаційно-психологічної сфери та адаптація зарубіжної термінології до українських реалій» [72].

Період з 1998 по 2005 рік можна назвати новим етапом процесу формування нормативно-правової бази у сфері забезпечення інформаційної безпекиу зв’язку зі швидким розвитком новітніх інформаційних

технологій. Проте зауважимо, що в цей час основний наголос робився саме на технічному аспекті забезпечення інформаційної безпеки. Зокрема, було прийнято Закон «Про концепцію Національної програми інформатизації» [59], розроблені законопроекти про «Про інформаційний суверенітет та інформаційну безпеку України (1999) [168], «Про Концепцію розвитку державної інформаційної інфраструктури України (2002) [44], «Про інформаційну безпеку України» (2004) [169].

Також у 2002 році Державним комітетом інформаційної політики і телерадіомовлення України була розроблена Концепція національної інформаційноїполітики України [159], яка встановлювала стратегічні переваги розвитку національної інформаційної системи, а також містила практичні рекомендації щодо її впровадження. Згідно з проектом концепції, основними перевагами національної інформаційної безпеки визначалися: розвиток інформаційної інфраструктури як складового економічного розвитку країни; створення умов для доступу громадян до інформації та забезпечення вільного обміну інформацією; забезпечення національної безпеки в інформаційній сфері, в тому числі захист від кібератак та кіберзлочинності; розвиток національної культури; забезпечення державного регулювання у сфері інформації та створення сприятливих умов для розвитку інформаційного бізнесу в Україні. Але ця концепція так і не була прийнята з ряду причин. Найбільш суттєвим чинником стало те, що влада, політичні еліти і саме суспільство не були готові до такого рівня розвитку інформаційних технологій, який був передбачений у концепції. Також через складну економічну та політичну ситуацію в країні національна інформаційна політика на той час не була пріоритетним завданням і не викликала належної уваги. Крім того, концепція не була достатньо відкритою та прозорою і не враховувала думку та інтереси різних суспільних груп, а також не містила чіткої стратегії та плану дій.

Однак зауважимо, що аналітична та законотворча робота щодо розвитку інформаційної сфери тривала, і в 2006 році була прийнята «Концепція розвитку інформаційного суспільства в Україні до 2015 року» [63], яку було оновленоу 2013 році [183]. Цей документ містив більш конкретні та реалістичні стратегії і заходи щодо розвитку інформаційної інфраструктури та розвитку інформаційного суспільства в Україні.

Потрібно зазначити, що законотворчий процес у сфері забезпечення національної безпеки рухався досить повільно, а сам термін «національна безпека» був закріплений на законодавчому рівні лише у 2003 році після ухвалення відповідного закону [63]. Важливо, що поряд із захистом інформаційних прав людини і громадянина закон проголосив об'єктом захисту інформаційне середовище. Також цим законом було визначено порядок вироблення державної політики у сфері національної безпеки, зокрема, через прийняття в установленому порядку стратегічних документів у вигляді доктрин, концепцій, стратегій та програм, в тому числі в інформаційній сфері.

Цікаво, що до переліку загроз національній безпеці та національним інтересам України в інформаційній сфері було віднесено намагання маніпулювати громадською думкою через поширення недостовірної, неповної або упередженої інформації, але законодавець розглядав їхв основному як загрози внутрішнього характеру, що демонструє правову свідомістьв країні на той час.

В наступні роки законодавець все більше акцентує увагу на виробленні державної стратегії щодо захисту національної безпеки, зокрема, з урахуванням можливих загроз інформаційного характеру. На початку 2007 року була затверджена Стратегія національної безпеки України [215], в якій одним з ключових завданьвизначено забезпечення національної безпеки в умовах глобалізації та інформаційно-комунікаційних технологій.

Крім того, стратегія наголошувала на необхідності розвитку демократії, правової влади та підвищення рівня безпеки громадян. Це означало, що національна безпека повинна забезпечуватися не тільки за допомогою військової сили, а також за допомогою демократичних інститутів, правопорядку та захисту прав людини. Водночас, є очевидним, що в межах удосконалення системи інформаційної безпеки основну увагу було спрямовано на захист інформаційно-комунікаційних технологій та інформаційно-аналітичну підтримку діяльності органів державної влади, і нічого не було зроблено в напрямі протидії деструктивним інформаційно-психологічним впливам.

У січні 2007 року також було ухвалено Закон «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [60], яким було встановлено пріоритетні напрями розвитку інформаційного суспільства в Україні на вказаний період, зокрема: створення інформаційної інфраструктури та забезпечення доступу до неї для всіх громадян України; підвищення рівня інформаційної культури населення та забезпечення доступу до інформації та знань; розвиток електронної демократії та електронного урядування; розвиток електронної комерції та створення умов для розвитку інформаційного бізнесу в Україні; захист інформаційної безпеки держави та громадян; розвиток інформаційної та телекомунікаційної галузей України. Закон також визначив основні завдання та принципи розвитку інформаційного суспільства і встановив механізми державного регулювання та захисту прав та свобод громадян в інформаційному просторі. Крім того, він передбачив залучення до розвитку інформаційного суспільства громадських організацій, науково-дослідних установ та підприємств, а також міжнародну співпрацю у цій сфері. Однак зауважимо, що так само, як і при виробленні Стратегії національної безпеки України [215], законодавець зосередив увагу майже винятково на сфері інформаційно-комунікаційних технологій, внаслідок чого інформаційну безпеку він пов’язує суто з технічними аспектами,

такими як захист ресурсів, інфраструктури і технологій. Натомість, Доктрина інформаційної безпеки України [41], яка базувалася на положеннях цього закону, вже визначала інформаційну безпеку в тому числіі як захист від інформаційно-психологічного впливу. Серед основних принципів забезпечення інформаційної безпеки було виділено, зокрема, достовірність, повноту та неупередженість інформації, яка поширюється в інформаційному просторі, хоча й розглядався такий вплив здебільшого як внутрішня загроза.

Окремо зауважимо, що прийняття згаданої Доктрини мало важливе значення для вироблення державної політики в усіх сферах: зовнішньо-політичній, сфері державної безпеки, воєнній, внутрішньо-політичний, економічній, соціальній та гуманітарній; науково-технологічній та екологічній, – оскільки в положеннях Указу Президента про її затвердження зазначалося, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки і водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Цей документ діяв протягом семи років і втратив чинність у зв'язку з підписанням в.о. Президента України О.Турчиновим Указу«Про рішення Ради національної безпеки і оборони України «Про скасування деяких рішень Ради національної безпеки і оборони України» та визнання такими, що втратили чинність, деяких указів Президента України» [219].

Варто нагадати, що в період з 2002 по 2010 рік тривала постійна робота над новою концепцією національно інформаційної політики України. У Верховній Раді було зареєстровано три різні проекти концепції, в редакції 2002, 2009 та 2010 років, однак влітку 2011 року законопроект був востаннє відкликаний, і концепція так і не була прийнята. Натомість влітку 2010 року було ухвалено Закон України «Про засади внутрішньої і зовнішньої політики» [61], який визначив пріоритетні напрямки діяльності держави з покладенням на неї обов'язку забезпечувати інтереси людини, гарантувати захист прав та свобод громадян, сприяти їх розвитку та

самореалізації, а також створювати умови для розвитку громадянського суспільства та зміцнення демократії та права.

За два роки після ухвалення цього закону, у червні 2012 року було затверджено оновлену редакцію Стратегії національної безпеки України [217], яка визначила інформаційні права людини як одну з основних складових безпеки і розвитку держави: держава зобов'язана забезпечити права громадян на свободу висловлювання, інформаційну прозорість та доступ до інформації, а також захистити їх від інформаційних загроз. Крім того, у Стратегії визначено такі пріоритетні напрямки діяльності держави в галузі інформаційної безпеки, як забезпечення захисту інформації від несанкціонованого доступу, використання та розповсюдження; підвищення рівня кібербезпеки та захисту від кіберзагроз; розвиток ефективної інформаційної політики та комунікації з громадськістю; створення національної системи забезпечення інформаційної безпеки; підвищення кваліфікації фахівців у галузі інформаційної безпеки. Проте, як зазначає В. Горбулін [136], цей документ не мав необхідного юридичного статусу, оскільки був затверджений розпорядженням Кабміну, а не ухвалений у вигляді закону.

У 2014 році, внаслідок військової агресії з боку Росії, розпочалася трансформація національного інформаційного законодавства [51] – відбулися кардинальні зміни у вимірі відносин між державою і громадянським суспільством. Зокрема, 28 квітня 2014 року Рада національної безпеки і оборони України прийняла Рішення «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [172], введене в дію Указом Президента 1 травня 2014 року [219]. У документі зазначається, що інформаційна безпека є невід'ємною складовою національної безпеки і має бути забезпечена належним чином. Також наголошується на необхідності захисту прав та свобод людини в інформаційному просторі та необхідності захисту державної інформації і запобігання її втраті, викраденню та

поширенню. Крім цього, Рішенням передбачається створення ефективної системи реагування на кібератаки та кіберзлочини, а також наголошується на важливості забезпечення захисту інформації в критичних інфраструктурах.

За рік, у травні 2015 року Указом Президента на зміну Стратегії інформаційної безпеки, затвердженої указом Віктора Януковича [217], було сформовано нову Стратегію національної безпеки України [220]. Відповідно до викликів і загроз на той період часу документом були визначені основні пріоритети державної політики у сфері інформаційної безпеки, зокрема, наступальні дії з боку Україні як асиметрична відповідь на всі форми і прояви інформаційної агресії з боку Росії; впровадження інтегрованої системи виявлення та оцінювання інформаційних загроз і адекватної оперативної відповіді на них; протидія російським інформаційно-психологічним операціям, спробам маніпулювати громадською думкою шляхом поширення неправдивої або спотвореної інформації; вироблення державної інформаційної політики, що відповідає вимогам часу; виявлення джерел поширення деструктивного контенту в інформаційному просторі України та унеможливлення їх діяльності; створення і розвиток спеціальних державних структур, що відповідають за протидію дезінформації з урахуванням досвіду країн-членів НАТО, підвищення медіаграмотності та медіакультури населення. Також вперше було розмежовано поняття безпеки інформації як захисту даних з погляду новітніх інформаційних технологій, й безпечності інформації як захисту людини та суспільства від деструктивних інформаційно-психологічних впливів. Серед недоліків Стратегії варто відзначити відсутність чіткого термінологічного визначення таких ключових понять, як «інформаційна війна», «інформаційна безпека», «національні інтереси», «дезінформація». Проте, слід відзначити, що ця проблема властива багатьом законодавчим документам стратегічного спрямування. Крім того до недоліків Стратегіїможна віднести занадто широкі пріоритети, які було складно

реалізувати в короткі терміни, оскільки вимагализначних інституційних реформ.

Після прийняття оновленої Стратегії національної безпеки, у лютому 2017 року була затверджена Доктрина інформаційної безпеки України [223], яка визначала національні інтереси України в інформаційній сфері та уточнювала засади вироблення державної інформаційної політики в умова гібридної війни, яку розпочала проти України Російська Федерація.

Згідно з положеннями Доктрини, завдання держави, як відповідь на актуальні загрози безпеці України в інформаційній сфері полягають в наступному: захист інформаційної безпеки, захист і розвиток вітчизняного інформаційного простору та конституційних прав громадян на інформацію, відкрита та прозора державна політика, формування та підтримання позитивного іміджу України у світі. Також з ухваленням Доктрини в офіційний обіг було впроваджено нові терміни у сфері стратегічних, урядових та кризових комунікацій, а також вироблення стратегічних наративів. Недоліком Доктрини можна назвати занадто широкий список державних пріоритетів, який вона містила, що розмивало їх першочергову важливість та в кризових умовах гібридної війни і відкритих бойових дій не сприяло їх досягненню.

Наступним важливим кроком, спрямованим на формування нової державної політики у сфері інформаційної безпеки, стало ухвалення в 2018 році закону «Про національну безпеку України» [62], який встановив фундаментальні принципи та засади національної безпеки та оборони, а також цілі та основні принципи державної політики, покликані гарантувати захист від загроз всього суспільства та кожного окремого громадянина.

Ще через рік, у квітні 2019 року було підписано Указ Президента України щодо питань інтеграції України до Європейського Союзу та НАТО [224], що мало важливе значення для процесу наближення

українського законодавства до європейських норм. Урядові доручалося забезпечити виконання відповідного плану заходів, яким, зокрема, ставилося завдання до кінця 2019 року опрацювати спільно з ЄС перспективи поглиблення співпраці у сфері протидії дезінформації, зокрема розвиток співпраці з East StratCom Task Force.

У межах реформування системи державного управління у 2019-2020 роках було прийнято рішення про ліквідацію та перерозподіл його функцій між іншими міністерствами та відомствами, зокрема, переважну частину функцій Міністерства інформаційної політики передали до Міністерства культури, молоді та спорту України, яке згодом було реформовано у Міністерство культури та інформаційної політики.

На початку 2020 року Міністерство культури, молоді та спорту України, яке було утворене у 2019 році на заміну трьом ліквідованим Міністерствам: інформаційної політики, культури та молоді і спорту, винесло на широке громадське обговорення проект закону «Про протидію дезінформації» [126], однак цей законопроект одержав негативну оцінку з боку громадських організацій та правозахисників, зокрема через те, що його розробники невиправдано звузили поняття дезінформації, не давши йому точного та детального визначення, і цим не забезпечили належної якості закону [50].

Також у 2020 році було затверджено нову Стратегію національної безпеки України [225], якою оновлено перелік загроз національній безпеці України та визначено зусилля щодо набуття повноправного членства України в ЄС та НАТО стратегічним курсом держави. Важливою особливістю Стратегії є наявність переліку документів, які мають визначити шляхи та інструменти її реалізації. Одним з таких документів зазначено Стратегію інформаційної безпеки [227], яка замінила собою Доктрину інформаційної політики 2017 року.

Крім того, у 2021 році було видано Указ Президента України «Про Стратегію комунікацій з питань євроатлантичної інтеграції України на

період до 2025 року» [229], основні завдання якої передбачають забезпечення ефективної взаємодії між владою та суспільством, підвищення рівня поінформованості громадськості про процеси європейської та євроатлантичної інтеграції України та зменшення пов'язаних з цим процесом маніпуляцій та дезінформації. А за кілька днів до повномасштабного російського вторгнення в Україну, 16 лютого 2022 року Указом Президента України було ухвалено Стратегію забезпечення державної безпеки [230]. Зокрема, цим документом ще раз визначено головні завдання державної політики у сфері інформаційної безпеки, проте він не містить якихось інноваційних рішень та не передбачає радикальних змін у визначенні загроз та напрямів боротьби з ними.

Справді важливою подією 2022 року в законодавчому регулюванні інформаційної безпеки країни стало ухвалення у грудні Закону України «Про медіа» [66], який набув чинності 31 березня 2023 року. У зв'язку з його прийняттям втратили чинність закони «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про Національну раду України з питань телебачення і радіомовлення»; «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування засобами масової інформації» [66]. Цим законом розпочато медійну реформу в країні, проведення якої є однією з вимог, висунутих Європейським Союзом до України в рамках підготовки до набуття нею повноправного членства в ЄС. Закон в цілому одержав позитивні відгуки громадських організацій та індустріальних союзів. Крім регулювання вітчизняних медіа, в ньому багато уваги приділено війні та питанням протидії дезінформації. Зокрема, закон містить обмеження діяльності в Україні суб'єктів медіа, власниками яких є громадяни держави-агресора або юридичні особи, зареєстровані у державі-агресорі [66].

Узагальнену інформацію про формування нормативно-правової бази у сфері захисту інформаційної безпеки та протидії дезінформації в Україні наведено в табл. 1.1.

Таблиця 1.1

Формування нормативно-правової бази у сфері захисту інформаційної безпеки та протидії дезінформації

Рік	Правовий акт	Нововведення у сфері захисту інформаційної безпеки та протидії дезінформації
1992	«Закон про інформацію»	Встановлення основних принципів державної інформаційної політики.
1992	Закон «Про друковані засоби масової інформації (пресу) в Україні»	Формування незалежних ЗМІ.
1996	Конституція України	Встановлення прав та свобод громадян в інформаційній сфері; забезпечення законодавчоїу бази для розвитку інформаційного права та інформаційної безпеки.
1997	Концепція національної безпеки України	Визначення основних напрямів державної політики у сфері інформаційної безпеки, визначення ролей різних галузей влади у цьому процесі та визначення заходів щодо підвищення рівня міжнародного співробітництва.
1998	Закон України «Про концепцію Національної програми інформатизації»	Визначення стратегічних цілей та основних принципів інформатизації.
2003	Закону України «Про основи національної безпеки України»	Встановлення правової основи для забезпечення національної безпеки, включаючи захист інформаційних прав людини і громадянина, об’єкта захисту — інформаційного середовища, та визначення порядку розроблення стратегічних документів у цій сфері.
2006	Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку інформаційного суспільства в Україні до 2015 року»	Визначення заходів щодо розвитку інформаційних технологій, забезпечення доступу до інформації, цифровізації суспільства, підвищення інформаційної грамотності та розвитку інформаційної інфраструктури.
2007	Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»	Визначення пріоритетнихнапрямів розвитку інформаційного суспільства, а також встановлення механізмів державного регулювання та захисту прав громадян в інформаційному просторі.
2007	Указ Президента України «Про Стратегію національної безпеки України»	Визначення одним з ключових завдань забезпечення національної безпеки в умовах глобалізації та інформаційно-комунікаційних технологій.
2009	Указ Президента України «Про доктрину інформаційної безпеки України»	Визнання інформаційної безпеки як невід'ємної складової кожної зі сфер національної безпеки. Водночас інформаційна безпека визнається важливою самостійною сферою забезпечення національної безпеки
2010	Закон України «Про засади внутрішньої і зовнішньої політики»	Визначення пріоритетних напрямків діяльності держави з покладенням на неї обов'язку забезпечувати інтереси людини, гарантувати захист прав та свобод громадян, сприяти їх розвитку та самореалізації, а також створювати умови для розвитку громадянського суспільства та зміцнення демократії та права.

Продовження таблиці 1.1

2012	Указ Президента України «Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Стратегії національної безпеки України"	Визнання інформаційних прав громадян як ключової складової безпеки та розвитку держави, а також встановлення пріоритетних напрямків забезпечення інформаційної безпеки.
2013	Розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні.	Окреслення більш конкретних та реалістичних стратегій і заходів щодо розвитку інформаційної інфраструктури та розвитку інформаційного суспільства в Україні.
2014	Указ в.о. Президента України «Про рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»	Акцентування уваги на інформаційній безпеці як складовій національної безпеки та захисті прав людини в мережі, критичних інфраструктурах та від кіберзлочинів.
2015	Указ Президента України «Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України"	Визначення пріоритетів державної політики, таких як захист від російської інформаційної агресії, створення системи виявлення загроз, підвищення медіаграмотності та медіакультури.
2017	Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України»	Визначення національних інтересів України в інформаційній сфері та уточнення засад вироблення державної інформаційної політики в умовах гібридної війни.
2018	Закон України «Про національну безпеку України»	Встановлення фундаментальних принципів та засад національної безпеки та оборони, а також цілей та основних принципів державної політики, покликаних гарантувати захист всього суспільства та кожного окремого громадянина від загроз.
2019	Указ Президента України «Про питання інтеграції України до Європейського Союзу та НАТО»	Надання урядові повноважень щодо забезпеченнчя виконання плану заходів стосовно співпраці з ЄС у сфері протидії дезінформації, включаючи розвиток співпраці з East StratCom Task Force.
2020	Указ Президента України «Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України"	Оновлення переліку загроз національній безпеці України і визначення заходів для отримання повноправного членства України в ЄС та НАТО як стратегічних напрямів державної політики.
2022	Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки»	Уточнення наявних та визначення додаткових пріоритетних напрямів державної політики у сфері забезпечення інформаційної безпеки.
2021	Указ Президента України«Про Стратегію комунікацій з питань євроатлантичної інтеграції України на період до 2025 року»	Визначення напрямів державної політики щодо забезпечення ефективної взаємодії між владою та суспільством, підвищення рівня поінформованості громадськості про процеси європейської та євроатлантичної інтеграції України та зменшення пов’язаних з цим процесом маніпуляцій та дезінформації.
2023	Закон України «Про медіа»	Початок медійної реформу в Україні відповідно до вимог Європейського Союзу у контексті підготовки до потенційного вступу в ЄС.

Джерело: узагальнено автором.

Підсумовуючи, можемо сказати, що починаючи з 1991 року в Україні державна інформаційна політика була спрямована переважно на забезпечення свободи слова та безпеку інформації, і значноменшою мірою орієнтована на безпечність самої інформації та захист громадян, суспільства і держави від потенційних загроз, які можуть виникнути внаслідок цілеспрямованого зовнішнього інформаційного впливу, а також всередині держави. Адже не можна забувати, що «наявність великої кількості різних національних груп, часто з відмінними ідентифікаційними, культурними та політичними позиціями, може призводити до напруженості» [85] в різних сферах, і передусім інформаційній. На нашу думку, це сталося через історичні та культурні чинники, такі як тоталітарне минуле України та невпевненість у своїй національній ідентичності, які спричинили бажання продемонструвати демократичні цінності та свободу висловлювання. Однакз часом усвідомлення необхідності забезпечення національної безпеки та захисту від інформаційних загроз почало зростати, і це спричинило формування нових стратегій та підходів до вироблення державної політики у сфері інформаційної безпеки.

1.3. Концептуальні підходи до розуміння механізмів вироблення державної політики у сфері протидії дезінформації

У рамках нашого дослідження важливо розкрити зміст механізмів вироблення державної політики та визначити роль і місце сфери протидії дезінформації в загальній системі державної безпеки України. Особливу увагу буде приділено аналізу основних теоретичних підходів та концепцій з метою більш глибокого розуміння сутності та характерних особливостей механізмів формування політики в зазначеній сфері. Це дозволить здійснити всебічний аналіз проблематики механізмів вироблення державної політики у сфері протидії дезінформації, оцінити їх

ефективність та запропонувати концептуальний підхід до вдосконалення таких механізмів.

Багатокомпонентність поняття «механізми вироблення державної політики» викликає необхідність розпочати його аналіз зі з'ясування наукових підходів до визначення феномену самої державної політики. В традиційному розумінні політика сприймається як «середовище взаємодії між різними соціальними групами: націями, народами, державами, партіями, владою і населенням, а також громадянами та їх об'єднаннями» [93, С. 27]. Крім того, політика визначається як «суспільне явище, забезпечуване правом і державою» [186], створених суспільством для реагування на його значущі проблеми.

Слід зазначити, що в україномовному середовищі може виникнути дефініційно-логічне ускладнення через використання терміну «політика» в кількох різних значеннях: в англійській мові, на відміну від української, розрізняють поняття «policy» (діяльність влади згідно з обраним курсом) і «politics» (боротьба за можливість зайнятись такою діяльністю, обравши власний курс) [246, С. 6]. В українській мові існує лише одне поняття – «політика». Однак в україномовному середовищі зазвичай, коли йдеться про «policy», вживається словосполучення «державна політика» або «публічна політика, а на позначення інших видів політик використовується просто термін «політика».

Однак в нашому дослідженні ми використовуємо термін «політика» у значенні «policy». Це означає, що вислови «державна інформаційна політика» та «інформаційна політика» або «державна політика у сфері протидії дезінформації» та «політика у сфері протидії дезінформації» є синонімічними та взаємозамінними. Варто відзначити, що державна політика, на відміну від політичної діяльності партій, рухів та інших добровільних об'єднань виражає загальні інтереси населення та є концентрованим відображенням інтересів [171]. Вона визначається як «головний інструмент реалізації базових цілей розвитку

суспільства" [Цит. 23]. Проте слід зазначити, що державну політику визначають як її офіційні суб'єкти – представники трьох гілок влади: законодавчої, виконавчої та судової, так і неофіційні учасники: представники бізнесу, політичні партії та громадські організації [83]. Таким чином, поняття "державна політика" відображає взаємодію держави з іншими акторами для досягнення визначених цілей у різних сферах життя.

У контексті протидії дезінформації державна політика охоплює широкий спектр стратегічних завдань, включаючи розробку та впровадження відповідного законодавства, забезпечення свободи слова і доступу до об'єктивної інформації, підтримку медіаорганізацій та підвищення інформаційної грамотності населення.

Поняття "протидія дезінформації" відображає комплекс заходів, спрямованих на виявлення недостовірної і маніпулятивної інформації та запобігання її поширенню.

Щодо розуміння суті більш загального терміну «державна політика», то існує кілька методологічних підходів, що охоплюють дослідження різних аспектів процесу прийняття рішень на державному рівні, формування та втілення державної політики, а також ролей акторів, процедур та контексту, що впливають на цей процес. Одним з найпоширеніших є діяльнісний підхід, який акцентується на вивченні самого процесу прийняття рішень, взаємодії між лідерами та втіленні публічної політики через реальні дії і програми. Прихильники такого підходу вважають, що державна політика формується та реалізується через конкретні дії та програми, які мають вплив на суспільство. Відповідно, вона розглядається як «політична діяльність держави та її органів» [14] (або «політична бездіяльність»,як зауважує ряд дослідників [151, 204, 187, 90]), тобто те, що уряди «вибирають робити або не робити» щодо певної суспільної проблеми [104, С. 5; 250, С.6]. В цьому ключі державна політика розглядається як «специфічна форма політико-управлінської

діяльності держави» [236, С. 321], «діяльність державних інституцій» [177, С. 6], «діяльність органів державної влади» та «взаємодія» [200], «сукупність повноважнихдій» [153] чи «послідовних дій» [108].

При цьому виокремлюється спрямованість таких дій на досягнення мети [186, С. 160] з наголосом на тому, що державну політику необхідно «відрізняти від щоденних рішень, які ухвалюють державні органи» [19, С. 39], оскільки вона «має більший масштаб, ніж рішення: вона є суттю послідовності рішень» [153]. Таким чином, державна політика тлумачиться як «курс дій» [187]; «план, курс дій, або напрям дій» [4, С. 75]; «напрям дій або утримання від них» [151, С. 22; 90, С. 5]; «курс дій уряду або його бездіяльність» [104, С. 6]; певний курс дій, «свідомо обраний з-поміж наявних альтернатив» [342, С. 11]; «напрям дій» [89, С. 122]; «напрям діяльності держави» [1, С. 35]; «наміри уряду» [30, С. 31]; «система цілеспрямованих заходів» [105, С. 35]; «стратегічний курс» [152, С. 66] та «стратегічні напрями» і «пріоритети» [89].

Така цілеспрямованість державної політики обумовлена необхідністю визначення мети та сенсу, які є необхідними елементами будь-якої суспільної діяльності [186, С. 160]. Основним завданням державної політики є розв’язання певної суспільної проблеми чи сукупності проблем або задоволення потреби (сукупності потреб) [205, С. 20]. Для досягнення цього необхідна «взаємодія багатьох агентів і організацій та встановлення складних взаємозв’язків між ними» [200], тому державна політика розглядається як «сукупність специфічних, неординарних дій, заходів та інститутів [200, С. 26; 86, С. 32].

Отже, відповідно до запропонованого підходу, державна політика визначається як сукупність заходів і дій, спрямованих на досягнення цілей та вирішення завдань, що виникають у суспільстві.

Існують й інші підходи до розуміння державної політики:як процесу прийняття рішень; сукупності нормативно-правових актів та заходів; результату діяльності інститутів державної влади;соціального процесу

взаємодії різних груп та інтересів у суспільствіта як системи, що включає цілі, завдання, ресурси, механізми тощо, «сконсолідовані на основі імперативної державної влади» [91]. Однак ці підходи мають свої обмеження, оскільки не враховують всіх аспектів державної політики, яка є складним та багатогранним феноменом, що потребує застосування різних підходів та методів аналізу. Тому традиційним є комплексний підхід до розуміння суті державної політики, а дослідження та аналіз здійснюються відповідно до ефективних галузей або сфер діяльності, на регулювання яких вона спрямована. Наприклад, економічна, соціальна, фінансова, правова, культурна, військово-промислова, інформаційна політика, політика національної безпеки тощо.

В рамках комплексного підходу вивчається специфіка галузі, в якій формується конкретна державна політика, її взаємодія з іншими галузями, рівень розвитку, проблеми та перспективи. Завдання, які вона вирішує, залежать від цієї конкретної сфери. Однак, загалом можна сказати, що державна політика «націлена на вирішення суспільних проблем, що потребують розв'язання, і реалізується органами публічного управління шляхом застосування відповідних механізмів та ресурсів» [170]. Державне управління, у свою чергу, виступає засобом реалізації такої політики [92].

Стратегічна спрямованість державної політики передбачає, що вона заснована на довгострокових цілях та завданнях. У контексті протидії дезінформації це означає необхідність вироблення довгострокових стратегій, спрямованих на ефективну протидію дезінформації з урахуванням різних аспектів, включаючи політичний, соціальний, культурний, економічний, технологічний контекст, що склався в певний період часу у країні та світі. Зокрема, політичний аспект передбачає аналіз політичного контексту, включаючи законодавство, політичні рішення, роль державних інституцій та інших акторів у формуванні та реалізації політики протидії дезінформації. Соціальний аспект охоплює аналіз суспільних процесів, демографічних змін, громадської думки та роль

широкої громадськості і громадських організацій, а також засобів масової комунікації у протидії дезінформації. Економічний аспект враховує економічні фактори поширення дезінформації та протидії їй, адже «недобросовісні фінансові заходи, які призводять до маніпуляцій або монополізації ринку медіа, можуть порушувати здорову конкуренцію» [54]. Тому важливо створювати механізми, які гарантуватимуть прозорість фінансових потоків і враховуватимуть економічні інтереси усіх зацікавлених сторін [54]. Технологічний аналіз включає оцінку застосування сучасних технологій, зокрема цифрових медіа, соціальних мереж, алгоритмів поширення та фільтрації інформації, ролі штучного інтелекту, онлайн-ботів та інших технологічних рішень.

Отже, підсумовуючи вищезазначене, можемо зробити висновок, що державна політика є сукупністю цілеспрямованих дій, які здійснюються суб'єктами державної політики відповідно до визначеного стратегічного напряму. Вона формується як відповідь на необхідність врегулювання суспільно значущого питання або розв'язання суспільно значущої проблеми.

З урахуванням того факту, що державна політика є складним поняттям, механізми її вироблення також є складними і багатогранними. Відповідно, і наукові погляди на сутність цих механізмів вирізняються різноманітністю, що обумовлює множинність підходів до їх визначення. Водночас важливо зауважити, що поняття механізмів вироблення державної політики у сфері протидії дезінформації не може бути зведене до сукупності механізмів протидії дезінформації, оскільки ці два поняття відображають різні аспекти діяльності держави у сфері протидії дезінформації.

Під механізмами протидії дезінформації розуміються інструменти та методи, що використовуються для захисту від дезінформації. Ці механізми включають заходи, спрямовані на виявлення, аналіз та контроль поширення дезінформації, а також засоби протидії їй.

Зі свого боку, механізми вироблення державної політики у сфері протидії дезінформації використовують процеси та інструменти для вироблення й оцінки стратегії та тактики протидії дезінформації на рівні державної політики. Ці механізми охоплюють аналіз ситуації в інформаційному просторі, визначення пріоритетних напрямів і цілей державної політики, розроблення планів та програм дій, а також координацію діяльності державних органів та інших структур.

Отже, механізми протидії дезінформації та механізми вироблення державної політики у сфері протидії дезінформації використовують два різні рівні дій, які тісно пов'язані та взаємодіють між собою для досягнення спільної мети – захисту національних інтересів держави. Проте, вони передбачають застосування різних технологій та стратегій.

Щодо з’ясування змістового наповнення поняття механізмів вироблення державної політики, то слід зазначити, що наукове середовище ще не має усталеного визначення самого терміну «механізм». Наприклад, В. Шемчук у своєму дослідженні теоретико-методологічних засад механізму захисту інформаційної безпеки держави [242], звертає увагу на етимологію слова «механізм», яке перекладається з грецької як «зброя» або «машина». Згідно з тлумаченням, запропонованимфахівцями інституту мовознавства ім. О. О. Потебні [195, С. 18], «механізм» може трактуватись як сукупність взаємопов’язаних елементів, що становлять певну систему для передачі та перетворення рухів.

У свою чергу, Б. Кормич у дослідженні державно-правового механізму інформаційної безпеки характеризує його як систему трьох взаємопов’язаних елементів: сукупність державних інституцій; сукупність ролей і відносин, а також форм і методів діяльності її суб’єктів; сукупність норм та принципів, які регулюють зміст і процес проведення державної політики [101, С. 132].

В. Ліпкан, Ю. Максименко та В. Желіховський трактують механізм захисту інформаційної безпеки як систему взаємопов'язаних і взаємоузгоджених інституцій [114, С. 137].

О. Приходько, розглядаючи механізм забезпечення безпеки з погляду державного управління, визначає його як систему, призначену для практичного здійснення державного управління та досягнення окреслених цілей, яка має певну структуру, методи, важелі, інструменти впливу на об'єкт управління з відповідним правовим, нормативним та інформаційним забезпеченням [46].

Схожим є підхід А. Нашинець-Наумової, яка розглядає механізм забезпечення інформаційної безпеки як систему різних засобів: політичних, кадрових, оперативно-розшукових, інформаційних, правових [141, С. 53]. Тоді як О. Зозуля розглядає державну політику крізь призму множинності різних механізмів [72, С. 45].

У свою чергу, О. Радченко під механізмом розуміє системну сукупність інституцій, структур, послідовних дій, форм, станів і процесів у державі [176]. Схожої думки дотримується В. Меркулов, який під механізмом розуміє систему інституційних (тобто організаційно оформлених) та неінституційних (або неформалізованих) цінностей, традицій, процедур, правил, зразків формування й функціонування органів виконавчої влади, розподілу між ними функцій, завдань та обов'язків, та взаємодію їх з недержавними за своєю природою інститутами громадянського суспільства [Цит. 15].

При цьому, у всіх визначеннях, які було розглянуто вище, присутнє слово «система». Зазначимо, що одним з перших вітчизняних науковців, хто досліджував концепцію системи як управлінської категорії, був Вадим Гетьман. Дослідник активно використовував системний аналіз та його застосування, а також розробив власні методи системного аналізу у політиці. Сьогодні це широко вживаний термін, який зустрічається у багатьох наукових дослідженнях різних галузей знань, оскільки визначає

будь-який комплекс, що складається з окремих взаємозамінних елементів та може мати різні форми.Таким чином, механізми вироблення державної політики можуть бути реалізовані як система, що містить безліч елементівта підсистем, які виконують свої функції та взаємодіють між собою задля досягнення визначеної мети.

Екстраполюючи такий підхід на предмет нашого дослідження, можемо сказати, що механізми вироблення державної політики у сфері протидії дезінформації є складною системою, яка складається з різних елементів, кожен з яких виконує свої функції у процесі формування та реалізації такої політики. Серед таких функцій можна виокремити розроблення та уточнення стратегії інформаційної безпеки, визначення пріоритетів та вибір оптимальних інструментів для ефективного захисту вітчизняного інформаційного простору тощо. Крім того, механізми вироблення державної політики включають систему моніторингу та оцінювання результатів, що дозволяє здійснювати коригування й оптимізацію процесу прийняття рішень на основі аналізу досягнутих результатів. Таким чином, підхід до визначення механізмів вироблення державної політики у сфері протидії дезінформації як до системи дозволяє розглядати цю проблему в комплексі, з урахуванням всіх її аспектів та взаємозв'язків між ними.

Підсумовуючи вищезазначене, можна сформулювати визначення механізмів вироблення державної політики у сфері протидії дезінформації як системи організаційних, інформаційних, правових та інших заходів, що мають на меті забезпечення ефективної державної політики у сфері протидії дезінформації, і взаємодіють між собою для досягнення визначеної мети. Ці механізми включають процес дослідження дезінформації та визначення загроз, які вона несе; розроблення стратегій, концепцій, програм та окремих політичних рішень щодо протидії дезінформації. Важливою складовою механізмів є визначення заходів та завдань, вибір інструментів та механізмів їх реалізації, а також оцінка

ефективності державної політики у зазначеній сфері. З метою забезпечення ефективної реалізації державної політики протидії дезінформації, механізми вироблення такої політики мають бути мультикомпонентними та детально пропрацьованими.

Водночас механізми вироблення державної політики у сфері протидії дезінформації можна розглядати як систему інститутів державної влади та громадянського суспільства, які беруть участь у відповідних процесах, таких як аналіз даних, розроблення стратегій, вибір інструментів та оцінка ефективності політики. При цьому не менш важливою складовою є координація їхніх дій та налагодження взаємодії між усіма акторами з метою реалізації спільних стратегій та дій. Також необхідні відповідне нормативно-правове та комунікаційне забезпечення.

Перелік інституцій, які можуть взяти участь у формуванні окремих політичних рішень, не є вичерпним або заздалегідь визначеним. Процес формування рішень, зокрема в експертно-аналітичному аспекті, може включати участь наукових установ, незалежних експертів та фахівців з різних галузей, як вітчизняних, так і зарубіжних, як самостійно, так і за запитом державних структур. У цьому контексті, механізми вироблення державної політики у сфері протидії дезінформації схожі на традиційні механізми вироблення державної політики в інших сферах, таких як економіка, право тощо.

Ключовими засадами державної політики у сфері протидії дезінформації є гарантування свободи слова та доступу до інформації, які є фундаментальними правами громадян. Важливо забезпечити баланс між вільним висловлюванням та захистом суспільства від неправдивої інформації та дезінформації.

Іншою важливою засадою є прозорість та відкритість державних інституцій, доступ до офіційної інформації та її публічне обговорення, що сприяє підвищенню довіри громадян до державної влади та зниженню можливостей поширення дезінформації.

Крім того, концептуальні засади державної політики у сфері протидії дезінформації включають використання інформаційних технологій та інструментів з метою забезпечення інформаційної безпеки громадян, суспільства і держави. Також важливо зосередитись на зміцненні міжнародної співпраці, обміні досвідом та координації зусиль різних країн у цій сфері. Ці концептуальні засади можуть скласти основу для вироблення ефективної державної політики у сфері протидії дезінформації.

Отже, системний підхід до визначення механізмів вироблення державної політики у цій сфері включає аналіз різних складових, таких як законодавча база, інституційна структура, фінансові ресурси, технічні можливості, комунікаційні стратегії тощо. Досліджується взаємодія цих елементів та їх вплив на формування і реалізацію державної політики у сфері протидії дезінформації, яка є складним і багатовимірним процесом.

Завершуючи аналіз складових елементів вироблення державної політики у сфері протидії дезінформації та їх взаємодії, переходимо до розгляду ще одного важливого аспекту нашого дослідження: ролі та місця сфери протидії дезінформації в загальній структурі забезпечення національної безпеки.

Згідно з чинною Стратегією інформаційної безпеки [227], сфера протидії дезінформації є структурним елементом системи забезпечення інформаційної безпеки. Тому можна стверджувати, що державна політика у сфері протидії дезінформації, яка є предметом нашого дослідження, пов’язана з інформаційною безпекою як частина та ціле. Протидія дезінформації є необхідним компонентом інформаційної безпеки, і національна безпека не може бути забезпечена без врахування інформаційної складової. Аналогічно, інформаційна безпека не буде всеохоплюючою в разі позбавлення її вектора, спрямованого на протидію дезінформації.

Проте необхідно зауважити, що саме поняття "інформаційна безпека" має велику кількість вимірів, різниця між якими полягає у

підходах, з яких розглядається це питання. Навіть за наявності певних принципових узгоджень щодо методології та системи світогляду між представниками різних галузей знання, відразу помітні розбіжності в їх баченні сутності та змісту інформаційної безпеки. Інакше кажучи, науковці, чиї дослідження мають спеціалізований характер, наповнюють термін власним змістом, і таким чином поняття дезінформації, як і методи протидії їй, розглядаються з двох позицій, які умовно можна поділити на технологічну і гуманітарну.

Технологічний підхід ототожнює поняття інформаційної безпеки з кібербезпекою і розглядає протидію дезінформації як захист даних від їх несанкціонованої модифікації чи знищення (М. Кондратюк [96], І. Логінов [115]). Тоді як науковці, що розвивають гуманітарний підхід (О. Литвиненко [111], А. Турчак [209], О. Дзьобань і В. Пилипчук [38], О. Горбатюк [20], В. Гурковський [25, С. 28], К. Захаренко [67], В. Фурашев [233, С. 55], Т. Ткачук [208]), об'єктом захисту визначають життєво важливі особистісні, суспільні і державні інтереси. Зокрема, Г. Ситник, наполягаючи на об'єктивно-суб'єктивній природі інформаційної безпеки, розглядає її як «атрибут буття об'єктів живої природи і соціальних взаємодій» [191].

В. Ліпкан, Ю, Максименко та В. Желіховський розглядають забезпечення інформаційної безпеки як комплексну проблему та виокремлюють три її аспекти*:* інформаційно-технічний, який забезпечує управління потенційними або реальними загрозами з метою захисту комп'ютерних, телекомунікаційних технологій та інших технологій зв'язку; інформаційно-психологічний, що передбачає управління реальними або потенційними загрозами, які можуть завдати шкоди психіці людини та суспільству; інформаційний, під яким розуміється забезпечення прав і свобод людини в інформаційній сфері (право на доступ до інформації і право на конфіденційнійсть персональних даних) [114, С. 137].

Важливо зазначити, що поряд із терміном «інформаційна безпека» активно використовується термін «безпека інформації». Хоча ці поняття взаємопов'язані, вони не є взаємозамінними. Науковці, зокрема Н. Волошина, зазначають, що на початковому етапі формування наукового розуміння цих категорій спостерігалося їх ототожнення, однак наразі переважна більшість дослідників чітко розмежовує ці поняття [14]. В одному випадку йдеться про вплив на системи обробки і зберігання даних, внаслідок чого захисту потребує інформація, а в іншому – загрозу несе сама інформація, і в такому разі актуальності набуває проблема захисту від неї. Інакше кажучи, сама сутність феномена безпеки обумовлює обов'язковий вибір об'єкта, без якого це поняття втрачає внутрішній зміст. Якщо об'єктом безпеки є інформація, то терміни «інформаційна безпека» та «безпека інформації» стають синонімами.Але якщо об'єктом захисту виступає будь-який інший учасник інформаційних відносин, то у словосполученні «інформаційна безпека» слово «інформаційна» вже починає нести уточнююче навантаження, а сам термін трактується як стан захищеності зазначеного об'єкта від загроз в інформаційній сфері. Таким чином, розглядаються різні спектри загроз, в залежності від того, що розуміється під «інформаційною безпекою» – безпека інформації чи її безпечність.

Зауважимо, що проблема забезпечення інформаційної безпеки в аспекті захисту самої інформації більш досліджена та регулюється низкою нормативно-правових документів, тоді як гуманітарний аспект розроблений менш докладно. Це пояснюється тим, що проблема захисту свідомості людини від деструктивного інформаційного впливу набула гостроти лише в останні роки, а сам «інститут інформаційної безпеки людини в Україні і світі є наймолодшим» [73].

Зміну пріоритетів обумовила розпочата у 2014 році гібридна війна проти України з боку РФ, в якій ключовим компонентом стала інформаційна складова. Концепція протидії дезінформації як руйнівному

інформаційному впливу на свідомість людей набула нормативного визначення в Доктрині інформаційної безпеки України у 2017 році [223], але сам термін «дезінформація» вперше був згаданий у Стратегії національної безпеки України в редакції 2020 року [225]. Проте, останній документ також не містить визначення дезінформації, а ототожнює це поняття з неправдивою інформацією, що суттєво розмиває його первинний зміст [75]. Не набуло законодавчого визначення це поняття і в Законі про медіа [66], який фахівці вважають кодифікацією інформаційних законів [43]. Таким чином в Україні склалася парадоксальна ситуація, коли вже створено окремі державні структури [228, 231], але немає офіційного визначення самого об'єкта, якому ці структури мають протидіяти.

Сформулювати таке визначення і буде завданням наступного розділу нашого дослідження, оскільки поняття дезінформації є базовим в теорії і практиці механізмів вироблення державної політики у сфері протидії цьому явищу.

1.4. Термінологічне визначення поняття «дезінформація» як базової категорії в проблематиці вироблення механізмів державної політики у сфері протидії дезінформації

Проблема дезінформації, породжена новими видами небезпек та загроз, є однією з актуальних тем, яка привертає увагу дослідників. Кількість наукових праць на зазначену тему постійно зростає, однак розбіжності в трактуванні самого феномену дезінформаціїчасто призводять до неправильного його розуміння. Вчені, які працюють у сфері інформаційної безпеки, згодні з тим, що надати вичерпне визначення цьому терміну вкрай складно, оскільки дезінформація є широким і динамічним поняттям, яке може приймати багато різних форм. Водночас, відсутність єдиного та чіткого визначення стає перешкодою у виробленні спільних методологій та стратегій протидії цьому явищу [50]. Отже, метою

цього розділу дослідження є розкриття поняття дезінформації, визначення його ключових складових та уточнення взаємозв'язку з іншими поняттями, пов'язаними з інформаційною безпекою.

Варто зауважити, що хоча явище дезінформації відоме з давніх часів [305], сам термін з'явився порівняно недавно. Зокрема, Oxford Living Dictionary зазначає, що це поняття закріпилося в Європі у 50-х роках минулого сторіччя і мало російське походження [320]. Українські науковці стверджують, що термін "дезінформація" був введений у використання у 1920-і роки в СРСР [45, С. 9] для позначення конкретних технологій, які застосовували розвідувальні служби з метою поширення хибної інформації для дезорганізації супротивника.

В цей само час американський журналіст У. Ліппман детально описав техніку дезінформації, яка використовувалася в СРСР [307]. Проте, Ліппман вважав, що радянська влада використовувала хибну інформацію не для боротьби з противником, а для переконання власного населення у правильності її політики та придушення будь-яких опозиційних думок.

Згодом на Заході були створені спеціальні дослідницькі центри та відділи, що займалися аналізом радянської дезінформації. Зокрема, проблему дезінформації як інструменту геополітичної боротьби та контролю над масами досліджували Г. Шиллер [328], С. Девіс [262], Р.Шульц і Р. Годсон [330] та інші західні вчені. Крім того, у 1984 році під час слухань перед Постійним комітетом з розвідувальної діяльності Палати представників США було оприлюднено Звіт ЦРУ про радянську приховану діяльність, відомий також як звіт Бореля [339]. У цьому документі докладно розглядалися методи і тактики, які використовувалися радянськими спецслужбами для дезінформації.

Після розпаду Радянського Союзу й денонсації Варшавського договору, що призвело до закінчення холодної війни, західні вчені продовжили вивчати феномен дезінформації. Головною темою їхніх досліджень стало вивчення впливу нових інформаційних технологій на

поширення дезінформації. У 2003 році А. Маттеларт [311] зазначав: «Інформації стало так багато, що ні порозумітися, ні розібратися в ній вже практично неможливо». У зв'язку із цим різко зріс інтерес до теми інформаційної безпеки. Все більше людей почали усвідомлювати, що дезінформація може серйозно впливати на громадську думку, вибори, геополітичні конфлікти та міжнародні відносини. Зрештою,вибори в США у 2016 році та наступні вибори в Європі з відчутним дезінформаційним впливом Росії привернули увагу до проблеми дезінформації та кібербезпеки на міжнародному рівні.Але ще до втручання Росії в американські та європейські вибори, своєрідним каталізатором процесу, який призвів до збільшення обізнаності світової громадськості щодо проблеми дезінформації та значного розвитку наукових досліджень у цій галузі, стала анексія Росією Криму у 2014 році та події, які за цим послідували.

Проте, слід зауважити, що незважаючи на підвищений інтерес до феномену дезінформації, до цього часу відсутній єдиний підхід до розкриття його сутності. Широке трактування цього поняття в наукових та медійних дискурсах порушує його семантичне наповнення, що призводить до ототожнення дезінформації із суміжними поняттями «обман», «помилка», «фейк», «маніпуляція» тощо. Разом з тим, поставлене перед нами завдання вдосконалення механізмів вироблення державної політики у сфері протидії дезінформації вимагає диференціації кожного з цих понять та конкретизації їхнього змісту.

В енциклопедичній і довідковій літературі термін «дезінформація» найчастіше подається через більш широке поняття неправдивої, недостовірної або хибної інформації. Зокрема, академічний тлумачний «Словник української мови» трактує дезінформацію як «введення в оману невірною інформацією» [195, С. 231], при цьому нічого не говориться про намір або мету, з якою поширюється така інформація. Великий тлумачний онлайн-словник сучасної мови повністю повторює таке визначення [10].

Подібне трактування зустрічаємо і в англомовних джерелах – зокрема Cambridge Advanced Learner's Dictionary & Thesaurus визначає дезінформацію як неправдиву інформацію, поширену з метою ввести людей в оману [257]. Оксвордський тлумачний словник англійської мови трактує дезінформацію як «хибну інформацію, спрямовану на введення в оману» [320]. «Вісник НАТО» також пропонує розуміти під дезінформацією «сфабриковані розповіді, створені для введення в оману» [13]. Тобто, йдеться про намір введення в оману як про усвідомлений акт діяльності людини.

Зауважимо, що науковці й раніше розглядали дезінформацію саме під таким кутом зору. Зокрема, у 2003 році навмисний характер поширення неточних та неправдивих даних при дезінформуванні відзначили хорватські вчені М. Туджман та Н. Мікеліч [338], а роком пізніше на «свідомий обман щодо правди» звернув увагу американський дослідник Джеймс Фетцер [288]. Україномовний Короткий філософський словник 2004 року також вказує на прагнення інформатора ввести реципієнта у стан омани, однак зауважує, що «дезінформація може бути і неусвідомленою, не перестаючи при цьому бути неправдою» [103].

Т. Попова та В. Ліпкан не погоджуються з таким підходом. Дослідники наголошують, що йдеться не про прикру помилку, зроблену не усвідомлено, а про навмисне ведення в оману, що і є метою дезінформації [157].

При цьому «Тлумачний словник українських термінів» вказує на не просто навмисний, а саме на зловмисний характер дезінформації, пропонуючи розуміти під цим поняттям будь-які недостовірні відомості, поширені із злочинною метою» [32]. На злому умислі наголошує й «Економічна енциклопедія», характеризуючи мету, з якою поширюється «неправильна інформація», як «антигуманну» [284].

В сучасних європейських та американських джерелах так само наголошується на зловмисному характері поширення дезінформації [32,

285, 338], і саме такий підхід зафіксовано у звіті британської Government Communication Service, що визначає дезінформацію як «навмисне створення та поширення» хибної, неточної чи невірної інформації [295]. У свою чергу, Л.Флоріді, протиставляючи інформацію дезінформації, говорить про останню як про хибні дані, які «цілеспрямовано поширюються з метою того, щоб отримувач повірив, що ці дані є інформацією» [290]

Українські науковці погоджуються з тим, що на відміну від помилки, незнання, недооцінки чи перебільшення, дезінформація є обманом свідомим [154; 161; 144, С. 27]. Метою такого обману є намір подати об'єктові інформацію, «яка вводить його в оману стосовно справжнього стану справ та створює викривлену реальність» [87]. Тобто дезінформація є умисним викривленням та поширенням хибних тверджень [156] з намаганням нав'язати об'єкту «неправдиве, спотворене і просто брехливе уявлення про реальну дійсність» [3].

Зауважимо, що в англомовному середовищі для диференціації недостовірної інформації вживають два терміни: дезінформація (disinformation) та місінформація (misinformation). Ключовим при такому поділі є фактор умисності: дезінформація – це завжди «навмисне введення в оману або упереджена інформація» [264], тоді як помилковою інформацією (misinformation) є та, «в яку вірять люди, які її поширюють». Такого підходу притримуються К. Вордл [345], Б. Шталь [332], Л. Флоріді [289], П. Беднар [253] та інші американські дослідники.

Другий критерій, за яким розрізняють дезінформацію та місінформацію, – це намір завдати шкоди. Якщо недостовірний контент створюється навмисно і з усвідомленим наміром завдати об'єктові шкоди, то можемо говорити про дезінформацію. Натомість місінформація – це ненавмисні помилки у публікаціях, коли автор не усвідомлює того, що інформація не відповідає дійсності, і при цьому не має наміру комусь зашкодити [345, 332, 289, 253].

Але потрібно зауважити, що водночас багато філософів вважають взаємний обман невід'ємним атрибутом соціуму. Як стверджує Ю. Харарі [235, С. 290], «ери правди ніколи не було», а Чарльз В. Форд доводить, що здатність обманювати – необхідна навичка людини, без якої нормальне соціальне спілкування неможливе [240]. О. Фрай також переконаний, що в умовах абсолютної правдивості суспільне життя немислиме, і цілковиту правдивість індивіда слід відносити, швидше, до патології, ніж до соціального ідеалу [344]. Тож можемо припустити, що це явище властиве всій людській цивілізації та охоплює майже всю історію людства [3]. При цьому очевидним є те, що неможливо обманути неусвідомлено (якщо йдеться не про прикру помилку, а саме про обман) Тож мають бути додаткові критерії чи певні умови, за яких хибні повідомлення виходять за рамки звичайного обману, і з'являються підстави говорити про дезінформацію.

Ряд дослідників такою підставою вважають намір суб'єкта завдати шкоди державним або суспільних інтересам, що може бути реалізовано через вплив на громадську думку [138, 119, 256, 322, 19]. Зокрема, корпорація RAND звертає увагу на те, що при виявленні недостовірної інформації перш за все слід звертати увагу на мету її поширення (аби з'ясувати,чи є це спробою вплинути на громадську думку) [322]. Схожий зміст вкладає у пояснення мети дезінформації українська «Економічна енциклопедія»: «ввести в оману громадську думку, викликати певну реакцію в адресата» [284]. А словник термінів на сайті телекомпанії Deutsche Welle (DW) конкретизує це визначення, трактуючи дезінформацію, як спробу «створити помилкове враження і, відповідно, підштовхнути об'єкт впливу до бажаних дій чи бездіяльності» [263].

Цікаво, що подібний підхід демонстрував і радянський «Контррозвідувальний словник», який визначав дезінформацію як спеціально підготовлені відомості для створення у супротивника невірного

уявлення про дійсність, на основі якої він може ухвалювати рішення, вигідні стороні, що дезінформує [Цит. 45].

Такі «відомості» можуть бути використані для виправдання воєнних дій, створення в країні обстановки хаосу та невизначеності, що може призвести до відсутності контролю з боку влади та відключення державних інституцій. Тому ряд дослідників вважають, що при визначенні дезінформації важливіше говорити не про намір (ввести об'єкт впливу в оману) і не про мету (підштовхнути його до прийняття певних рішень), а про наслідки, які несе за собою поширення недостовірної інформації.

Щодо цього в сучасному науковому дискурсі існує дві точки зору. Одні науковці пропонують вважати дезінформацією будь-які хибні відомості, поширені в інформаційному просторі, оскільки «в наш час дезінформація може і не переслідувати конкретної мети, визначеної чиїмись інтересами. Але від цього вона не стає менш небезпечною, оскільки так само впливає на процес прийняття рішень» [9], тоді як інші говорять про дезінформацію, як про неправдиву інформацію, що «має або може мати негативні наслідки для реалізації конституційних прав громадян та/або загрожувати національній безпеці» [138]. Подібну позицію зустрічаємо і в англомовному дискурсі, де стверджується, що крім того, що дезінформація породжує безлад та викривлює суспільні дискусії [32], вона є небезпечною, оскільки спрямована на те, щоб викликати розкол суспільства, завдати йому шкоди загостренням існуючих конфліктів та підірвати довіру до інститутів державної влади [256]. Зокрема, Кодекс ЄС з протидії дезінформації, визначає це явище як таке, що«може завдати суспільної шкоди, як-от загроза демократичним політичним процесам та процесам розроблення політик, захисту здоров'я громадян ЄС, довкілля або безпеки».

Цікаво також проаналізувати, як з огляду на характер наслідків і шкоди, яких може завдати поширення хибних відомостей, співвідносяться між собою поняття «дезінформація» і «фейк». У всі періоди розвитку

цивілізації фейки як форма деструктивного впливу на людську свідомість привертали увагу та вивчалися науковцями і суспільними діячами [49]. У сучасному науковому дискурсі існують два протилежні погляди: ряд дослідників розглядають фейк як окремий феномен, відмінний від суміжного поняття «дезінформація», тоді як в інших джерелах ці два терміни подаються як взаємозамінні [107, 166].

Перш ніж досліджувати взаємозв'язок між поняттями «дезінформація» та «фейк», необхідно сформувати єдиний семантичний простір щодо їх розуміння. Зауважимо, що слово «фейк» є мовним запозиченням, що не має точного українського відповідника і в публіцистичному стилі вживається на позначення всього, що є несправжнім та/або породжує несправжнє. Натомість в наукових джерелах для позначення того, чого насправді немає, використовується поняття симулякрів [77], внесене в нашу постмодерну епоху Жоржем Бата [73] та розвинуте Ж. Бодріяром [8]. Уточнимо, що наразі поняття «симулякр» вживається в тому значенні, в якому його розумів Ж. Бодріяр. Екстаполюючи його теорію на досліджуване нами поняття дезінформації та її різновидів, можемо стверджувати, що фейк є симулякром третього порядку, оскільки це «перехід від знаків, які щось приховують, до знаків, які приховують, що нічого немає» [8, С. 12]. Інакше кажучи, фейк – це "точна копія, оригіналу якої ніколи не існувало" [Цит. 73]. О. Золотар називає такі симулякри «інформаційними фантомами" [Цит. 73].

На окрему увагу заслуговує також термін «фейкові новини» (fake news), оскільки він часто ототожнюється з дезінформацією [194, 248, 119, 310], особливо в англомовній аудиторії. Зокрема, таке ототожнення ми спостерігаємо у Ханта Олкота і Меттью Генцкоу, які визначають фейкові новини як «новини, які завідомо помилкові, що може з'ясуватися під час їх перевірки, і вони можуть ввести в оману читачів» [248]. Термінологічний словник сайту Міжнародного агентства «Missions Publiques» [119] також визначає фейкові новини як «тип пропаганди, що складається з навмисної

дезінформації або оманливої інформації», а в доповіді Європейської Комісії про цифрову трансформацію за 2018 рік фейкові новини було запропоновано визначити як «навмисні спроби спотворити новини» для «просування ідеологій, плутанини, незадоволення і створення поляризації» [310].

Цікаво, що у словнику Merriam-Webster зазначається, що свого часу поняття fake news («підроблені новини») замінило собою вислів false news («неправдиві новини») [315]. Таким чином фейками почали називати не всі неправдиві новини, а лише навмисно створені підробки, які імітують те, чого насправді не існує. У 90-ті роки це поняття застосовували до сатири на зразок The Onion або Daily Show [43], але вислів не користувався особливою популярністю, аж доки американські експерти не використали поняття fake news для пояснення «шокуючих результатів виборів»[11] у США у 2016 році. Уже ставши президентом Дональд Трамп у своєму Твітері звинуватив CNN, Buzzfeed і The New York Times у поширенні фейкових новин [337]. Власне, від цього моменту термін став набирати популярності, про що свідчить різке збільшення кількості запитів у Google для пошуку цього словосполучення, а тлумачний словник англійської мови Collins English Dictionary оголосив вираз fake news головною фразою 2017 року [337].

Проте занадто широке використання цього словосполучення та надмірна його політизація розмили сам зміст поняття та зміцнили в ньому суб‘єктивний складник [138]. В результаті у 2018 році упорядники доповіді «Багатомірний підхід до дезінформації», підготовленої на замовлення Єврокомісії [298], відмовилися від словосполучення «фейкові новини», пояснивши своє рішення тим, що ця фраза «не адекватна для вирішення складної проблеми дезінформації», і віддали перевагу термінові «дезінформація» [298]. При цьому єврокомісар М. Габріель спеціально наголосила, що «сформульовані на сьогодні визначення різновидів дезінформації та пропаганди все ще потребують подальшого детального

аналізу» [174]. На нагальній потребі визначення цих понять у зв'язку з неоднозначними їх трактуваннями наголошують і відомі зарубіжні експерти у сфері протидії фейкам, зокрема лідерка організації First Draft К. Вордл [117], яка зазначає, що насправді під фразою fake news люди розуміють щось «більше, ніж новини», і це щось «стосується всієї інформаційної екосистеми» [345].

Однак зауважимо, що Оперативна робоча група зі стратегічних комунікацій (Стратком) і далі використовує термін «фейкові новини» [280], щоправда, лише в розділі, де публікуються повідомлення, що стосуються Росії [267]. Сам Стратком тепер надає перевагу термінові «дезінформація», що зближує його позицію з лінією Єврокомісії, хоча з самого початку метою для створення Страткому була боротьба саме із фейковими новинами.

Окремо зупинимося на лексичній ваді терміну «фейкові новини». На наш погляд, в цьому словосполученні закладена семантична помилка, адже новини – це окремий журналістський жанр, який характеризується стислим викладом інформації про подію, яка відбулася нещодавно [133], тоді як «фейк» означає імітацію, підробку або повну вигадку. Але вигадка не може бути інформаційним жанром. Таким чином, вираз fake news складається з двох суперечливих слів, які взаємовиключають одне одного. Підтвердження цієї позиції ми знайшли в опублікованому ЮНЕСКО «Посібнику із журналістської освіти» [341], укладачі якого вважають, що поняття «новини» означає достовірну інформацію у відкритому доступі, а інформація, що не відповідає цим стандартам не може бути «новинами». Таким чином заперечується сама можливість використання терміну «фейкові новини», оскільки він є оксиморoном.

Зважаючи на всі вищезазначені аргументи, ми також пропонуємо відмовитися від використання словосполучення fake new, а на означення вигадки чи підробки використовувати термін fake або «симулякр». При цьому, беручи до уваги досліджені нами вище ознаки дезінформації,

можемо зробити висновок, що наявність двох ключових чинників переводить фейк в одну площину з дезінформацією: 1) приховується його хибність (тобто вбачається намір ввести об’єкт в оману); 2) метою створення та поширення фейку є прийняття об’єктом неправильного рішення з питання, що має суспільний інтерес.

Переходячи до подальшого аналізу поняття дезінформації, мусимо зауважимо, що досі ми багато уваги зосередили на об’єкті дезінформації і оминули увагою феномен її суб’єктів. Водночас, ряд науковців вбачають джерело загрози головною кваліфікуючою ознакою, яка дозволить ідентифікувати дезінформацію: це можуть бути урядові структури іншої держави або інтереси приватної особи чи організованого злочинного угруповання.

Зокрема, Г. Почепцов наполягає на тому, що на реальне викривлення інформаційного простору із серйозними наслідками впливають не «випадкові та хаотичні процеси щодо породження малої брехні», породжені індивідами-аматорами, а «свідомі та системні вибори дезінформації», здійснені колективами фахівців [160]. З чого науковець робить висновок про те, що «фейки продукують громадяни, дезінформацію – держава» [160]. З такою думкою погоджуються й інші вітчизняні дослідники, зокрема Д. Золотухін [75] та К. Басай [333]. Схожу позицію знаходимо і в закордонних джерелах. Так, Д. Фелліс визначає дезінформацію як «урядову чи військову діяльність» [286], а Х. Фокс говорить про оманливу інформацію, яка стала «предметом витоку інформації з боку уряду чи розвідки» [291]. На роль держави вказує і «Oxford Living Dictionary», за версією якого дезінформацію поширюють урядові організації, спрямовуючи її проти опонентів або ЗМІ [320].

Таким чином, ми з’ясували, що держава може бути не тільки об'єктом, а й суб'єктом дезінформації, оскільки має величезні можливості вироблення та поширення хибної інформації. Деякі держави створюють для цього спеціальні структури та підрозділи, як це було, наприклад, у

СРСР. Сучасна держава також може відкрито використовувати дезінформацію у війні проти іншої держави, як це робить Росія. При цьому держава-суб'єкт дезінформації може поширювати неправдиву інформацію про свої власні дії та про дії інших держав, а також про стан їхньої економіки, політики тощо для створення негативного образу цих держав або формування громадської думки проти них.

Щодо об'єкту дезінформації, то, як зазначалося вище, його визначення значною мірою залежить від галузі знань, в якій працює дослідник, оскільки представники політичної науки, психології, соціології тощо визначають такий об'єкт з різних точок зору. Так, Д. Фелліс говорить, що дезінформація спрямовується на широкий загал, оскільки «може використовуватися для маніпуляції громадською думкою та формування підтримки чи протидії певній політичній, соціальній чи економічній ініціативі» [286]. Але він також зазначає, що дезінформація може бути спрямована на завдання шкоди не лише суспільним інтересам, а й індивідуальним правам та свободам [286]. Зауважимо, що значна частина вітчизняних дослідників не поділяє такий підхід. Зокрема Г. Почепцов вважає, що кінцевими об'єктами дезінформації виступають держави, корпорації та великі групи населення [162], а В. Шлапаченко додає, що об'єктом дезінформації може бути також «особа або група осіб, які уповноважені приймати рішення» [243], оскільки дезінформація – це інструмент політичної маніпуляції, спрямованої на маніпулювання думкою громадськості та формування певних політичних переваг. В інших (приватних) випадках це буде не дезінформація, а неправдиві відомості.

Отже, можемо підсумувати, що при визначенні дезінформації на перший план виходять: свідомість (індивідуальна чи колективна) в якості об'єкта, і деструктивний вплив або спроба такого впливу з боку суб'єкта. Очевидним є той факт, що при взаємодії цих двох чинників може мати місце феномен інформаційно-психологічної маніпуляції.

Зауважимо, що у вітчизняних джерелах спостерігаються різні підходи до тлумачення самого терміну «маніпуляція» та його співвіднесення з поняттям дезінформації. Ряд дослідників визначають ці два поняття як рівнозначні, тоді як аналітики Інституту масової інформації розглядають маніпуляцію як ключову функцію дезінформації, що становить її природу [78]. Натомість вітчизняні дослідники В. Шлапаченко, О. Саєнко, В. Ліпкан, О. Колісник демонструють протилежний підхід, визначаючи дезінформацію як спосіб [243, 157] або як інструмент маніпуляції [243, 94].

На наш погляд, обидва підходи вірні, а різне тлумачення відбувається через двозначність самого поняття маніпуляції. Якщо має місце фактологічна маніпуляція (спотворення інформації), то йдеться про маніпуляцію як інструмент для дезінформування. Але якщо ми визначаємо маніпуляцію як вид інформаційно-психологічного впливу, то маніпуляція розглядається як мета, а дезінформація – як інструмент для досягнення цієї мети.

Автор терміну «чорна риторика» К. Бредемайер називає маніпуляцію головною функцією дезінформації, ключове завдання якої – змінити уявлення об’єкта про певні факти чи ситуацію в цілому [254]. При цьому Бредемайер розглядає маніпулювання і як спеціальний прийом, покликаний спрямувати спілкування в потрібне русло та підвести об’єкт до певних висновків [254]. Тобто йдеться про технологію, за допомогою якої суб’єкт (маніпулятор) одержує (чи прагне одержати) бажаний результат (наприклад, змінити громадську думку щодо певного питання).

Розглянемо докладніше ключові характеристики маніпулювання. Перша умова – прихована форма маніпуляції (сам факт її наявності повинен залишатися непоміченим). Г. Франке, який першим досліджував технології формування громадської думки, визначив маніпулювання як «таємний вплив» [292]. Г. Шиллер пише, що маніпуляція є прихованим

примусом до певних дій [327], а Л. Прото визначає маніпулювання як метод прихованого впливу на здійснення вибору реципієнта [Цит. 195].

Друга ключова характеристика психологічної маніпуляції – завдання шкоди особі, на яку чиниться вплив, з метою моделювання та структурування її картини світу [324]. Е. Шостром наголошує при цьому, що маніпуляція є методом експлуатації, керуванням та контролю [329].

Вітчизняний дослідник Є. Доценко визначає маніпулювання як вид психологічного впливу, результатом якого стає «виникнення в іншої людини намірів, які не відповідають актуально існуючим у неї бажанням» [Цит. 106]. С. Соловйов, говорить про перетворення особи, на яку чиниться вплив, на «знаряддя виконання чужих інтересів» [199]. А. Додонов робить акцент на нав'язуванні об’єктові впливу «варіантів подальшого розвитку подій, «підказки», як вчинити, який зробити вибір тощо» [40].

Третьою умовою маніпуляції є створення штучного середовища, в яке буде занурений об’єкт. Таке середовище формується з фактів і подій, яких ніколи не було насправді, а також з думок «експертів», які озвучують фальшиву експертизу. Тобто створюється фейкова реальність, підробка, інформаційна містифікація. Як пише Г. Шиллер, «успіх гарантований, якщо той, хто зазнає маніпуляції, вірить, що все відбувається природно і неминуче. Для маніпуляції потрібна фальшива дійсність, в якій її присутність не буде відчуватись» [327].

Результатом успішної маніпуляції стає те, що об’єкт управління, на якого чиниться прихований вплив, починає неправильно оцінювати дійсність та приймати невигідні для себе рішення. Якщо при цьому маніпулятор прагне змінити думку особи чи групи осіб щодо важливого суспільного питання або спричинити прийняття нею помилкового рішення, що має суспільний, військовий чи державний інтерес, то є підстави говорити про феномен дезінформації.

Тож підсумовуючи усе вищевикладене, можемо виокремити кваліфікуючі ознаки дезінформації, виділені більшістю дослідників:

– хибність інформації: перша і головна ознака, оскільки хибність є природою дезінформації;

– наявність умислу: створення та поширення завідомо хибної інформації;

– приховування умислу: прагнення видати хибну інформацію за істинну;

– зловмисність: намір нашкодити інтересам особи, на яку чиниться вплив;

– цілеспрямованість – поширення завідомо хибної інформації з метою формування у реципієнта викривленого уявлення про дійсність;

– наявність стратегічної мети: намагання вплинути на формування громадської думки або на прийняття особою чи групою осіб важливих для суспільства чи держави рішень;

– бажаний наслідок: певні зміни в суспільстві чи державі, вигідні суб'єкту дезінформації.

Погодившись з тим, що дезінформація – це спосіб інформаційно-психологічного впливу, та визначивши засіб такого впливу (хибна неправдива або модифікована інформація), об'єкт впливу (особа чи група осіб або суспільство), мету впливу (формування помилкового уявлення про реальність), наслідки впливу (прийняття об'єктом певних рішень, вигідних суб'єкту) та його ймовірний результат (серйозні зміни в суспільстві, що ведуть до погіршення загальної ситуації), можемо поєднати всі наведені ознаки в такому визначенні: ***дезінформація – це створення та поширення з політичною чи іншою стратегічною метою завідомо хибної чи свідомо модифікованої інформації як істинної для інформаційно-психологічного впливу на об'єкт з метою формування в нього помилкового уявлення про реальність та підштовхування до певних дій чи бездіяльності.***

Ми застосували доволі широке визначення терміну, оскільки надмірне його звуження призведе до обмеження випадків, які можна буде ідентифікувати як дезінформацію. Також ми свідомо не зупинилися на воєнних, розвідувальних та інших спеціальних аспектах дезінформації, оскільки неможливо в одному дослідженні охопити всі сфери цього надзвичайно складного і багатовимірного феномену. До того ж ми розглядаємо поняття дезінформації у межах механізмів вироблення державної політики, а її природою є публічність, тоді як військовими, розвідувальними та іншими сферами займаються спеціальні служби, діяльність яких не є відкритою та прозорою.

При цьому необхідно зауважити, що під поняттям дезінформації ми розуміємо як самі хибні відомості, які були навмисно створені з певною метою, так і процес їх поширення, який може мати різні форми та методи й різні канали комунікації.

Висновки до розділу 1

Результати аналізу наукових джерел, присвячених дослідженню феномену дезінформації та виробленню ефективних механізмів протидії їй, свідчать про високу актуальність зазначеної теми та значну увагу, що їй приділяє академічна спільнота. Сучасна наукова література пропонує різні моделі, інструменти, стратегії і практики, спрямовані на протидію дезінформації. Проте, досі практично відсутні дисертаційні роботи, які розглядають питання державної політики у сфері протидії дезінформації.

Крім того, після комплексного дослідження історичної динаміки та сучасних тенденцій формування нормативно-правової бази в інформаційній сфері зроблено висновок, що з 1991 року в Україні державна інформаційна політика була спрямована переважно на забезпечення свободи слова та безпеку інформації, а менше уваги приділялося безпечності самої інформації та захисту громадян, суспільства

і держави від потенційних загроз, що можуть виникнути внаслідок деструктивного інформаційного впливу. Це обумовлено історичними та культурними факторами, зокрема, тоталітарним минулим України та невпевненістю у своїй національній ідентичності, що призвело до бажання демонструвати демократичні цінності та свободу слова. Однак, з часом зросло усвідомлення необхідності забезпечення національної безпеки та захисту від інформаційних загроз, що спричинило формування нових стратегій та підходів до вироблення державної політики.

Розкрито зміст механізмів вироблення державної політики та визначено роль і місце сфери протидії дезінформації в загальній системі державної безпеки України. Особливу увагу приділено аналізу основних теоретичних підходів та концепцій з метою більш глибокого розуміння сутності та характерних особливостей механізмів формування політики в зазначеній сфері, що дозволило здійснити всебічний аналіз проблематики механізмів вироблення державної політики у сфері протидії дезінформації, оцінити їх ефективність та запропонувати концептуальний підхід до вдосконалення таких механізмів.

Зокрема, сформульовано визначення механізмів вироблення державної політики у сфері протидії дезінформації як системи організаційних, інформаційних, правових та інших заходів, що мають на меті забезпечення ефективної державної політики у сфері протидії дезінформації, і взаємодіють між собою для досягнення визначеної мети. Ці механізми включають процес дослідження дезінформації та визначення загроз, які вона несе; розроблення стратегій, концепцій, програм та окремих політичних рішень щодо протидії дезінформації. Важливою складовою механізмів є визначення заходів та завдань, вибір інструментів та механізмів їх реалізації, а також оцінка ефективності державної політики у зазначеній сфері. З метою забезпечення ефективної реалізації державної політики протидії дезінформації, механізми вироблення такої

політики мають бути мультикомпонентними та детально пропрацьованими.

Водночас констатовано, що механізми вироблення державної політики у сфері протидії дезінформації можна розглядати як систему інститутів державної влади та громадянського суспільства, які беруть участь у відповідних процессах, таких як аналіз даних, розроблення стратегій, вибір інструментів та оцінка ефективності політики. При цьому не менш важливою складовою є координація їхніх дій та налагодження взаємодії між усіма акторами з метою реалізації спільних стратегій та дій. Також необхідні відповідне нормативно-правове та комунікаційне забезпечення.

Зазначено, що перелік інституцій, які можуть взяти участь у формуванні окремих політичних рішень, не є вичерпним або заздалегідь визначеним. Процес формування рішень може включати участь державних органів, наукових установ, громадських організацій, незалежних експертів та фахівців з різних галузей, як вітчизняних, так і зарубіжних. У цьому контексті, механізми вироблення державної політики у сфері протидії дезінформації схожі на традиційні механізми вироблення державної політики в інших сферах, таких як економіка, право тощо.

З урахуванням того, що державна політика є сукупністю цілеспрямових дій, які здійснюються суб’єктами державної політики відповідно до визначеного стратегічного напряму, наголошено на необхідності вироблення довгострокових стратегій, спрямованих на ефективну протидію дезінформації з урахуванням різних аспектів, включаючи політичний, соціальний, культурний, економічний та технологічний контекст.

В ході дослідження також виявлено, що саме поняття дезінформації потребує термінологічного уточнення й конкретизації відповідно до сучасних викликів національним інтересам держави. Встановлено, що через різноманітність форм та контекстів, в яких може з’являтися

дезінформація, уточнення терміну повинно враховувати цю багатовимірність та відображати масштаб проблеми і її деструктивний вплив на суспільство.

Виокремлено кваліфікуючі ознаки дезінформації: хибність інформації, наявність умислу та його приховування, намір завдати шкоди через інформаційно-психологічний вплив на об’єкт, наявність стратегічної мети такого впливу та його бажаний наслідок. З урахуванням наведених критеріїв запропоновано авторське визначення феномену дезінформації, як створення та поширення з політичною чи іншою стратегічною метою завідомо хибної чи свідомо модифікованої інформації як істинної для інформаційно-психологічного впливу на об’єкт з метою формування в нього помилкового уявлення про реальність та підштовхування до певних дій чи бездіяльності.

Констатовано, що до дезінформації слід відносити як самі хибні відомості, так і процес їх поширення, що може мати різні форми, методи та канали комунікації.

Основні результати розділу 1 опубліковано в наукових працях автора: *[49, 50, 51, 54, 85]*.

РОЗДІЛ 2
МЕХАНІЗМИ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

2.1. Механізми вироблення державної політики у сфері протидії дезінформації у країнах розвиненої демократії: досвід США та Європейського Союзу

Двадцять перше сторіччя характеризується швидким розвитком технологій та зростанням впливу глобальних інформаційних мереж на свідомість людей, що створило нові можливості для поширення дезінформації. У зв'язку з цим питання інформаційної безпеки стає надзвичайно актуальним насвітовому рівні. У цьому розділі будуть представлені основні підходи до вироблення механізмів протидії дезінформації у США та Європейському Союзі, оцінено їх ефективність та розглянуто можливість адаптації до умов України.

Перш ніж зосередити увагу на подіях, які розгорнулися в останнє десятиріччя, коротко дослідимо історію інформаційного протистояння між Заходом та Сходому період холодної війни, оскільки її досвід - «важливе підґрунтя для розуміння тенденцій відносин у сучасному світі» [9], особливо в контексті того, що нову хвилю конфронтації між США та Росією «все частіше іменують «новою холодною війною» [5].

Початком відкритого інформаційного протиборства між країнами НАТО та СРСР можна вважати 1947 рік. Саме тоді було прийнято Доктрину Трумена [260], яка ознаменувала початок боротьби США з поширенням комуністичного впливу у світі, а також було засновано Комітет з питань нерозповсюдження атомної зброї [118] та висунуто план Маршалла [300]. Всі ці події трактуються як початок холодної війни, яка

завершилася лише у 1991 році, після розпаду СРСР. Ця війна не призвела до відкритого збройного конфлікту, але була супроводжена ідеологічним та політичним протистоянням, шпигунством, змаганням за впливи на глобальному рівні та іншими формами конфронтації.

На той час найбільш ефективним каналом масової комунікації було радіо, оскільки його сигнал швидко та легко долав кордони і досягавцільової аудиторії у різних точках світу. Кожна сторона конфлікту створювала радіостанції, які вели пропаганду та намагалися впливати на громадську думку у власній та в інших країнах. Зокрема, створене у США радіо «Свобода» активно діяло у Європі, демонструючи переваги демократії над комунізмом [239]. На противагу йому «Радіо Москва» пропагувало комуністичні ідеї та сприяло поширенню інформації, яка була корисною для комуністичного блоку [45]. Основним способом боротьби з ворожою пропагандою було взаємне блокування сигналів радіо, для чого створювалися спеціальні радіостанції, які перешкоджали поширенню сигналу супротивника. Також вживалися заходи щодо вигнання іноземних журналістів, які працювали на території протиборчої країни, оскільки їхня діяльність розглядалася як пропагандистська.

Також у багатьох країнах були сформовані спеціальні урядові агентства, які не тільки збирали та аналізувати пропаганду супротивника, а й використовували цю інформацію для розроблення власних стратегій протидії дезінформаціїта пропаганди своїх ідеологій. Такі агентства були створені в США (Центральне розвідувальне управління), Великій Британії (Відділ інформаційних досліджень), Франції (Служба психологічних дій), Німеччині (Федеральна розвідувальна служба) та інших країнах.

Крім урядових агентств деякі країни, зокрема США та Велика Британія, активно розвивали внутрішні медіа, для чого були створені незалежні медіаорганізації (радіо «Свобода», «Голос Америки», BBC та інші). Також важливим інструментом протидії дезінформації була дипломатія. Країни використовували дипломатичний тиск та домовленості,

щоб контролювати поширення дезінформації на міжнародному рівні [45]. Загалом, в цей період державні політики західних країн, спрямовані на протидію дезінформації, були складними та мінливими. Різні країни використовували різні підходи та інструменти, але загалом всі вони намагалися забезпечити незалежну та об'єктивну інформацію для своїх громадян та контролювати поширення дезінформації в міжнародному масштабі.

Після закінчення холодної війни формально припинилося й інформаційне протистояння, однак насправді протиборство тривало, лише змінився його характер. Замість намагань відкритого домінування в інформаційному просторі країни-опонента держави почали вживати більше заходів для зміцнення своєї власної позиції у глобальному просторі.

Чергове загострення інформаційного протистояння відбулося після анексії Криму. Втім, на той час дезінформація ще «не стояла на першому місці в політичному порядку денному» [234]. Справжнім тригером стали події 2016 року, коли США офіційно звинуватили Росію у втручанні в президентські вибори [266], а в лютому 2017 року таке ж звинувачення в бік Росії висунула Франція [23]. Відтоді й інші країни (Велика Британія, Польща, Німеччина, Нідерланди, Болгарія, Македонія, Чехія) та міжнародні організації, такі як ЄС і НАТО, не раз заявляли про підозру втручання Росії у внутрішні справи інших країн та спроби вплинути на президентські та парламентські вибори шляхом кібератак, провокацій, дезінформації та інших методів.

Для протидії цьому країни Заходу створюють спеціальні механізми, які включають моніторинг інформаційного простору, виявлення дезінформації та оперативну відповідь на неї, вироблення стратегій протидії на національному рівні та співпрацю з іншими країнами і міжнародними організаціями. Зокрема, у країнах НАТО таким механізмом є створений у 2009 році передовий центр кіберзахисту [316]. У 2016

членами Альянсу було визнано кіберпростір сферою операцій, «у якій НАТО має захищатися так само ефективно, як і в повітрі, на суші та на морі» [318] та підтверджено оборонний мандат НАТО [318]. І хоча Центр не прямо протидіє дезінформації, оскільки його головним завданням є забезпечення кібербезпеки, однак збір та аналіз відповідної інформації може допомогти у виявленні та протидії дезінформаційним кампаніям, що базуються на кібернападах та кібершпигунстві. Крім того, Передовий центр кіберзахисту НАТО співпрацює з іншими організаціями, включаючи Європейський союз, з метою координації спільних заходів у сфері кібербезпеки та протидії дезінформації.

Передовийцентркіберзахистутакож дієвЕстонії (NATO Cooperative Cyber Defence Centre of Excellence) [317]. Його було створено після того, якв 2007 році ця країна стала жертвою однієї з найбільших кібератак в історії, що призвело до блокування доступу до державних веб-сайтів та інших інформаційних ресурсів. Після цього інциденту Естонія приділила багато уваги розвитку своєї кіберзахисної здатності та вважається однією з провідних країн у галузі кібербезпеки.

У 2014 році також був створений Передовий центр стратегічних комунікацій (StrategicCommunicationsExcellenceCentre, StratCom) [317] з метою забезпечення ефективної комунікації та протидії дезінформації в Латвії та інших країнах Балтії та Східної Європи. Центр співпрацює з громадськістю, владними структурами, ЗМІ та іншими зацікавленими сторонами з метою забезпечення якісної та достовірної інформації та запобігання поширенню дезінформації.

У 2017 році Фінляндією та Литвою було створено Передовий центр протидії гібридним загрозам у Хельсінкі (HybridCoE) [301]. Його основною метою є сприяння в обміні досвідом та координація дій в протидії гібридним загрозам. Станом на квітень 2023 року до складу Центру входили33 країни-учасниці, зокрема країни Європейського Союзу, країни НАТО та країни Східного партнерства [301].

Крім того, у 2015 році представники Литви, Латвії та Естонії розробили спільний неформальний документ щодо необхідності координації зусиль для протидії російській пропаганді. Документ був переданий в рамках Європейського Союзу та підтриманий іншими країнами ЄС. На його основі був розроблений План дій щодо стратегічної комунікації [275], який оприлюднив Високий представник ЄС. Таким чином, у березні 2015 року з метою координації зусиль країн-членів НАТО та партнерів у сфері протидії дезінформації в Центральній та Східній Європі була створена Східна робоча група зі стратегічних комунікацій (East StratCom Working Group) [148], яка ввійшла до структури Європейської служби зовнішніх справ (EEAS). У грудні того ж року було створено Оперативну робочу групу Східних Балкан, а в червні 2017 року – Оперативну робочу групу Півдня (Близький Схід, Північна Африка та регіон Перської затоки).

У грудні 2018 року робочу групу East StratCom було реорганізовано в East StratCom Task Force відповідно до Плану дій [283], спрямованого на підвищення ефективності протидії дезінформації та гібридним загрозам у Європейському Союзі. Цей План також надав визначення дезінформації і встановив перелік заходів щодо матеріалів, які вважаються дезінформаційними.

Згідно зінформацією, яка опублікована на офіційному сайті East Stratcom Task Force, станом на березень 2021 року в Робочій групі працювало 16 штатних співробітників, представників 11 країн-членів Європейського Союзу та НАТО [148]. Крім того, до роботи було залучено близько 400 журналістів та активістів, які працюють на волонтерських засадах.

У рамках своєї діяльності Робоча група реалізує проект EUvsDisinfo, контент якого доступний 15 мовами. Сайт містить огляди та аналізи дезінформаційних кампаній, які зазвичай походять від держав, що не дотримуються міжнародних правил і норм, зокрема Росії. EUvsDisinfo веде

моніторинг дезінформаційних кампаній в соціальних медіа, телевізійних програмах та інших джерелах інформації з метою надання громадськості, ЗМІ та політичним лідерам достовірної інформаціїщодо розповсюдження дезінформації і пропаганди, спрямованої проти Європейського Союзу [268].

З цією метою публікується щотижневий «Огляд дезінформації» [268], який є головним продуктом Робочої групи та одним з джерел інформації для Схеми швидкого реагування на дезінформацію (Rapid Alert System for Disinformation - RAS). За формою це доступний для розуміння звіт, який містить конкретні описи прикладів дезінформації та маніпуляцій, спрямованих на дискредитацію ЄС та його інституцій. Звіт також може оприлюднювати інформацію про заходи, які були вжиті для протидії дезінформації, включаючи кроки, зроблені ЄС, державами-членами, соціальними мережами та іншими сторонами для зменшення впливу дезінформації та підвищення медіаграмотності населення. Таким чином, щотижневий огляд East Stratcom є джерелом інформації для тих, «хто хоче бути свідомим про загрози дезінформації та маніпуляції в Європі та світі, а також є інструментом для формування стратегій протидії дезінформації та забезпечення захисту від неї» [82].

East Stratcom Working Group також генерує власні аналітичні матеріали, навчає уряд, державні органи ЄС, журналістів і аналітиків протидії дезінформації та проводить спільні заходи з усіма зацікавленими сторонами.

Зауважимо, що ЄС звертає велику увагу на забезпечення кращої координації між державами-членами ЄС. З цією метою у квітні 2016 року була видана «Спільна рамкова стратегія з протидії гібридним загрозам: відповідь Європейського Союзу» [281], яка передбачає координовані дії та співпрацю між державамидля ефективної протидії таким загрозам як ключовому виклику безпеці та стабільності в Європейському Союзі. Документ, зокрема, містить визначення гібридної загрози та описує її

основні характеристики. Далі наведено заходи політичного, економічного, комунікаційного та кібернетичного характеру, які можуть бути вжиті для протидії таким гібридним загрозам.

У Стратегії зазначається, що для ефективного контролю гібридних загроз важливо розвивати обмін інформацією та вдосконалювати інструменти обміну секторальними розвідувальними даними між членами ЄС та країнами-партнерами. З цією метою у структурі Європейської служби зовнішньої дії було створено Підрозділ гібридного синтезу, який отримує, аналізує та обмінюється інформацією з обмеженим доступом та інформацією з відкритих джерел, орієнтуючись на індикатори та попереджувальні сигнали про гібридні загрози, які посилають різні актори [281].

За місяць, у травні 2016 року Комітетом закордонних справ Європейського Парламенту було розглянуто проект звіту про стратегічну комунікацію ЄС для протидії пропаганді, спрямованій проти Європейського Союзу третіми сторонами (2016/2030(INI) [279] та запропоновано відповідну стратегію протидії. А в червні 2016 року на засіданні Ради Європейського Союзу з питань загальних справ у Люксембурзі Верховним представником ЄС з питань закордонних справ і політики безпеки Федерікою Могеріні була презентована Глобальна стратегія ЄС (EU Global Strategy) [282], яка стала першим оновленим документом такого роду за останні 13 років. Зокрема, було визначено, що ЄС має бути більш дієвим та гнучким у своїй зовнішній політиці, щоб відповідати на нові виклики та можливості, з якими Європейський Союз стикається у сучасному світі.

Отже, можемо виділити три ключові інструменти реагування на дезінформацію та інші гібридні загрози, розроблені Європейською Комісією у 2015-2016 роках: Оперативна групу зі стратегічних комунікацій (East StratCom Task Force), Координаційна група з питань гібридних загроз (Hybrid Fusion Cell) та Система швидкого оповіщення (RAS-DIS)[185].

Четвертим таким інструментом став прийнятий у 2018 році загальноєвропейський добровільний Кодекс щодо протидії дезінформації [270], який було ухвалено перед черговими виборами до Європарламенту. Першими підписантами Кодексу стати онлайн-платформи Facebook, Google, Twitter, Mozilla, а також рекламодавці і представники рекламної індустрії. У 2019 році Кодекс підписала Microsoft,у 2020 році– Kreativitet & Kommunikation, Goldbach Audience (Швейцарія)AG і TikTok, який став 16-ю стороною з числа підписантів [270].

16 червня 2022 року було подано посилений Кодекс, який підписали 34 сторони (тобто 18 з них приєдналися до Кодексу після 10 червня 2020 року) [274]. Підписанти зобов'язалися вжити заходів у кількох напрямах: демонетизація (скорочення фінансових стимулів для розповсюджувачів дезінформації); прозорість політичної реклами (більш помітне маркування, розкриття спонсора та публікація витрат на рекламу і періоду показу); кращий захист користувачів (вдосконалені цифрові інструменти розпізнавання патогенного контенту, більша прозорість рекомендаційних систем, підвищення медіаграмотності тощо); більш тісна співпраця з фактчекерами (розширення їх діяльності на всі держави-члени ЄС, спрощена процедура доступу до інформації та справедлива фінансова винагорода); розширена підтримка дослідників (зокрема, автоматизований доступ до знеособлених або агрегованих даних). Всього посилений Кодекс містить 44 зобов’язання та 128 заходів [273].

Як зазначили в ЄС, «це перший випадок, коли галузь на добровільних засадах погодила набір стандартів саморегулювання для боротьби з дезінформацією» [269]. Однак, аналітики зауважують, що добровільні зобов’язання не регулюються законодавчо, через що «зупинити інформаційні маніпуляції надзвичайно складно» [23].

Зі свого боку, Європейський Союз з метою підвищення рівня захисту від дезінформації та недостовірної інформації в цифрових медіа також

проголосив підтримку мережі незалежних фактчекерів. Наслідком такого рішення стало створення у листопаді 2018 року Соціальної обсерваторії дезінформації та соціального медіааналізу (SOMA) [265]. Наступного року було створено більш потужний міжнародний партнерський проект – Європейську обсерваторію цифрових медіа (EDMO) [277], який об'єднав фахівців з фактчекінгу для аналізу програмного забезпечення та відстеження поширення дезінформації цифровими медіа в багатьох країнах світу.

При цьому з кожним роком збільшується бюджет, спрямований на протидію інформаційним загрозам. Наприклад, бюджет Європейської служби зовнішніх справ (EEAS) на стратегічну комунікацію зріс з 1,9 млн євро у 2018 році до 5 млн євро у 2019 році [70]. Однак зазначимо, що окремі експерти вважають фінансові ресурси, які виділяються ЄС на протидію дезінформації, не співмірними загрозі, яку вона становить [234]. Хоча слід зауважити, що такі оцінки є суб'єктивними, а розмір бюджету і його відповідність загрозі можуть бути предметом подальшої дискусії серед експертного співтовариства.

Разом з тим, подальше загострення стосунків Європейського Союзу та РФ призвело до того, що 3 грудня 2020 року був ухвалений оновлений План дій в галузі європейської демократії (European Democracy Action Plan) [271]. Цей документ виділяє протидію дезінформації як один з трьох ключових напрямів захисту демократичних прав і свобод та диференціює помилкову інформацію (misinformation), дезінформацію (disinformation), цілеспрямовану інформаційну кампанію впливу (information influence operation) та іноземне втручання в інформаційний простір (foreign interference in the information space) [271]. На відміну від Плану дій 2018 року, де головний акцент було зроблено на виробленні та донесенні контрнаративів, в оновленому документі міститься вимога більш енергійних заходів, включаючи блокування веб-ресурсу, який несепатогенний контент.

Крім того, у рамках стратегії ЄС з цифрового регулювання, Європейський Парламент влітку 2022 року ухвалив Пакет цифрових послуг, який включає два закони: Закон про цифрові ринки (DMA) [272] та Закон про цифрові послуги (DSA) [323]. Цей пакет став реакцією ЄС на екстремально швидкі зміни бізнес-моделей та цифрових послуг в інформаційному просторі, а також на війну РФ проти України, яка виявила недоліки у почасти застарілій системі правил, що регулюють інформаційний простір. Серед таких недоліків можна виокремити складність управління дезінформацією та легкість поширення фейків.

Закон про цифрові ринки (DMA), який набув чинності 1 листопада 2022 року, має на меті регулювання діяльності та обмеження надмірної влади великих платформ. Натомість, Закон про цифрові послуги (DSA) спрямований на регулювання всіх онлайн-ресурсів, включаючи невеликі веб-сайти, з метою створення безпечного цифрового середовища для споживачів інформації. DSA встановлює нові правила щодо протидії незаконному контенту в Інтернеті, зокрема товарів, послуг та інформації і, крім того, передбачає заходи щодо зменшення ризиків у мережі та підвищення прозорості діяльності онлайн-ресурсів, які мають надавати додаткову інформацію про свою роботу, зокрема про спосіб функціонування їхніх алгоритмів відбору інформації з метою таргетованого впливу на споживачів, а також про способи та інструменти контролю і фільтрації небажаного контенту. Ці норми стали обов’язковими до виконання з 1 січня 2024 року.

На підставі проведеного аналізу стратегій протидії дезінформації в ЄС можемо зробити висновок, що цясфера є динамічною та постійно розширюється. Дезінформаційні кампанії стають все складнішими та використовують нові технології, що вимагає від протидійних структур постійного оновлення та адаптації своїх стратегій та інструментів. У зв'язку з цим, важливо досліджувати не лише досвід Європейського Союзу,

але й інших країн та регіонів, таких як Сполучені Штати Америки, з метою знаходження оптимальних рішень для ефективної протидії дезінформації.

Як уже зазначалося, США почали активно розвивати державну інфраструктуру протидії дезінформації після президентських виборів 2016 року [266]. Таким чином, в рамках Національної стратегії безпеки кіберпростору, яка була затверджена того ж року, Державним департаментом США було створено Глобальний центр взаємодії (Global Engagement Center, або скорочено GEC) [340], який займається протидією дезінформації та пропаганді, джерелом створення та поширення яких є терористичні організації, держави-спонсори тероризму та інших суб'єкти, які створюють загрозу національній безпеці США. Зауважимо, що спочатку GEC був створений як "Центр протидії пропаганді іноземних терористичних організацій", але в 2017 році був перейменований в Global Engagement Center і отримав додаткові повноваження для боротьби з іншими формами дезінформації та впливу на громадську думку [340]. Основна мета GEC полягає у захисті безпеки національних інтересів США, зменшенні впливу пропагандистських повідомлень на громадську думку в США та за кордоном, та збільшенні здатності американських державних органів, міжнародних партнерів та громадськості реагувати на дезінформацію та інші загрози національній безпеці.

Також наприкінці 2017 року Федеральне бюро розслідувань створило Робочу групу з протидії закордонному впливу (Foreign Influence Task Force), яка входила до складу відділів контррозвідки, кібербезпеки, протидії злочинності та боротьби з тероризмом. Завданням групи було розроблення стратегій та технічних рішень, які допоможуть виявляти та запобігати такому втручанню в майбутньому. У звіті Робочої групи, оприлюдненому у березні 2018 року, було наголошено, що дезінформація має серйозний вплив на громадську думку та демократичні процеси в США. У зв’язку з цим у вересні 2018 року у Сполучених Штатах Америки було створено Foreign Influence Task Force (Центр зовнішнього шкідливого

впливу) [287], головна мета якого полягає у запобіганні зовнішньому впливу на виборчий процес, законодавчу роботу та інші суспільні процеси в США. Крім того, що Центр аналізує інформацію про можливий зовнішній шкідливий вплив на США, він координує роботу спецслужб, займається підготовкою рекомендацій щодо удосконалення системи захисту від зовнішнього впливу тощо. У 2021 році Foreign Influence Task Force було перейменовано у Mis-, Dis-, andMalinformation (MDM) team (Команду з дезінформації, неправдивої та шкідливої інформації) [345].

У 2018 році в США також була створена Комісія з досліджень кіберпростору (Cyberspace Solarium Commission, CSC), яка провела широкі консультації з громадськістю та зібрала думки експертів з різних галузей, щоб розробити рекомендації з кібербезпеки, які були представлені у звіті до Конгресу США в березні 2020 року.Загалом Звіт містив більше 80 рекомендацій, основні з яких: створення національної стратегії кібербезпеки та забезпечення фінансування науково-дослідних робіт у галузі кібербезпеки; удосконалення системи кіберзахисту критично важливих інфраструктур; підвищення рівня кібербезпеки в промисловості та на малих підприємствах; покращення співпраці між різними відомствами США у сфері кібербезпеки; підтримка розвитку кадрів у галузі кібербезпеки; забезпечення безпеки виборів у США шляхом покращення кіберзахисту виборчої системи; підвищення рівня кібербезпеки в оборонному секторі США.

Комісія CSC і далі активно працює. Зокрема, її рекомендації та пропозиції до американського уряду викладені у «Білій книзі протидії дезінформації у США» [261], презентація якої відбулася наприкінці 2021 року. У Білій книзі рекомендується створення вищого керівництва з протидії дезінформації, яке має координувати всі зусилля в цій сфері в усіх державних відомствах та між ними. У сфері законодавства та регулювання містяться рекомендації щодо створення законодавчих механізмів для протидії дезінформації, встановлення вимог до соціальних мереж стосовно

дотримання прозорості та звітності, заборони розміщення політичної реклами без вказівки замовника. Рекомендації у сфері кібербезпеки включають захист від кібератак та від розповсюдження шкідливих програм, розробку технічних інструментів для виявлення та видалення дезінформації, а також забезпечення безпеки виборів та зменшення впливу іноземних держав на рішення виборців. Також Біла книга містить рекомендації щодо розвитку програми навчання з медіаграмотності та критичного мислення для громадян [261].

Зауважимо, що медіаосвіта в США здійснюється в різних контекстах, включаючи формальну освіту у школах та університетах, неформальну освіту у бібліотеках, музеях та інших освітніх установах, а також в медіаіндустрії та інших сферах. У школах США медіаосвіта часто входить до складу курсу з мови та літератури, соціальних наук або здоров'я та фізичного виховання. Також діють різні програми, зокрема, Федеральна комісія з комунікацій розробила програму "Медіаграмотність на сьогоднішній день", яка допомагає вчителям та батькам навчати дітей критично сприймати інформацію, яку вони отримують з мас-медіа. Крім того, існують різноманітні неурядові організації, які працюють у сфері медіаосвіти. Однією з них є "Media Literacy Now", яка допомагає батькам, педагогам та законодавцям зрозуміти важливість медіаосвіти та сприяє впровадженню законодавчих актів про медіаосвіту у різних штатах.

Слід окремо зауважити, що в США діє Закон про свободу інформації, відповідно до якого Федеральний суд США у 2016 році виніс заборону провайдерам блокувати інтернет-сайти, підтримавши цим ідею свободи слова та принцип відкритості інтернету [201]. Відтоді блокування будь-яких інтернет-ресурсів не допускається за винятком випадків, коли сайт містить порнографію, пропагує насильство, тероризм або іншу незаконну діяльність. Також у США діє закон DMCA, який дозволяє видаляти матеріали з Інтернету, які порушують авторські права.

Підсумовуючи вищевикладене, можна сказати, що на сьогоднішній день в ЄС та США визначені ключові напрями протидії дезінформації, створена відповідна нормативно-правова база та сформовані структури аналітичного й практичного характеру. При цьому уряд спирається як на власні структури, так і на співробітництво з приватними компаніями та інститутами громадянського суспільства. Крім іншого, протидія дезінформації передбачає розвиток медіаграмотності у населення, зокрема шляхом забезпечення доступності та якості медіаосвіти.

2.2. Механізми вироблення державної політики у сфері протидії дезінформації на сучасному етапі розвитку інформаційної безпеки України

Одним із найбільших викликів, що стоять перед українською державою у секторі інформаційної безпеки, є протидія дезінформації як ключовій технології інформаційної війни, ініційованої Російською Федерацією проти України. Це завдання стає особливо актуальним на тлі зростаючої глобалізації та доступності Інтернету. Слід зауважити, що незважаючи на зусилля органів державної влади та активність громадських організацій, ситуація в державі залишається складною. У цьому контексті важливо здійснити комплексний аналізсучасного стану механізмів вироблення державної політики у сфері протидії дезінформації, щоб оцінити ефективність наявних інструментів та методіві запропонувати можливі шляхи їх вдосконалення.

Важливою вимогою до розуміння певної політичної стратегії є наявність точних, чітких, логічних і максимально наближених до реальностітермінологічних визначень, які застосовуються при її описі чи коментуванні. Тому перед початком аналізу вважаємо за необхідне визначити змістове наповнення поняття «інформаційна війна» як основного джерела загроз інформаційній безпеці держави.

Необхідно зазначити, що термін «інформаційна війна» не має чіткого та однозначного тлумачення в жодній із сфер державної політики як в Україні, так і в світі. Це пояснюється складністю та багатогранністю цього явища, яке може мати різні інтерпретації, в залежності від контексту, в якому воно розглядається. Наприклад, фахівці в галузі інформаційних технологій можуть включати до поняття «інформаційна війна» використання комп'ютерних технологій для знищення важливих даних, тоді як представники гуманітарного підходу бачать у ній, перш за все, інформаційно-психологічну складову.

У більш широкому тлумаченні під інформаційною війною можуть розумітися комунікативні процеси, що включають в себе відкриті та приховані цілеспрямовані взаємодії між інформаційними системами, що передбачають отримання вхідних даних, обробку цих даних або зміну внутрішнього стану системи та надання результату або зміну зовнішнього стану [244]. Якщо в якості такої інформаційної системи розглядати людину, то інформаційний вплив на неї здатний запустити такі програми, як «активізація бажань, думок і провокування вчинків, скерованих на самознищення» [244]. При цьому коло учасників такого протиборства може розширюватись до всіх, хто є присутнім у певний проміжок часу в інформаційному просторі усіх протибочих сторін.

У 1980-х роках, коли почалосяактивне вивчення феномену інформаційноївійни,дослідники запропонували термін "інформаційна війна другого покоління", яка характеризується застосуванням дезінформації та маніпуляції черезвикористання інформаційних технологій та електронних комунікаційних засобів для досягнення військово-політичних цілей [27]. Особливістю такої форми війни є постійні атаки на інформаційний простір опонентаз метою знищення його інформаційної переваги [27].

Зауважимо, що питання авторства самого терміну "інформаційна війна" досить спірне. Багато дослідників вважають, що він був запропонований військовим аналітиком Т. Роною [326], який у 1976 році в

аналітичній доповіді компанії Boeing вперше акцентувавувагу на критеріях, що лягли в основу інформаційної війни в її сучасному розумінні Але така точка зору не є одностайною. Наприклад Є. Магда стверджує, що термін «інформаційна війна» вперше вжив у 1967 році колишній директор ЦРУ Ален Даллес у книзі «Таємна капітуляція» [116, С. 120]. Проте є докази того, що цей термін вживався ще раніше. Зокрема, одним із творців терміну «інформаційна війна» можна вважати Пола Барана, який використав його у 1948 році в книзі "Логіка національної стратегії " [2]. Щоправда, Пол Баран розглядав інформацію не як засіб ведення активних дій проти іншої країни, а як засіб захисту власної національної безпеки.

Зазначимо, що крім широкого визначення, у більш вузькому розумінні інформаційна війна може інтерпретуватисьяк воєнне мистецтво знешкодження супротивника та ведення успішних військових дій («війна - мистецтво обману» [334]). Зокрема, А. Сигал [331] досліджує питання того, як сучасні держави розуміють своїх потенційних воєнних супротивників, та як вони збирають й аналізують інформацію про їх мотивації, цілі, дії та реакції на події.

Першим прикладом сучасної інформаційної війни в її технічному розумінні можна вважати операцію «Буря в пустелі», проведенуСША в Іраку у 1991 році, коли інформаційні технології вперше було використано як засіб ведення бойових дій. Однак, якщо цю операцію і можна віднести до інформаційної війни, то вона є її нетиповим прикладом, оскількина той час інформаційні та кібернетичні технології були значно менш розвиненими, і їх застосування в бойових діях не було настільки поширеним, як сьогодні.

В офіційному документі термін «інформаційна війна» вперше з’явився у директиві міністра оборони США DODD 3600, виданій 21 грудня 1992 року як відповідь нашвидкий розвиток інформаційних технологій та їх використання для підваження інформаційної безпеки інших держав. У самому документі термін "інформаційна війна» був

визначений як дії, спрямовані на захоплення, контроль та використання інформації для впливу на супротивника.

У 1990-х роках технічні аспекти інформаційної війни, такі як хакерство, конфіденційність, комп’ютерні віруси, розглядають Д. Гартлі [297], М. Кеннеді [304], М. Лібіцкі [306] та інші науковці. Зокрема, М. Лібіцківизначає інформаційну війну як "використання інформаційних технологій та засобів для досягнення політичних, економічних або військових цілей шляхом знищення, модифікації або контролю інформації, що належить іншій стороні" [306, С. 6]. Схоче визначення надає Ф. Хоффман, однак зауважує, щотака форма війни може відбуватися не тільки між державами, але й між іншими суб'єктами, зокрема у сфері бізнесу, які можуть бути зацікавлені в здобутті контролю над інформацією) [299, С. 17].

Однак в контекті інформаційної війни виникає проблема не тільки захисту інформації від знищення або пошкодження, а й захисту суспільства від самої інформації, яка може мати деструктивний вплив. Зокрема, Т. Рона визначає інформаційну війну як "використання інформації та медіа-технологій для досягнення політичних та військових цілей" та виділяє три аспекти інформаційної війни: інформаційна домінація, інформаційна дезінформація та інформаційна диверсія [325].

В українському науковому дискурсі інтерес до теми інформаційної війни зріспісля початку російської агресії проти України. Зокрема, В Ліпкан розглядає інформаційну війну як найвищий рівень інформаційного протиборства між державами, а також всередині держави «шляхом широкомасштабної реалізації способів і методів інформаційного насильства (інформаційної зброї) [113], що здійснюється, зокрема, з метою повалення уряду таінспірування громадянської війни як джерела перманентного хаосу, контрольованого суб’єктом управління цим хаосом [113].

П.Шевчук теж говорить про інформаційну зброю, спроможну «порушити психічне здоров'я, спонукати до спонтанних дій, спричинити тимчасові чи незворотні зміни і самознищення, підкорити свідомість (та підсвідомість) особистості і спрямувати її в необхідному для суб'єкта впливу напрямі» [241].

Інформаційна війна розглядається також як «дії, що вчиняються для досягнення інформаційної переваги у підтримці національної воєнної стратегії через вплив на інформацію та інформаційні системи противника при одночасному гарантування безпеки власної інформації і інформаційних систем» [245, С. 14]; та як використання пропаганди, спрямованої проти певної держави чи державної політики або економічної системи, для «активізації дій громадянського суспільства проти власних урядів» [100].

Зауважимо, що на противагу таким досить вузьким визначенням, Г. Почепцов розглядає інформаційну війну як комплексне явище, де полем дій є: інфраструктура основних систем життєзабезпечення держави (телекомунікації, транспортна мережа, електростанції, банківський сектор тощо); промислове шпигунство (викрадення інформації, на яку поширюється авторське право, модифікація або знищення важливих даних); несанкціонований доступ до конфіденційних даних, продукування і поширення дезінформації; радіоелектронне втручання в діяльність військових об'єктів та виведення з ладу військових комунікацій тощо [163, С. 128].

Також необхідно зазначити, що часто відбувається змішування та взаємне переплетення термінів «інформаційна війна» та «інформаційні операції», але вони не є взаємозамінними. Наприклад, С. Соловйов пропонує класифікувати поняття «інформаційна війна» та «інформаційна операція» залежно від типу аудиторії, на яку спрямована інформаційна атака: інформаційна операція охоплює вузьке коло осіб чи навіть одну

особу, тоді якінформаційна війна спрямована на масову свідомість та протяжна у часі і має багато проміжних цілей [200, С. 198].

Отже, підсумовуючи вищевикладене, можна сформулювати загальне визначення інформаційної війни як процесу використання інформаційних технологій та медіа-ресурсів з метою впливу на громадську думку, національну безпеку та соціальну стабільність держави.

Офіційне визначення терміну «інформаційна війна», то воно містилося у «Стратегічному оборонному бюлетені України» 2012 року [218], і якщо відкинути політичний аспект, воно адекватно відображало суть цього явища: «інформаційна війна – форма протиборства між суб'єктами (державами, блоками, партіями тощо), що передбачає інформаційний вплив на населення з використанням засобів масової інформації, комп'ютерних мереж тощо з метою формування відповідної суспільної думки, підриву морального духу як усього суспільства, так і окремих його інституцій». Проте зазначений документ втратив чинність у 2016 році після прийняття нового Стратегічного оборонного бюлетеня України [222], який не містить визначення цього поняття.

Згодом термін «інформаційна війна», який не є формально закріпленим у законодавстві, було замінено на інше термінологічно неврегульоване поняття «гібридна війна». Очевидно, це було зроблено з метою підтвердження комплексного характеру загрози з боку Російської Федерації, оскількигібридна війна поєднує в собі різні методи та засоби, такі як військові операції, політичні та економічні тиски, кібератаки, терористичні акти, поширення дезінформації тощо.

Паралельно було введено поняття «спеціальні інформаційні операції» як елемент гібридної війни, що може бути виправданим з точки зору управління загрозами. Така заміна дозволяє формулювати терміни більш точно та прецизійно, що, у свою чергу, сприяє кращому розумінню природи використання інформації в конфліктах та розробленню ефективних заходів протидії. Так, наприклад, В. Горбулін зауважує, що

«війни в інформаційному середовищі в сучасній науці та військових доктринах, на відміну від журналістської практики, зазвичай прийнято називати інформаційними операціями» [21] та стверджує, що термін «інформаційні операції» як більш вузьке поняття дає змогу точніше, ніж традиційний термін «інформаційні війни», дослідити місце та роль інформаційного протиборства як компоненти глобальних протистоянь [21]. О. Верголяс також наполягає на тому, що термін "інформаційна війна" більше публіцистичний, ніж науковий, та містить елементи маркетингу і політичної пропаганди, які можуть розмивати реальні проблеми та загрози [12, С. 54]. Подібний підхід демонструє і Т. Ткачук, визначаючи інформаційну війну як«сукупність цілеспрямованих інформаційних впливів» [208]. Зазначені автори розуміють інформаційну війну як набір окремих інформаційних заходів та операцій, спрямованих на масову свідомість з метою досягнення конкретної цілі в рамках загальної стратегії гібридної війни. Є очевидним, що розробники сучасної державної політики в Україні обрали саме такий підхід.

Проте існує й інший, відповідно до якого інформаційна війна визначається як поєднання різних методів та засобів впливу, що взаємодіють між собою та підсилюють один одного в ході досягнення намічених стратегічних цілей. Таким чином, підкреслюється взаємозв’язок та взаємодія різних методів, включаючи інформаційні операції, кібератаки, політичні впливи тощо, які виникли у зв’язку зі змінами ситуації на політичній, соціальній або військовій арені. І наш погляд інформаційну війну доцільно розглядати саме як системну, об’єднану єдиним задумом і протяжну в часі сукупній дій, в ході реалізації яких досягаєтьсясинергетичний ефект від координації та поєднання різних видів інформаційних операцій з метою досягнення більш широкої мети.

Зазначимо, що термін "інформаційна війна" широко вживається не тільки в наукових та дослідницьких працях, а й у нормативно-правових актах різних країн та документах міжнародних організацій. Зокрема,

Європейський Союз визначає інформаційну війну як застосування інформаційних технологій з метою впливу на громадську думку в масштабах національних та міжнародних конфліктів [278]. А також, як використання спеціальної інформації та комунікаціних засобів з метою втручання у справи ворога, зменшення ефективності його дій та підвищення власної бойової готовності та ефективності дій власних військ [39]. Отже, термін «інформаційна війна» є широковживаним та загальноприйнятним для опису нових видів загроз і конфліктів, що виникають у сучасному світі.

Щодо визначення самого терміну «загроза», то на відміну від загальновживаного тлумачення загрози, під якою розуміється «можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь» [197], у Законі України «Про національну безпеку» загроза визначається як «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» [62].

У науковому контексті загроза зазвичай розглядається як «родова ознака безпеки» [22, С. 14] і визначається як сукупність певних чинників та умов, які несуть реальну або потенційну небезпеку об’єкту захисту [Цит. 204], або як «сукупність намірів і можливостей одного суб’єкта завдати шкоди інтересам іншого» [Цит. 204], чи як «ситуація, яка характеризується ймовірністю виникнення небезпеки» [112], або як«безпека на її нульовому рівні» [112]. Однак таке широке трактування загроз може призвести до їх ототожнення з такими категоріями, як «ризик» і «виклик».

Не надають достатньої чіткості щодо коректного розмежування цих понять і наукові джерела, де виклик визначається як «наміри або дії однієї зі сторін зовнішніх або внутрішніх відносин, які спрямовані на вирішення суперечностей у відносинах, демонстративно нехтуючи національними

інтересами іншої сторони та можливістю заподіяти їм шкоду» [110, С. 17], а загроза – як «початкова стадія зародження ескалації напруженості та протистояння між суб'єктами міжнародних відносин» [Цит. 18, С. 109]. Таким чином, спостерігається повне ототожнення понять «загроза» і «виклик», хоча насправді вони не є взаємозамінними. Як результат, практично в усіх державних документах до 2022 року поняття «виклик» та «загроза» тісно пов'язані між собою та розглядаються як єдине поняття: «сучасні виклики і загрози в безпековій сфері», «спільні виклики і загрози» в міжнародному вимірі тощо. Це ускладнює класифікаціювизначених чинників, оскільки вони є різними поняттями, які вимагають різних управлінських механізмів.

В цьому контексті доцільним здається підхід, запропонований О.Резніковою [179], якапояснює ці терміни так, як вони трактуються міжнародними стандартами: ризик – це вплив невизначеності на очікувані результати (ISO 31000:2018 «Управління ризиками - Внутрішній аудитор»), а загроза – це потенційна причина небажаної події, яка може завдати шкоди фізичним особам, активам, системам або організаціям, навколишньому середовищу або суспільству (ISO 22300:2021 "Безпека та стійкість - Термінологія").

Разом з тим, концепція того, що інформація може становити загрозу, не є новою, і з кожним наступним етапом розвитку технологій та зростанням їх можливостей, ця проблема стає все більш актуальною та привертає увагу дослідників. Зокрема, Н. Вінер, який є одним з основоположників теорії інформації, ще у 1950 році висловив стурбованість щодо проблем інформаційної безпеки та звернув увагу на можливість використання інформації для маніпулювання масовою свідомістю [347].

Серед перших, хто звернув увагу на потенційну небезпеку інформації, також був М. Маклуен, який у 1962 році зазначив, що засоби масової комунікації мають величезний вплив на сприйняття людьми

реальності та нашу здатність розуміти світ [313], і згодом розвинув цю ідею, стверджуючи, що засоби масової комунікації стали знаряддями для маніпулювання свідомістю людей та використовуються для досягнення політичних і військових цілей [312].

Схожу думку про те, що технічний прогрес може стати джерелом маніпулювання людьми, висловив у 1964 році німецький філософ Г. Маркузе [309].

Окрему увагу філософизвертали на проблему широкого використання мережевих систем. Так, З. Бжезинський ще в 1970 році стверджував, що сучасне суспільство, яке формується під впливом техніки та електроніки, переживає руйнацію традиційних відносин, коли, з одного боку, відбувається фрагментація життя людини, а з іншого, – формується її цілісний глобальний світогляд [255, С.9]

М. Кастельс у своїй концепції «суспільства мережевих структур» характеризує його як суспільство, де провідну роль відіграють різноманітні мережеві форми взаємодії, які впливають на організаціюта функціонування суспільства, провідною ознакою якого стає «домінування соціальної морфології над соціальною дією» [258].

Е. Тоффлер, просуваючи ідею впровадження децентралізованих комп'ютерних мереж, в яких контроль та управління розподілені між багатьма користувачами [335], передрік появу Інтернету та передбачив появу нових медіа, порівнявши їх з «революційною нервовою системою для всього світу» [336]. Все це призведе не лише до розширення доступу до інформації та розвитку комунікаційних можливостей, – вважав Тоффлер, – а й спричинить зміну соціальних норм, цінностей і переконань, а також матиме значний вплив на економічні та політичні процеси.

В рамках дискусії про масові комунікації Г. Маклуен висловив думку про те, що медіа не тільки надають нам інформацію, а й визначають форму та спосіб сприйняття та розуміння нами цієї інформації [312].

Згодом Р. Нойман охарактеризував нові медіа як цифровий формат ЗМІ, які є постійно доступними і передбачають можливість активної взаємодії зі споживачами інформації, тобто користувачі можуть в режимі реального часу оцінювати, коментувати, репостити вже розміщений контент та створювати власний [319, С. 50]. Схожий підхід демонструє М. Кастельс, говорячи про розвитоknової форми комунікації, яку він називає «масовими самокомунікаціями» [259].

І справді, ввійшовши в цифрову епоху, ми стали свідками того, що публікація власного контенту більше не стримується обмеженнями, які мали силу раніше. «З'явилися нові медіаформати, такі як вебсайти, соціальні мережі, блоги, відеохостинг і подкасти, які працюють в автономному режимі й самі визначають формат і способи поширення власного чи партнерського контенту і взаємодію з його споживачами» [54]. У зв'язку з цим Д. Беккер провів паралель між появою соціальних медіа та виникненням писемності, вказуючи таким чином на співмірність їх значущості [252]. Проте відповідь на питання, який вплив матиме налюдство цей новий елемент реальності – позитивний чи негативний – не є однозначною. Як пише Г. Почепцов [161], щоразу нові технології дають світові не лише те, що було задумано, а й побічні негативні наслідки, які даються взнаки повною мірою. Людина «пливе на хвилі позитиву, щоб потім поринути з головою в море негативу, про який ніхто не замислювався, запускаючи у світ ці нововведення» [161]. З такою думкою погоджується А. Зібертович, який зауважує, що соціальні медіа працюють інакше, ніж очікувалося. Замість того, щоб пояснювати світ, вони частіше використовуються як інструменти дезінформації, в результаті чого «соціальні медіа більше вносять розбрат між людьми, ніж допомагають їм спілкуватися» [Цит. 69].

Депрофесіоналізація медіасфери, спричинена можливістю швидкої та безкоштовної публікації контенту всіма охочими, призвела до значного поширення дезінформації. Згідно з результатами соціологічних досліджень, у 2020 році близько 54 відсотків українських користувачів

Facebook поширювали дезінформаційні та маніпулятивні повідомлення, навіть не усвідомлюючи цього [132]. Такий само відсоток українців вважає, що вони здатні відрізнити правду від фейку [33].Однак експерти вважають цей відсоток завищеним [35].

Як зазначає Джеймс Кац, «натовпи є мудрими, але не надто мудрими» [303], що може зробити їх привабливими для суб'єктів, які хочуть маніпулювати та впливати на інформаційне середовище. Для цього використовується контент, який має емоційну складову та привертає увагу своєю сенсаційністю. На важливість емоційного впливу вказував ще Ф. Ніцше: "Безсумнівно, ми не можемо домогтися могутності без виклику вражень і хвилювань» [143]. Професійні фактчекери наголошують, що якщо новина викликає яскраву емоцію, то потенційно вона є фейковою [235]. В результаті, як зазначає В. Тарасюк, «сучасна людина стикається з медіазамінниками реальних фактів і симулякрами. й змушена взаємодіяти з ними через неможливість охопити всі події дійсності» [201]. Така заміна стала наслідком перенасичення інформацією, коли у вільному доступі постійно знаходиться значний неконтрольований обсяг даних, які людина зчитує щодня. Як стверджує П. Сінґер, у 2000 році концентрація уваги користувачів інтернету тривала в середньому дванадцять секунд, а 2015 році вона вже зменшилася до восьми [190].

Іншим аспектом явища постправди стає віртуалізація сприйняття соціальної реальності. З розширенням використання соціальних медіа та цифрових платформ розуміння дійсності може бути спотворене або зміщене через формування альтернативних реальностей, де «ілюзорне сприймається як дійсне» [16, С. 17], а «створена технічними засобами реальність набуває значущості, оцінюється як вища, краща, справжня» [16, С. 17]. Таким чином, під впливом медіа дійсність перестає бути реальною, перетворюючись на сконструйовану професійними технологами віртуальну вигадку, і саме споглядання цього нового символічного світу перетворює людину на слухняний об'єкт зовнішніх маніпуляцій.

Ефективним запобіжником від включення в процес маніпуляції є контрсугестія [48], однак дослідження психологів підтвердили, що люди, занурені у віртуальний світ, втрачають здатність протистояти зараженню чужими думками [146].

Люди мають тенденцію сприймати інформацію через призму своїх власних когнітивних спотворень, а саме – цілеспрямовано шукати та приймати інформацію, яка підтверджує їхні власні переконання, навіть якщо така інформація не має об'єктивного підґрунтя. Крім того, як стверджує Карен Норт, люди не лише «реально потребують підтверджуючої інформації» [Цит. 246], а й «хочуть знайти людей, які думають так само, щоб сказати їм, чому їхня думка є правильною» [Цит. 246].

Деякі організації використовують такі особливості людської психіки для здійснення таргетованого впливу на інтернет-користувачів. Завдяки точному таргетуванню й добору відповідного контенту людина опиняється в інформаційній оболонці, яка екранує інформаційні подразники, що не порушують гармонію її індивідуальної картини світу. Йдеться про системи «інформаційних бульбашок» та «луна-камер», які розглядаються фахівцями як сприятливе середовище для поширення дезінформації [138, С. 4].

Є очевидним, що в сучасному інформаційному просторі медіа не лише відображають події реального світу і ретранслюють соціальні смисли, а й самі продукують ці смисли та генерують нову «реальність». М. Маклуен, відомий своїм критичним поглядом на роль медіа у суспільстві,порівнює зміст повідомлення ЗМІ із соковитим шматком м’яса, який приносить із собою злодій, щоб приспати пильність сторожового пса нашого розуму [312, С. 22].

Ж. Бодріяр зазначає, що сучасні медіа прагнуть не стільки показати реальну ситуацію, скільки позначити свою позицію, висловити власну думку, яка за визначенням є суб’єктивною, а отже не може достовірно

відображати об’єктивну реальність. Таким чином, медіа «починає структурувати культурний простір в поняттях медійної реальності» [8], тобто, по суті, створює гіперреальність.

Цікавим є погляд на формування такої гіперреальності С. Дацюка [29]. Аналізуючи події 16 лютого 2022 року, коли не відбулося відкрите збройне вторгнення Росії, на яке всі чекали, С. Дацюк запитує: «Де з самого початку була подія?» І відповідає: «Вона була в медіа - там аргументувалася, відображалася, коментувалася. Але насправді повістка денна була завантажена подією, що полягалау відсутності події» [29]. І філософ робить висновок про те, що настає не просто ера постправди, а ера постподії і медіаподії, колиголовна подія відбувається не в реальному світі, а всередині самого медіа. Інакше кажучи, на наших очах медіа стають квазіекзистенціальним простором, куди поступово переміщається основне життя. І цей аспект має бути покладений як базовий в основу осмислення сучасних інформаційних війн [29].

Сьогодні все частіше говорять про те, що якщо подія не відбулася в медіа – вона не відбулася для соціуму, оскільки для людини не може бути значимою подія, про яку вона не знає. Ця думка не є новою. А. Моль ще в 1970-х роках писав: “Те, що не потрапило до каналів масової комунікації, сьогодні майже не впливає на розвиток суспільства [Цит. 101, С. 36]. У зв’язку з цим є очевидним значний вплив медіа на наші переконання, думки та спосіб сприйняття світу. Вони конструюють неповторну реальність, через яку ми сприймаємо та інтерпретуємо навколишній світ.

Водночас, у науковому дискурсі спостерігається розмаїтість поглядів дослідників на методи і прийоми, за допомогою яких медіа спотворюють дійсність та формують паралельні реальності. Свого часу У. Ліппман відзначав роль медіа у формуванні та підтриманні стереотипів, які «підміняють у суспільній свідомості політичну реальність» [308, С. 114]. У сучасному світі медіа активно використовують не тільки стереотипи, але й різноманітні образи та іміджі. Також одним з найбільш поширених

залишається класичний метод вибіркового представлення. Причому, цей метод є дуальним. З одного боку, «людина зацікавлена лише в тій інформації, яка підтверджувала б її переконання й оцінювання» [Цит. 68]. А з іншого боку, медіа, будучи заангажованими, можуть обирати, яку інформацію надавати споживачам,щоб задовольнити свої власні потреби та досягти своїх цілей. Однак, якщо стосовно масмедіа держава може встановлювати механізми контролю якості їх контенту, то в соціальних медіа ця проблема залишається нерозв'язаною. Особливо це стосується анонімних онлайн-ресурсів, які безперешкодно розповсюджують недостовірну інформацію, не боячись можливих наслідків.

З приводу цього висловлюють занепокоєність як окремі фахівці-практики, такі науковці. Зокрема, у 2020 році під час слухань в Комітеті Верховної Ради з питань цифрової трансформації доктор наук з державного управління, доцент та на той час завідувач кафедри інформаційної політики та цифрових технологій в Національній академії державного управління при Президентові України О. Карпенко запропонував ідентифікувати користувачів мережі Інтернет, що могло б вирішити дуже багато питань, пов'язаних із кіберзахистом і сферою кібербезпеки. Однак ця пропозиція була визнана «дуже соціальною дискусійною» і не знайшла широкої підтримки в експертному середовищі.

На наш погляд, ключовим чинником, що спонукає політиків загравати в цьому питанні з електоратом, продовжуючи рухатися в популістичному ключі, є непідготовленість суспільства «до переходу від матеріального світу до інформаційного [88]. Зараз ми все ще мислимо в рамках індустріального суспільства, тоді як фактично вже вийшли з нього і увійшли в інформаційну еру, де «суб’єктом усіх сучасних трансформацій і перетворень виступає інформація, яка стала основним товаром, стратегічним ресурсом і засобом виробництва» [149].

Раніше нами було зроблено висновок, що протягом багатьох років державна інформаційна політика України, яка намагалася продемонструвати

демократичні цінності та свободу слова, мало уваги приділяла питанням захисту від інформаційних загроз, які можуть виникнути, зокрема,внаслідок цілеспрямованого зовнішнього інформаційного впливу. В результаті, країна виявилася абсолютно неготовою до розв'язаної проти неї інформаційної війни у 2014 році.

Незважаючи на контроверсійність такого припущення, можливо в майбутньому доведеться визнати, що недотримання необхідного балансу між інформаційними свободами окремих індивідів та забезпеченням національної безпеки призвело до перекосу в бік індивідуальних інформаційних свобод і поставило під загрозу національну безпеку держави.

Свідченням неготовності держави приймати важливі рішення, пов'язані із сучасними інформаційними трансформаціями, є затягнення з врегулюванням відповідного законодавчого поля. Особливо слід зазначити, що в Україні досі не прийнято закон про дезінформацію,і серед чинників, що пояснюють цю ситуацію, можна відмітити непопулярність цієї теми серед медіа-спільноти та небажання політиків потрапляти під їхню критику з цього приводу. Як наслідок, «факти дезінформації сьогодні стоять фактично над законом, адже немає ані відповідної нормативної бази, ані механізму захисту від фейків» [49].

Маємо факт зволікання розгляду й інших питань, що свідчить про недостатню увагу до проблем інформаційної безпеки. Одним з таких питань є створення інтегрованої системи оцінки інформаційних загроз та реагування на них. Вже у 2018 році була розроблена та подана на розгляд і затвердження урядом відповідна Концепція [99], проте на сьогодні ні ця концепція, ні будь-який альтернативний варіант не прийняті.

У свою чергу, дослідники пропонували методики та інструментарій для раннього виявлення загроз інформацій безпеці. Зокрема, ще у 2012 році науковці Національної академії державного управління висунули ідею запровадження паспорта загроз [192]. Ще раніше це питання

розглядали Богданович В. Ю., Семенченко А. І. та Єжеєв М. Ф. [7]. У 2021 році Дзюба Т. М. та Опанасенко М. І.[145] знову повернулися до цієї теми.

Також до теми формування паспортів загроз звертається О. Рєзнікова [178, 179, 180], яка розгялає такі паспорти як зручну форму «систематизації результатів стратегічного аналізу, які використовуються для планування й адаптивного управління у сфері національної безпеки» [179].

До інших інструментів раннього виявлення загроз в інформаційній сфері також також належать різноманітні програмні та апаратні засоби для обробки та візуалізації геопросторової інформації. Зокрема, цим питанням займаються О. Резнікова [180, С. 38–39], Ю. Гладун із співавторами [17, С. 119], Н. Ткачук [207] та інші дослідники.

Існують й інші підходи до вибору методик раннього оцінювання загроз, причому основним є постійний моніторинг інформаційного простору, який можна здійснюватися як вручну, так і за допомогою автоматизованих систем збору та аналізу даних [56, 321].

Одним з перспективних напрямків є метод використання систем автоматичного аналізу текстів, що передбачає застосовування алгоритмів машинного навчання для виявлення ключових слів, термінів та інших індикаторів, які можуть свідчити про потенційні загрози в інформаційному просторі [147, 76]. Такий аналіз дозволяє швидко й ефективно виявляти нові загрози та тренди у розповсюдженні дезінформації й може бути використаний для запобігання таким загрозам в режимі реального часу.

Існують й принципово інші підходи до раннього виявлення дезінформаційних загроз. Зокрема, О. Данилюк [28] пропонує використовувати досвід радянської школи підривної діяльності з розгорнутою агентурною мережею як методику раннього виявлення гібридних загроз. Це передбачає «проактивний циклічний пошук» ознак такої діяльності силами «спеціально підготовлених фахівців центральних органів державної влади в кожній сфері державного управління та суспільного життя». Однак зазначимо, що цей підхід стосується більш агресивних дій в

інформаційному протиборстві і зазвичай пов’язується з діяльністю спеціальних служб.

Підсумовуючи вищевикладене, можемо зробити висновок, що враховуючи гнучкість та адаптивність системи раннього виявлення загроз, згадані вище інструменти, такі як паспорти загроз, моніторинг інформаційного простору, аналіз геопросторових даних, система автоматичного аналізу текстів, можуть застосовуватись в комплексі або окремо, і їх вибір залежить від конкретних потреб та умов. Проте, для ефективної протидії дезінформації необхідно більше, ніж просто ідентифікувати загрозу. Необхідний комплекс заходів, який передбачає весь алгоритм дій від вироблення стратегії державної політики у сфері протидії дезінформації до швидкої реакції на поточну загрозу та оцінювання результатів. Ми пропонуємо алгоритм, який має п'ять складових: Визначення, Захист, Виявлення, Реагування та Відновлення.

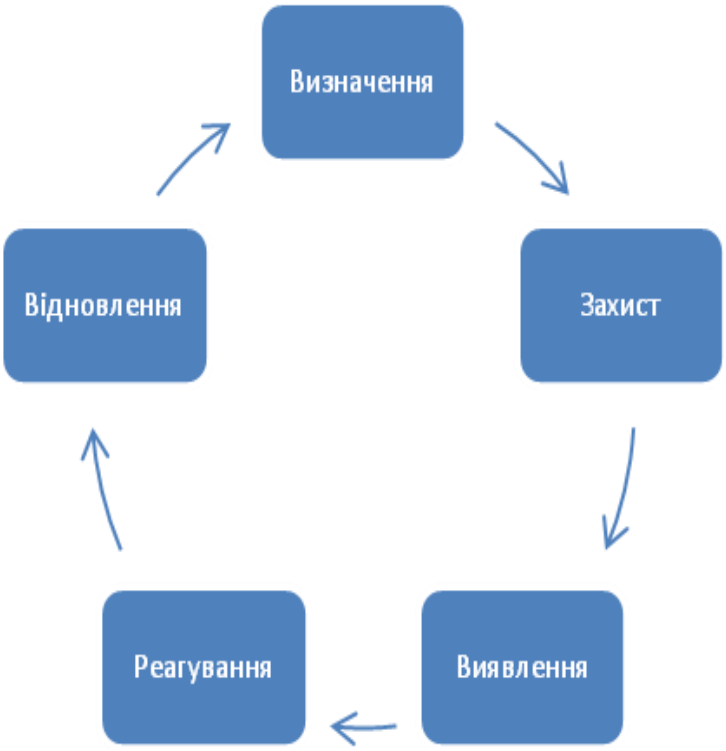


Рис. 2.1. Концепція протидії дезінформації

Джерело: складено автором за [348]

Розглянемо запропоновану концепцію протидії дезінформації детальніше. На стратегічному рівні, що належить до високого рівня управління, розробляються та приймаються ключові стратегічні рішення у сфері протидії дезінформації. Тут проводиться стратегічний аналіз потенційних дезінформаційних загроз, що можуть підважити інформаційну безпеку держави, а також розробляються стратегії державної політики протидії дезінформації та заходи, спрямовані на запобігання або подолання таких загроз. Таким чином, на стратегічному рівні виробляються ключові напрямки та методики протидії дезінформації з метою захисту державних інтересів та суспільства в цілому.

На тактичному рівні протидії дезінформації визначаються конкретні методи та заходи, спрямовані на реалізацію загальної стратегії протидії дезінформації на практичному рівні. Тактичний рівень можна поділити на дві основні функції: захист і виявлення.

На функції захисту вживаються заходи для захисту від дезінформаційних загроз. Це може включати розробку та впровадження механізмів фільтрації та перевірки інформації, підвищення обізнаності громадськості щодо методів дезінформації, вдосконалення заходів захисту від кібератак, а також розвиток та впровадження законодавчих та регуляторних механізмів для запобігання поширенню дезінформації.

На рівні виявлення зусилля зосереджуються на здатності вчасно виявляти та аналізувати дезінформаційні загрози в реальному часі, що дозволяє оперативно реагувати та вживати відповідних заходів для їх припинення чи мінімізації впливу. Функція виявлення дезінформаційних загроз може включати створення моніторингових систем для виявлення небажаних впливів у медіа, соціальних мережах та інших платформах, а також розвиток аналітичних інструментів для аналізу та ідентифікації дезінформаційних кампаній.

На операційному рівні протидії дезінформації вживаються конкретні заходи та стратегії, спрямовані на негайне реагування на дезінформаційні загрози та відновлення нормального функціонування після їхнього впливу.

На рівні реагування важлива оперативна реакція на виявлені дезінформаційні атаки. Це може включати швидке розгортання комунікаційних стратегій для нейтралізації дезінформації, розробку та розповсюдження правдивої інформації, а також співпрацю з медіа та іншими зацікавленими сторонами для виправлення недоречностей.

Рівень відновлення включає заходи, які вживаються після того, як дезінформаційна атака вже відбулася. Зокрема, це заходи, спрямовані на відновлення стабільності та довіри до інформаційного середовища. Це може включати проведення аналізу причин і наслідків атаки, розробку та реалізацію стратегій відновлення довіри громадськості до інформаційних джерел та інституцій, а також підвищення стійкості до подібних атак у майбутньому.

Важливо зауважити, що одним з результатів реалізації цієї концепції є потреба у створенні моделі інституціонального механізму вироблення державної політики у сфері протидії дезінформації. Це дозволить систематизувати та узгодити дії різних відомств та організацій, які займаються протидією дезінформації, забезпечуючи їх координацію та взаємодію. У наступному розділі роботи буде зроблено спробу розробки такої моделі, визначити її складові та принципи функціонування, а також механізми впровадження та контролю за її роботою.

2.3. Модель інституціонального механізму вироблення державної політики у сфері протидії дезінформації: розроблення та перспективи розвитку

У процесі формування механізмів державної політики у сфері протидії дезінформації, на нашу думку, найбільшим ефективним підходом

є використання інституціональної моделі, яка розглядає політику як складне системне явище [26, С. 32], що охоплює різні аспекти. Застосування інституціональної моделі в політичному аналізі обумовлене рядом факторів, серед яких:

1. Комплексність. Політична система складається з різних взаємозалежних інститутів та організацій, тому фокусування лише на процесах формування та прийняття рішень обмежує розуміння державної політики як комплексної системи. Інституціональна модель дозволяє досліджувати взаємодію та вплив різних інститутів на політичні процеси.

2. Стійкість та зміни. Інституції, у порівнянні з окремими політичними рішеннями, тяжіють до більшої стійкості та повільніших змін. Дослідження інституціональних чинників дозволяє краще зрозуміти, які сили та інтереси формують політичні інститути, та як вони впливають на політичні процеси з часом.

3. Широкий контекст. Інституціональна модель враховує не лише формальні політичні інститути, а й неформальні правила, норми та цінності, які також мають значний вплив на політичну систему. Врахування широкого контексту, в якому ухвалюються політичні рішення, дозволяє побачити зв'язки між політикою та іншими сферами життя, такими як економіка, культура та суспільство.

4. Довгострокові наслідки. Аналіз інституціональних факторів дозволяє передбачити, як зміна інституціональних рамок впливатиме на стабільність та мінливість політичної системи у майбутньому а також прогнозувати можливі тенденції та подальший розвиток такої системи.

5. Взаємодія акторів. Інституціональна модель враховує роль та взаємодію різних акторів у політичній системі, включаючи державні структури, наукові установи, приватний сектор, громадянське суспільство тощо. Вона аналізує, як ці інститути взаємодіють між собою та як впливають на прийняття рішень.

6. Національні особливості. Інституціональна модель передбачає контекстуальний підхід до політики з огляду на особливості конкретної країни, регіону чи культурного середовища. Вона визнає, що політичні системи та інститути можуть відрізнятися в різних контекстах і потребують ретельного аналізу та розуміння їх унікальних особливостей.

Дж. Аї вбачає три основні переваги інституціональної моделі: визначення чітких ролей та відповідальності різних інституцій; забезпечення стабільності та передбачуваності державної політики; ефективність і прозорість державних інституцій [251].

Зауважимо, що ключовим позитивним аспектом є узгоджені та синхронні дії, а також партнерські взаємовідносини між державними структурами та іншими зацікавленими сторонами, що нівелюють «боротьбу за місце під сонцем» державних організацій, які хоч і пов’язані між собою, але кожна «живе своїм життям» [249].

Як зазначає О. Дем’янчук, особливості розвитку інституціональної моделі державної політики проявляються у визначенні цілей та встановленні пріоритетів, у структурі управлінської ієрархії та у співвідношенні повноважень між усіма учасниками політики, а також у розмірах та силі впливу «горизонтальної» складової публічної політики [40].

У контексті розробки моделі інституціонального механізму вироблення державної політики у сфері протидії дезінформації важливо відзначити, що існують певна зони, в межах яких державні структури мають свою відповідальність (табл. 2.1). Ці зони відповідальності охоплюють різні аспекти діяльності, включаючи вироблення політики, прийняття рішень, впровадження заходів та контроль за їхнім виконанням. Державні структури відіграють ключову роль у цих процесах, оскільки вони мають доступ до ресурсів, законодавчих повноважень та можливостей для координації дій у сфері протидії дезінформації.

Таблиця 2.1

Зони відповідальності державних структур у сфері протидії дезінформації

Державний орган	Роль	Зона відповідальності
Міністерство культури та інформаційної політики	Вироблення культурних ініціатив. Розвиток програм медіаосвіти та інформаційної грамотності Розробка та впровадження стандартів та етичних правил для медіа	Розвиток національного інформаційного простору країни. Формування культурної політики. Взаємодія з медіа.
Міністерство освіти	Розвиток програм медіаосвіти та інформаційної грамотності.	Інтеграція медіаосвіти в навчальні програми.
Мінцифри	Розробка технологічних інструментів для виявлення та аналізу шкідливих впливів у мереж.і	Розвиток інформаційних технологій та цифрова трансформацію суспільства.
Національна рада з питань телебачення і радіомовлення	Встановлення стандартів контенту та контроль за його дотриманням. Видача ліцензій на медіаорганізації.	Регулювання телекомунікаційного ринку та захист прав споживачів.
Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ)	Моніторинг та аналіз інформаційних загроз. Захист від дезінформаційних індидентів.	Забезпечення безпеки інформаційних систем та захисту від кібератак.
Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКЕК)	Моніторинг мережі та реагування на поширення дезінформації.	Регулювання діяльності операторів зв'язку та інтернет-провайдерів.
Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (ДЦК ДССЗІ)	Моніторинг та аналіз інформаційних загроз. Кіберзазхист.	Виявлення, аналіз та реагування на кіберзагрози.
Головний ситуаційний центр при РНБОУ (ГСЦ РНБОУ)	Аналіз загроз і вироблення стратегії відповіді на них.	Аналіз ситуації з безпеки країни.
Міністерство зовнішніх справ	Дипломатичні зусилля з виявлення та протидії дезінформаційним загрозам.	Захист інтересів країни на міжнародній арені.
Національна поліція України	Розслідування кримінальних справ, пов'язаних із поширенням дезінформації та кіберзагрозами.	Забезпечення правопорядку та безпеки внутрішньої ситуації.
Міністерство оборони	Виявлення та припинення дезінформації. Попередження про можливі загрози. Розвиток стратегічних комунікацій.	Захист суверенітету та територіальної цілісності країни, забезпечення інформаційної безпеки.
Служба зовнішньої розвідки України	Аналіз зовнішніх загроз та розробка заходів протидії.	Збір та аналіз інформації.

Джерело: складено автором.

Важливо зауважити, що відповідно до Конституції України вищим координаційним органом у системі органів державного управління в галузі національної безпеки та оборони є Рада національної безпеки та оборони (РНБОУ), яка забезпечує формування і реалізацію державної політики в цій сфері. Також РНБОУ є органом, що має в компетенції визначення стратегічних національних інтересів, розробку планів забезпечення національної безпеки та прийняття рішень щодо найважливіших питань у

цій сфері. РНБОУ відповідає за проектування державних програм, законів, директив та інших нормативних актів, пов'язаних з національною безпекою і обороною. Слід відзначити, що найсміливіші та найбільш невідкладні заходи, спрямовані на протидію негативному інформаційному вплиу, що виходить з Російської Федерації, були прийняті саме Радою національної безпеки і оборони. Це стало можливим завдяки тим особливим повноваженням, яким наділено Раду. Зокрема, РНБОУ має право ухвалювати рішення щодо кризових ситуацій, які можуть негативно вплинути на національну безпеку України. Оскільки будь-яке загострення ситуації може бути визнане кризовим, такі повноваження дозволяють ефективно та оперативно реагувати на проблеми, розв’язання яких за інших обставин може забрати значно більше часу та ресурсів через необхідність додаткових узгоджень та дотримання бюрократичних процедур.

Проте, як зауважують критики такого підходу, хоч він і є найпростішим та дозволяє швидко ухвалювати радикальні рішення, на які за інших обставин могли б піти роки [6], така тактика підважує засади верховенства права та примат закону [71], і може призвести до втратити довіри з боку міжнародних партнерів. Тому важливо зберегти баланс між ефективністю і демократією. Так, у травні 2017 року відповідно до Закону України «Про санкції» [64] Указом Президента України [219] було введено в дію рішення РНБО про застосування санкцій до більш як 450 компаній і 1200 осіб. Особливістю цього рішення стала вимога до інтернет-провайдерів блокувати на території України доступ до «Mail.ru», «Яндекс», «Лабораторія Касперського», «Dr.Web» та низки інших російських соцмереж і інтернет-сервісів. Реакція на таке рішення виявилася суперечливою як всередині України, так і з боку світової спільноти. В НАТО запевнили, що підтримують позицію Києва, оскільки рішення про блокування російських інтернет-ресурсів є питанням національної безпеки, а не свободи слова [173] Водночас, генеральний

секретар Ради Європи заявив, що блокування сайтів суперечить свободі слова, а «такі широкі заборони не відповідають принципу пропорційності» [47]. Правозахисна організація Freedom House у своєму звіті зазначила, що ці санкції значно обмежили права українців і завдали шкоди інформаційному простору, але так і не досягли тих цілей, які переслідувала українська влада, коли їх запроваджувала [293]. Подібну позицію висловили «Репортери без кордонів» та ряд інших неурядових міжнародних організацій, а також окремі незалежні експерти. Зокрема, фахівець з міжнародного інформаційного права А. Пазюк, провівши детальний правовий аналіз зазначеного Указу Президента та рішення РНБО, дійшов висновку, що вони не відповідають критеріям законності та обґрунтованості [150]. З іншого боку, у певних обставинах навіть країни з розвиненою демократією змушені шукати способи обмеження свободи слова, а таке тимчасове обмеження демократії розглядається як захист власних цінностей [201]. Зокрема, це стосується рішення про блокування по всій Європі російських каналів RT та Sputnik [36].

Зазначимо, що крім проведення жорсткої санкційної політики, Рада національної безпеки і оборони виконує свої конституційні повноваження, координуючи та контролюючи діяльність органів виконавчої влади у сфері національної безпеки і оборони. Однак, ця функція викликає певну тривогу серед експертів, оскільки Президент України, який очолює РНБОУ, може використовувати цей орган як механізм впливу на дії уряду, незважаючи на те, що він не є головою виконавчої влади [71].

У складі РНБОУ також діє Головний ситуаційний центр України [221], створений у 2015 році з метою інформаційно-аналітичного супроводження діяльності державних органів, зокрема правоохоронних та безпекових. Центр функціонує як програмно-апаратний комплекс, що здійснює збирання, накопичення та обробку інформації, необхідної для підготовки та прийняття рішень у сфері національної безпеки і оборони [182].

Головний ситуаційний центр є ключовим елементом єдиної мережі ситуаційних центрів центральних органів виконавчої влади. Проте фахівці висловлюють думку, що цей орган потребує комплексного реформування, оскільки не виконує жодних аналітичних функцій, які характерні для подібних структур в інших країнах [180]. Слід зазначити, що на сучасному етапі у світі функціонує близько 300 ситуаційних центрів, які надають аналітичну підтримку урядам різних країн [167]. Такі центри відіграють важливу роль у перетворенні великого обсягу даних (Big Data) у структуровану аналітичну інформацію щодо ризиків і загроз національній безпеці, оскільки «більшість керівників страждають сьогодні вже не від браку вихідних даних, як це було раніше, а від надлишку» [207]. Наприклад, Президент США послуговується інформацією з чотирьох ситуаційних центрів; в Німеччині діє загальний інформаційно-ситуаційний центр федерального центру та земель, а в структурі наднаціонального європейського управління працює Спільний ситуаційний центр ЄС [207]. Проте, незважаючи на цю глобальну тенденцію, Головний ситуаційний центр України й далі займається переважно простим збором даних, що призводить до того, що в «Україні відбувається перетворення інформаційно-аналітичної діяльності на рудимент та інструмент узагальнення статистики» [207]. Ця проблема є предметом обговорення серед експертів і може вимагати комплексного реформування з метою досягнення вищого рівня аналітичних функцій та ефективного використання наявних даних.

Додатково до Головного ситуаційного центру, з метою забезпечення ефективної протидії дезінформації та збереження інформаційної безпеки України, у березні 2021 року було створено Центр з протидії дезінформації. Він функціонує як робочий орган Ради національної безпеки і оборони [228]. Основними завданнями центру є: аналіз та моніторинг подій та явищ у інформаційному просторі України, зокрема оцінка стану інформаційної безпеки та присутності України у світовому

інформаційному просторі; виявлення та дослідження потенційних загроз інформаційній безпеці держави, а також чинників, що впливають на формування таких загроз; прогнозування та оцінка їх наслідків для безпеки національних інтересів України; виявлення дезінформації і ворожої пропаганди та протидія їм, а також зменшення спроб деструктивного впливу на громадську думку [226].

Окремим напрямом діяльності Центру є вироблення пропозицій для Ради національної безпеки та оборони України у таких аспектах:

– розробка концептуальних підходів до вироблення державних стратегій у сфері протидії дезінформації;

– координація діяльності органів виконавчої влади у сфері інформаційної безпеки;

– здійснення системних заходів для сприяння суб'єктам сектору безпеки, інших державних органів у підвищенні їхньої ефективності;

– удосконалення законодавства та наукової бази для забезпечення захисту інформаційної безпеки та протидії дезінформації.

Крім того, Центр має додаткові повноваження, серед яких:

– участь у розвитку системи стратегічних комунікацій;

– участь у виробленні стратегії інформаційної безпеки України та аналіз її ефективності;

– участь у створенні системи оцінки інформаційних загроз та оперативного реагування на них;

– напрацювання методології моніторингу дезінформаційних матеріалів та маніпулятивної інформації тощо.

Отже, є очевидним, що Центр протидії дезінформації був створений з великими очікуваннями, але його ефективність не відповідає поставленим завданням. Діяльність центру обмежується переважно моніторингом та спростування окремих дезінформаційних повідомлень. В такий спосіб функції державного органу у сфері протидії дезінформації дублюють завдання, які вже успішно виконуються громадськими

організаціями, такими як "Детектор медіа", "Стопфейк" та інші, які отримують фінансування від міжнародних організацій. Хоча головною метою Центру має бути координація зусиль відповідних державних органів для ефективної протидії дезінформації із залученням до цього процесу всіх суб'єктів, які формують та реалізують державну політику у цьому напрямі.

Глибше вивчаючи інституціональну роль РНБО у сфері протидії дезінформації, варто відзначити важливу базову установу науково-аналітичного супроводу для Президента України та РНБОУ – Національний інститут стратегічних досліджень (НІСД), що функціонує як консультативно-дорадчий орган, який проводить науково-аналітичні та прогнозні дослідження щодо розвитку України та її національної безпеки. Інститут готує та представляє Президентові України та РНБОУ аналітичні матеріали, проекти програмних документів та нормативно-правових актів» [140]. У сфері протидії дезінформації НІДС здійснює широкий спектр досліджень для аналізу та виявлення актуальних загроз національній безпеці. Він бере участь у розробці стратегій протидії дезінформації та надає рекомендації щодо використання нових технологій. Інститут також розробляє необхідний інструментарій та формулює рекомендації залучення громадськості до цього процесу. Значну увагу привертають аналітичні доповіді експертів НІДС, серед яких виділяються дві фундаментальні монографії, що мають високий рівень цитування в наукових працях: «Світова гібридна війна: український фронт» (ред. В.П. Горбулін, 2017), та «Національна стійкість в умовах мінливого безпекового середовища» (О. Резнікова, 2022) [179].

Щодо органів виконавчої влади, то згідно зі Стратегією національної безпеки, уряд має обов'язок забезпечувати формування та реалізацію інформаційної політики держави, забезпечувати інформаційний суверенітет, фінансувати програми, пов'язані з інформаційною безпекою, а також спрямовувати і координувати діяльність міністерств та інших органів виконавчої влади у цій сфері [227].

Ця діяльність залучає різні силові та цивільні міністерства, організації та комітети, які безпосередньо або опосередковано працюють у сфері інформаційної безпеки. Проте, недостатня структурованість управління та координація дій різних інститутів призводять до неефективності у виконанні ними своїх функцій. Різні органи виконують подібні функції, тоді як інші залишаються нереалізованими через недостатні ресурси або непорозуміння між відомствами стосовно повноважень і відповідальності.

У рамках аналізу діяльності уряду наша увага перш за все зосереджена на діяльності Міністерства культури та інформаційної політики України (МКІП). Під його егідою створено Центр стратегічних комунікацій та інформаційної безпеки, який переважно акцентує увагу на просвітницькій роботі [238]. Зокрема, у 2021 було запущено національний проект з медіаграмотності «Фільтр»[125]. Згідно з результатами всеукраїнського тесту з медіаграмотності, проведеного восени 2022 року в рамках Глобального тижня медіаграмотності, більше половини учасників продемонстрували високий рівень критичного мислення [232]. За підсумками 2022 року основними результатами роботи МКІП у сфері протидії дезінформації та поширенні достовірної інформації стали: створення телемарафону #UAразом; діяльність Школи протидії дезінформації в рамках підвищення кваліфікації для українських держслужбовців та робота проекту з медіаграмотності «Фільтр»; розширення діяльності національного інформагентства «Укрінформ»; участь у спільній роботі, спрямованій на застосування міжнародних санкцій до російських телеканалів та заборону їх мовлення; розробка євроінтеграційного закону «Про медіа» [124]. Водночас, було прийнято й ряд неефективних рішень. Зокрема, у 2021 році МКІП передало Мінінтеграції управління держпідприємством, що включає в себе телеканали FREEДОМ, UATV та агентство "Укрінформ" [121], але за короткий час це підприємство повернулося до МКІП.

Щодо Міністества освіти, то діяльність цього відомства у сфері протидії дезінформації спрямована переважно на розвиток медіаосвіти та медіаграмотності. У 2011 році медіаосвіту було введено як експериментальну складову шкільної програми в рамках програми ООН «Освіта для сталого розвитку» [131]. Цей крок відображав початок розвитку умінь аналізу та критичного мислення щодо інформації. У квітні 2016 року Президія НАПН України схвалила оновлену Концепцію, що враховує швидкий розвиток технологій та масмедіа [80]. Наразі медіаграмотність викладається в закладах загальної середньої освіти у формі окремих курсів або інтегровано в інші навчальні премети [131].

Міністерство закордонних справ активно впроваджує Комунікаційну стратегією для підвищення іміджу України та протидії дезінформації [123]. Це включає комунікацію з партнерами за кордоном та оперативне спростування недостовірної інформації про Україну [122]. Зокрема, з початку збройної агресії РФ проти України Росія використовує «всі методи і способи дезінформації, спрямовані на дискредитацію самого рішення країн-членів НАТО постачати озброєння Україні». [53]. Особливої уваги потребує викриття таких фейків у країнах ЄС, де представники органів державної влади повинні організувати поширення власних контрнаративів, що пояснюють важливість підтримки України у війні проти Росії. [53]

Також значну роль у протидії дезінформації відіграє Міністерство цифрової трансформації, особливо з урахуванням того, що «сучасним трендом стають цифрові технології» [84]. Перш за все варто відзначити проект «Дія», який є прикладом створення прямого каналу комунікації між громадянами та державою. Крім того, від початку березня 2022 року у будь-якій точці Україні за наявності Wi-Fiy «Дії» можна переглядати телемарафон #UAразом та слухати «Українське радіо» [175].

Національна рада України з питань телебачення і радіомовлення (НРТР) відіграє ключову роль у формуванні державної політики у сфері

протидії дезінформації. Це незалежний колегіальний орган, що «здійснює державне регулювання, нагляд та контроль у сфері медіа» [66]. Громадська рада є дорадчо-консультативним органом при НРТР.

Крім того, у 2022 році національним медіарегулятором було проведено комунікацію з керівництвом Єврокомісії, рядом європейських регуляторних органів, європейськими супутниковими платформами та глобальними медіагрупами з метою вироблення правових механізмів для заборони трансляції російських телеканалів в інформаційному просторі ЄС. Результатом цієї роботи стало блокування Європейською Комісією не лише телеканалів RT та Sputnik (які були першими включені до санкційних списків), а й телеканалів «РТР Планета»/RTR Planeta, «Россия 24»/Russia 24, «Международный телецентр»/TV Centre International [134]. Також, з метою протидії поширенню дезінформації, ще у грудні 2020 року НРТР підписала Меморандум про співпрацю з громадською організацією «Центр медіареформи» (ГО «Стопфейк») [135].

Важливо відзначити, що в сучасних умовах, коли дезінформація становить загрозу національній безпеці держави, громадські організації не лише сприяють прозорості та відповідальності влади, а й виступають експертами та консультантами державних органів, а також здійснюють моніторинг інтернет-простору з метою виявлення і спростування дезінформації та стають ініціаторами просвітницької роботи серед населення. Серед таких громадських організацій – Інститут масової інформації» (IMI) [79], медіаорганізація "Інтерньюз-Україна" [81] , ГО «Детектор медіа» [37], ГО «Стопфейк», що адмініструє однойменний сайт StopFake.org [237], незалежна ініціатива InformNapalm [303], український проект фактчекінгу VoxCheck [342], неурядовий проект Texty.org.ua [314]. Окрім основного змісту, на веб-сайті Texty.org.ua діє розділ «Інфовійна» [202] та успішно реалізований проект "Тролесфера", в ході якого оброблено значний обсяг даних із соціальної мережі Facebook та

проаналізовано особливості діяльності проросійських тролів в цій мережі [203].

Підсумовуючи вищевикладене, можемо констатувати, що в Україні зроблено значну роботу у сфері протидії дезінформації, проте зберігається дуже розгалужена система залучення державних інституцій з дещо дублюючими та перехрещеними повноваженнями» [51], що обмежує їх ефективність. У зв'язку з цим виникає необхідність розроблення моделі інституціонального механізму вироблення державної політики у сфері протидії дезінформації. Це дозволить забезпечити ефективне та координоване реагування держави на дезінформаційні загрози.

Необхідно зауважити, що забезпечення ефективного та координованого реагування держави на загрози дезінформації охоплює значно більше, ніж проста реакція на окремі події. Це передбачає систематичний аналіз та прогнозування потенційних сценаріїв, розвиток адаптивних стратегій та механізмів захисту, а також постійний моніторинг та вдосконалення методів протидії. Крім того, координоване реагування означає співпрацю між усіма суб'єктами, які «мають владу та контроль над інформаційними механізмами. Такими суб'єктами можуть бути органи державної влади, політичні лідери, ЗМІ, соціальні медіа, громадські організації та об'єднання» [85]. Тільки шляхом спільних зусиль та обміну досвідом можна ефективно протидіяти дезінформації.

Також важливо врахувати, що ефективність інституціонального механізму державного управління у сфері протидії дезінформації значною мірою залежить від ряду факторів, серед яких особливо важливим є політичний контекст. Вплив політичного фактора можна розглядати через кілька ключових аспектів. По-перше, успішне впровадження та функціонування механізмів протидії дезінформації потребує активної підтримки з боку політичних лідерів та урядових структур. Це передбачає наявність чіткої політичної волі та розуміння загрози дезінформації, що дозволить ухвалювати рішучі заходи для її протидії. Зауважимо також, що

різні актори на політичній арені можуть мати власні інтереси та пріоритети, що може затримати чи ускладнити ухвалення та впровадження необхідних заходів. Крім того, ефективна протидія дезінформації потребує належної законодавчої бази. Політичні процеси, такі як прийняття нових законів чи зміна існуючих, можуть бути складними і вимагати широкої політичної підтримки.

Крім політичного контексту, важливим фактором, який впливає на ефективність інституціонального механізму вироблення державної політики у сфері протидії дезінформації, є інформаційна культура. Цей аспект охоплює рівень освіченості суспільства, його здатність критично оцінювати інформацію та відрізняти дезінформацію від об'єктивної правди. Високий рівень інформаційної культури сприяє зменшенню вразливості суспільства перед дезінформацією, оскільки люди стають менш схильними до маніпуляцій та поширення міфів. Таким чином, врахування рівня інформаційної культури населення та розробка програм її підвищення є важливим елементом успішної стратегії протидії дезінформації. Активна просвітницька діяльність, впровадження освітніх програм та підтримка медіа-освіти можуть сприяти формуванню критичного мислення та відповідального ставлення до інформації в суспільстві.

Також значним фактором, який впливає на ефективність моделі, є рівень технологічного розвитку суспільства. Високотехнологічні засоби та інноваційні підходи до збору, аналізу та поширення інформації можуть значно підвищити швидкість та ефективність реагування на дезінформацію. Наприклад, розвиток штучного інтелекту та аналітичних систем дозволяє автоматизувати процес фільтрації та аналізу інформації з метою виявлення шаблонів дезінформації та маніпуляцій.

Застосування сучасних технологій також дозволяє доносити достовірну інформацію та контролювати поширення дезінформації у режимі реального часу. Таким чином, рівень технологічного розвитку визначає можливості

суспільства протидії дезінформації та впливає на швидкість та якість реагування на загрози.

Роль громадянського суспільства також є ключовим фактором у протидії дезінформації та впливає на ефективність інституціонального механізму державного управління в цій сфері. Громадянське суспільство виступає як важливий стейкхолдер у забезпеченні прозорості, відкритості та публічного дискурсу, що сприяє виявленню та розкриттю випадків дезінформації. Громадські організації, незалежні медіа, активісти та журналісти можуть відігравати важливу роль у контролі інформації, перевірці її достовірності та поширенні правдивих фактів. Їхні зусилля спрямовані на розкриття дезінформації та надання громадянам доступу до об'єктивної та достовірної інформації. Крім того, громадянське суспільство може впливати на формування політики у сфері протидії дезінформації шляхом активної участі в публічному обговоренні, лобіюванні та сприянні прийняттю відповідних законодавчих ініціатив. Його мобілізація та організаційна діяльність можуть стимулювати урядові структури до прийняття ефективних заходів протидії дезінформації.

Міжнародна співпраця також відіграє важливу роль у протидії дезінформації та формуванні ефективних механізмів державного управління в цій сфері. Партнерство між країнами сприяє розробці та впровадженню спільних стратегій та програм, спрямованих на протидію дезінформації в глобальному масштабі. Крім того, міжнародні організації та форуми надають платформу для обговорення проблеми дезінформації та спільного пошуку шляхів її вирішення.

Участь у міжнародних ініціативах дозволяє країнам зміцнювати свої внутрішні механізми протидії дезінформації шляхом використання найкращих практик та стандартів, розроблених на міжнародному рівні. Крім того, така співпраця сприяє встановленню довіри між країнами та підвищенню ефективності спільних зусиль у боротьбі з дезінформацією.

Фінансові ресурси є ключовим фактором для успішної реалізації моделі інституціонального механізму державного управління у сфері протидії дезінформації. Належне фінансування дає змогу розробляти та впроваджувати нові технології та інновації у цій сфері. Також достатні фінансові ресурси дозволяють забезпечити навчання та підготовку фахівців у галузі протидії дезінформації, а також підтримувати дослідницькі проекти та ініціативи, спрямовані на виявлення та аналіз дезінформаційних загроз. Крім того, належне фінансування сприяє розвитку та підтримці мережі партнерів у сфері протидії дезінформації, зокрема громадських організацій, активістських груп, незалежних дослідницьких центрів та інших.

Нарешті, стратегічне партнерство відіграє важливу роль у формуванні та реалізації інституціонального механізму державного управління у сфері протидії дезінформації. По-перше, стратегічне партнерство дозволяє об'єднувати ресурси та експертизу різних сторін для спільного розроблення та впровадження ефективних стратегій боротьби з дезінформацією. Це може включати обмін даними, спільні дослідження, розробку технологічних рішень та координацію дій для виявлення та протидії дезінформаційним кампаніям. По-друге, стратегічне партнерство сприяє підвищенню ефективності та швидкості реагування на поточні виклики та загрози у сфері дезінформації. Швидкий та координований обмін інформацією дозволяє оперативно реагувати на негативні впливи дезінформації та вживати відповідних заходів для її ліквідації. По-третє, стратегічне партнерство сприяє підвищенню рівня довіри та легітимності дій у сфері протидії дезінформації. Спільна діяльність та взаємна підтримка дозволяє зміцнювати довіру громадськості до рішень державних органів та збільшувати ефективність їх впровадження.

На рис. 2.2. представлені фактори, що впливають на формування інституціонального механізму вироблення державної політики у сфері протидії дезінформації.

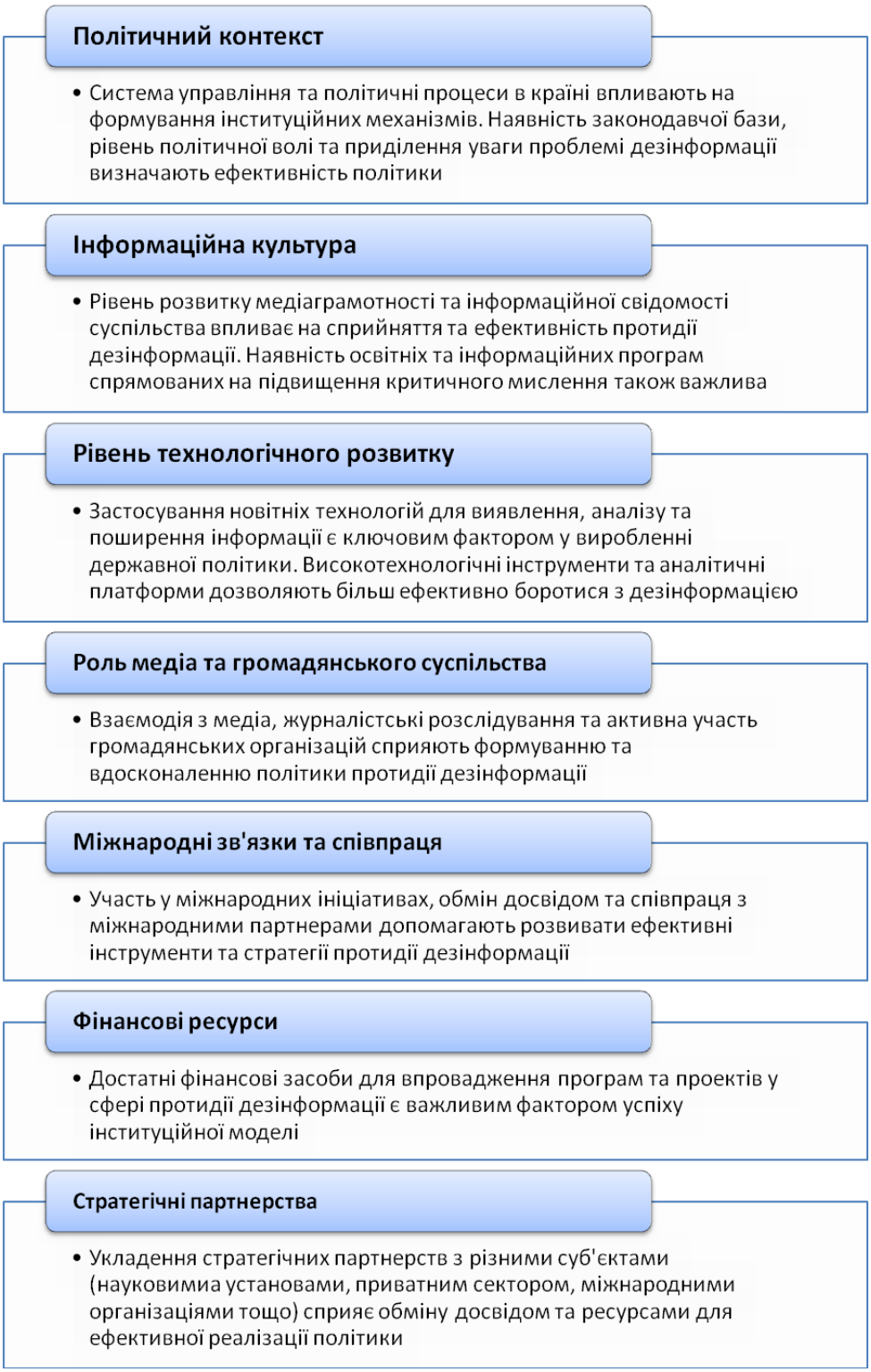


Рис. 2.2. Ключові фактори, що впливають на формування інституціонального механізму вироблення державної політики у сфері протидії дезінформації

Джерело: складено автором.

Ґрунтуючись на результатах аналізу ключових факторів, що можуть вплинути на ефективність інституціонального механізму вироблення державної політики у сфері протидії дезінформації, ми можемо перейти до аналізу основних принципів та стратегій які будуть лежати в основі такого механізму. Це дозволить визначити загальні принципи, за якими будуть виконуватися всі подальші дії.

Однією з ключових стратегій є розробка ефективних заходів захисту. Враховуючи складність сучасного інформаційного середовища та швидкість поширення дезінформації, важливо розробити імунітет до негативного впливу шляхом впровадження адекватних заходів захисту. Ця стратегія передбачає аналіз потенційних загроз, розробку превентивних заходів та механізмів реагування на випадки дезінформації. Ключовою метою є забезпечення надійного захисту інформаційного простору та збереження довіри громадськості до інформаційних джерел.

Другою стратегією є ефективний моніторинг і аналіз. Враховуючи постійну зміну інформаційного ландшафту та розвиток нових методів поширення дезінформації, важливо мати систему, що забезпечує постійний моніторинг і аналіз інформаційного середовища. Ця стратегія передбачає впровадження ефективних інструментів та методів для виявлення та аналізу дезінформації, включаючи використання аналітичних інструментів, штучний інтелект та спеціалізовані алгоритми. Метою цієї стратегії є оперативна реакція на дезінформацію, розуміння її поширення та впливу, а також розробка на цій основі стратегій протидії та запобігання майбутнім загрозам.

Третьою стратегією є швидка реакція та оперативні контрдії. Ця стратегія передбачає налагодження механізмів та процедур, спрямованих на оперативне виявлення, аналіз та реагування на випадки дезінформації. Важливо мати систему швидкого реагування, яка дозволяє оперативно втручатися та контролювати поширення дезінформації, а також відновлювати довіру до інформації шляхом надання достовірної інформації та відповіді на маніпулятивні чи неправдиві повідомлення. Ця стратегія спрямована на

мінімізацію шкоди від дезінформації та швидке відновлення нормального функціонування інформаційного середовища.

Серед ключових принципів ефективної політики протидії дезінформації важливе місце займає принцип доказової основи. Цей принцип передбачає, що будь-які заходи та стратегії, спрямовані на боротьбу з дезінформацією, повинні базуватися на найкращих доступних доказах та наукових дослідженнях. Врахування науково обгрунтованих підходів дозволяє забезпечити ефективність та обґрунтованість у виборі стратегій протидії. Крім того, цей принцип підкреслює важливість систематичного аналізу даних та використання емпіричних даних для прийняття рішень у сфері протидії дезінформації. Науково обгрунтовані підходи дозволяють уникати суб'єктивних оцінок та ефективніше використовувати ресурси для досягнення мети – забезпечення інформаційної безпеки та захисту громадян від шкідливого впливу дезінформації.

Далі розглянемо принцип співпраці і координації дій. Цей принцип передбачає активну взаємодію між різними суб'єктами, що мають інтерес та вплив у цій сфері, з метою спільного досягнення поставлених цілей. Співпраця охоплює об'єднання зусиль між державними органами, громадськими організаціями, приватним сектором та міжнародними партнерами для розробки та впровадження ефективних стратегій протидії дезінформації. Це може включати спільне планування заходів, обмін інформацією, ресурсами та експертними знаннями, а також координацію дій для запобігання поширенню дезінформації та реагування на неї.

Координація дій є не менш важливою складовою цього принципу і передбачає систематичне узгодження дій між різними суб'єктами з метою досягнення спільних цілей. Це включає в себе узгодження стратегій, розподіл відповідальності, встановлення механізмів комунікації та спільний моніторинг ефективності заходів.

Наступним виокремимо принцип прозорості та відкритості, який є невід'ємною складовою ефективного інституційного механізму державного

управління у сфері протидії дезінформації та передбачає доступність інформації про дії, рішення та процеси, пов'язані з протидією дезінформації, для громадськості та зацікавлених сторін.

Прозорість означає відкритий доступ до інформації про стратегії, дії та ресурси, що використовуються для протидії дезінформації. Це включає в себе публічні звіти, відкриті дані, проведення консультацій з громадськістю та забезпечення доступу до рішень і процесів управління.

Відкритість означає готовність до взаємодії із зацікавленими сторонами та громадськістю, до обговорень, консультацій та обміну інформацією. Це також включає в себе відкритість до критики та відповідальність за результати дій.

У свою чергу, принцип задіяності різних інститутів визначає необхідність активної участі різних органів, установ та організацій у процесі формування та реалізації стратегій протидії. Цей принцип сприяє комплексному підходу до проблеми дезінформації та забезпеченню взаємодії різних структур із різними компетенціями та ресурсами.

Також важливо дотримуватись принципу активної комунікації з цільовими групами, під якими ми розуміємо широкий спектр суспільства, включаючи громадян, медіа, державні та недержавні організації, а також інші зацікавлені сторони. Забезпечення відкритості, доступності та взаємодії з громадськістю сприяє побудові довіри до державних інституцій та ефективному розповсюдженню інформації про заходи захисту від дезінформації. Цей принцип дозволяє забезпечити взаєморозуміння, співпрацю та сприйняття заходів протидії дезінформації на різних рівнях суспільства, що є важливим елементом ефективної стратегії боротьби з цією загрозою інформаційної безпеки.

Останній принцип - оцінювання результатів, є завершальним кроком у циклі політики протидії дезінформації. Цей принцип передбачає систематичний аналіз та оцінку ефективності заходів, які були впроваджені, з метою виявлення досягнених результатів, виявлення слабких сторін та

можливостей для поліпшення. Оцінка результатів дозволяє не лише визначити ефективність інституційної моделі та її складових елементів, але й забезпечує постійне вдосконалення стратегій протидії дезінформації на основі накопиченого досвіду та найкращих практик. Такий підхід дозволяє забезпечити адаптацію до змін у сфері інформаційної безпеки та ефективну реакцію на нові виклики та загрози.

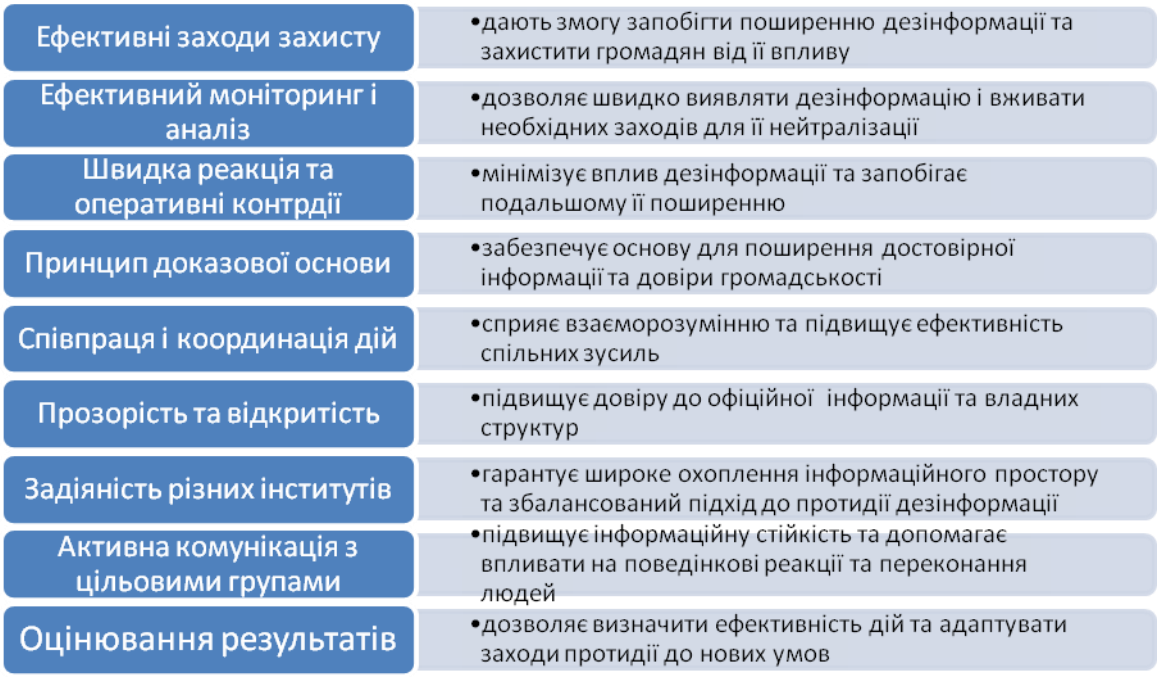


Рис. 2.3. Ключові принципи та стратегії моделі інституціонального механізму вироблення державної політики у сфері протидії дезінформації

Джерело: складено автором.

Після визначення принципів та стратегій ми переходимо до наступного етапу – аналізу методів та засобів збору, аналізу та поширення інформації про дезінформацію. Першим важливим елементом у цьому контексті є моніторинг медіа та соціальних мереж, який відіграє ключову роль у виявленні дезінформації. Цей метод передбачає постійне відстеження публікацій у засобах масової інформації та соціальних мережах з метою виявлення потенційно недостовірної інформації. Він дозволяє оперативно

реагувати на поширення дезінформації та вживати відповідних заходів протидії.

Аналітичні інструменти є важливим елементом у виявленні та аналізі дезінформації. Ці інструменти допомагають обробляти великі обсяги даних, виявляти тенденції та патерни поширення неправдивої інформації, а також встановлювати джерела дезінформації.

Експертна оцінка є важливим етапом у визначенні достовірності інформації. Цей метод передбачає залучення фахівців з різних галузей для оцінки об'єктивності та достовірності інформації, що допомагає зробити обґрунтовані висновки.

Публічні кампанії спрямовані на підвищення обізнаності громадськості щодо феномену дезінформації та методів боротьби з нею. Цей метод передбачає активне поширення інформації через різноманітні канали з метою формування критичного мислення та навичок розпізнавання дезінформації серед населення.

Створення спеціальних урядових або недержавних структур, таких як спеціалізовані ради, комітети або комісії, допомагає у координації зусиль у протидії дезінформації. Ці організації можуть займатися як розслідуванням конкретних випадків дезінформації, так і розробкою стратегій протидії загальним трендам в цій сфері.

Міжнародне співробітництво відіграє важливу роль у протидії дезінформації, оскільки цей феномен часто перетинає межі країн. Спільна робота між державами, міжнародними організаціями та іншими зацікавленими сторонами дозволяє обмінюватися досвідом та ресурсами у боротьбі з дезінформацією.

Законодавчі заходи, такі як прийняття та реалізація спеціальних законів та регулятивних актів, є важливим інструментом у протидії дезінформації. Вони встановлюють правила та стандарти для вирішення проблеми дезінформації та забезпечують їх виконання.

Ці методи допомагають сформувати комплексний підхід до протидії дезінформації та забезпечують ефективність інституціонального механізму державного управління у цій сфері. Проте кожен з цих методів має як свої

переваги, так і недоліки (табл. 2.2). Тому важливо ретельно обирати та комбінувати їх для максимально ефективної протидії дезінформації.

Таблиця 2.2

Методи та засоби збору, аналізу та поширення інформації

Функція	Переваги	Недоліки
Моніторинг медіа та соціальних мереж		
Відстеження поширення інформації та виявлення дезінформації у медіа та соціальних мережах	**Швидкість реакції:** Дозволяє оперативно виявляти та реагувати на дезінформацію в режимі реального часу	**Обмежений обсягом аналізу:** Моніторинг може не охопити всі джерела дезінформації або не враховувати певні контекстуальні фактори
Аналіз тенденцій та популярних тем для виявлення потенційно шкідливих впливів	**Глибокий аналіз:** Надає можливість докладного аналізу контенту та ідентифікації ключових тенденцій	**Велика кількість даних:** Обробка великого обсягу інформації може бути витратною за часом та ресурсами
	Підвищення ефективності: Допомагає визначати ефективність заходів протидії дезінформації та коригувати стратегію відповідно до результатів моніторингу	**Ризик помилок:** Існує можливість неправильного інтерпретування даних або невірного визначення дезінформаційного контенту
Аналітичні інструменти		
Аналіз та обробка великих обсягів даних для виявлення та аналізу дезінформації.	**Обробка великого обсягу даних**: Дозволяє швидко та ефективно обробляти великі масиви інформації.	**Потреба у великих обсягах даних:** Метод потребує значних обсягів даних для ефективної роботи.
Виявлення патернів та тенденцій у поширенні дезінформаційного контенту.	**Виявлення складних зв'язків:** Допомагає виявити складні зв'язки між різними джерелами дезінформації та їх поширенням.	**Ризик помилок:** Недостатність точних алгоритмів може призвести до помилкового аналізу даних.
Використання алгоритмів машинного навчання та штучного інтелекту для автоматизації аналізу	**Автоматизація процесу:** Застосування алгоритмів машинного навчання дозволяє автоматизувати процес аналізу даних.	**Складність в розумінні результатів:** Потребує кваліфікованих аналітиків для правильного інтерпретування результатів.
Експертна оцінка		
Оцінка ризиків та загроз, пов'язаних з дезінформацією.	**Експертна думка:** Використання знань та досвіду кваліфікованих експертів для оцінки ситуації.	**Суб'єктивність:** Оцінка може бути суб'єктивною, залежно від думки та поглядів кожного експерта.
Визначення рівня впливу дезінформації на суспільство, політику та економіку.	**Швидкість:** Може забезпечити швидкий аналіз та оцінку ситуації за участі кваліфікованих фахівців.	**Неоднорідність результатів:** Різні експерти можуть давати різні оцінки, що може призвести до неоднозначних результатів.
Формування рекомендацій щодо протидії дезінформації на основі експертної думки	**Гнучкість:** Метод може бути адаптований до різних контекстів та ситуацій.	**Залежність від складу експертної групи:** Результати можуть значно змінюватися в залежності від складу та компетенції експертної групи.
Публічні кампанії		
Залучення громадськості до участі у протидії дезінформації та підвищення її обізнаності щодо методів її виявлення.	**Масовий вплив:** Дозволяє досягти широкого аудиторії та залучити до участі різні соціальні групи.	**Ефективність:** Часто важко виміряти конкретний вплив публічних кампаній на свідомість та поведінку громадян.

Продовження таблиці 2.2

Сприяння формуванню культури критичного мислення та медіаграмотності.	**Інформаційна доступність:** Публічні кампанії можуть поширювати інформацію широкомасштабно, використовуючи різні медійні канали.	**Витрати:** Проведення публічних кампаній може бути дорогим та часо- і ресурсомістким.
Спеціальні комісії та агентства		
Створення спеціалізованих організацій для координації та проведення заходів щодо виявлення, аналізу та протидії дезінформації.	**Спеціалізація:** Організації можуть бути спеціалізовані саме на роботі з дезінформацією та мати відповідний досвід і знання.	**Фінансування:** Недостатнє фінансування може обмежувати їхню ефективність та можливості.
Забезпечення ефективної співпраці між різними державними та недержавними структурами у сфері протидії дезінформації.	**Координація:** Комісії, ради та комітети забезпечують координацію дій між різними зацікавленими сторонами та забезпечують їх співпрацю.	**Політизація:** Існує ризик політизації роботи таких організацій та комісій, що може впливати на їхню об'єктивність та ефективність.
Вироблення та реалізація стратегій інформаційного контрзаходу та підвищення інформаційної стійкості суспільства.	**Гнучкість:** Вони можуть швидко реагувати на виниклі ситуації та розробляти стратегії протидії.	**Відсутність співпраці:** Іноді може бути складно досягти співпраці між різними стейкхолдерами через різні інтереси та підходи.
Міжнародне співробітництво		
Співпраця між державами та міжнародними організаціями для ефективної протидії дезінформації та обміну інформацією.	**Ресурси:** Дозволяє залучати ресурси та експертизу з різних країн для вирішення спільних проблем.	**Різні підходи:** Різні країни можуть мати різні підходи до протидії дезінформації, що може ускладнити спільну роботу.
Вироблення спільних стратегій та стандартів у сфері протидії дезінформації.	**Обмін досвідом:** Дозволяє країнам взяти на озброєння досвід та практики інших країн у протидії дезінформації.	**Політичні обмеження:** Політичні відмінності між країнами можуть призвести до затримок або обмежень у співробітництві.
Обмін найкращими практиками та технологіями між країнами для підвищення інформаційної стійкості суспільства.	**Міжнародний вплив:** Може мати більший вплив на глобальному рівні в протистоянні дезінформації.	
Законодавчі заходи		
Регулювання та контроль за поширенням дезінформації шляхом прийняття відповідних законодавчих актів.	**Юридична обов'язковість:** Законодавчі заходи мають юридичну силу та зобов'язують суб'єктів до їх виконання	**Обмеження свободи слова:** Іноді законодавчі заходи можуть ставити під загрозу свободу слова та вираження думок
Забезпечення правової бази для притягнення до відповідальності тих, хто поширює дезінформацію.	**Універсальність:** Можливість створення загальнодержавних правил та норм, що регулюють дії всіх суб'єктів.	**Складність процесу:** Процес прийняття законодавчих актів може бути складним та тривалим.
Створення правил та норм, спрямованих на запобігання та припинення дезінформаційних дій.	**Можливість притягнення до відповідальності:** Законодавчі акти надають правові механізми для притягнення до відповідальності осіб, що поширюють дезінформацію.	**Виклики виконання:** Необхідності впровадження та забезпечення виконання законодавчих заходів можуть викликати труднощі

Джерело: складено автором.

Розглянувши методи та засоби збору, аналізу та поширення інформації про дезінформацію, переходимо до наступного етапу – визначення механізмів протидії цьому явищу. Важливо зауважити, що для успішної інституціональної моделі протидії дезінформації необхідно встановлення системи механізмів, яка охоплює всі аспекти формування та реалізації державної політики у цій сфері. Від цього залежить ефективність та системність заходів протидії дезінформації. Тому розгляд і розробка конкретних механізмів в контексті цієї моделі є важливим етапом у виробленні успішної стратегії протидії дезінформації.

Першим механізмом, який розглянемо, є формування спеціалізованих робочих груп або комісій для аналізу ситуації та вироблення стратегій. Цей механізм передбачає створення організаційних структур, які складаються з експертів, представників владних органів, громадських організацій та інших зацікавлених сторін з метою координації та співпраці у сфері протидії дезінформації. Такі робочі групи або комісії зазвичай складаються з фахівців з різних сфер - від інформаційних технологій до політичних наук, що дозволяє забезпечити комплексний підхід до аналізу та розробки стратегій. Вони виконують ряд функцій, включаючи вивчення ситуації на інформаційному просторі, ідентифікацію ключових проблем та викликів, а також розробку та реалізацію конкретних заходів і стратегій протидії дезінформації.

Наступним дієвим механізмом є проведення досліджень інформаційного простору для виявлення та аналізу патернів дезінформації. Основна мета таких досліджень полягає в ідентифікації та аналізі шаблонів, які можуть включати поширення фейкових новин, маніпулювання інформацією, створення конспірологічних теорій чи інші методи впливу на громадську думку. Це дозволяє не лише виявити потенційні випадки дезінформації, а й зрозуміти їхні причини, механізми поширення та вплив на суспільство, що, у свою чергу, дає можливість розробляти більш ефективні

стратегії протидії дезінформації та впроваджувати необхідні заходи з мінімізації її впливу.

Серед ключових механізмів протидії дезінформації необхідно також назвати розробку та ухвалення відповідних законодавчих актів та регуляторних норм. Такий механізм відіграє важливу роль у створенні правової бази для боротьби з дезінформацією, що визначає правила та процедури, за якими буде відбуватися реагування на дезінформаційні дії та їхні наслідки. Законодавчі акти можуть передбачати встановлення відповідальності за поширення дезінформації, механізми контролю за медійним простором, регулювання діяльності інтернет-платформ, а також створення стандартів та процедур для виявлення та виправлення фактів дезінформації. Такі законодавчі ініціативи відображають стратегічні підходи держави до забезпечення інформаційної безпеки та підтримки демократичних цінностей у суспільстві.

Встановлення механізмів моніторингу та виявлення дезінформації в режимі реального часу є ще одним дієвим засобом протидії дезінформації. Він полягає у впровадженні систем, які постійно відстежують та аналізують інформаційний простір для оперативного виявлення дезінформаційних інцидентів в режимі реального часу. Цей механізм включає в себе розробку та застосування спеціалізованих алгоритмів та програмних засобів для виявлення потенційно небезпечних матеріалів. Такі системи можуть використовувати штучний інтелект, машинне навчання та інші технології для пошуку та аналізу патернів дезінформації.

Механізм, що включає розробку і впровадження програм медіаграмотності та інформаційної безпеки є ключовим компонентом стратегії протидії дезінформації. Цей механізм передбачає розробку та реалізацію освітніх програм та ініціатив, спрямованих на підвищення рівня медіаграмотності та інформаційної компетентності серед населення. Програми медіаграмотності можуть охоплювати такі аспекти, як розпізнавання фейкових новин, критичне мислення щодо джерел інформації,

здатність аналізувати медійний контент з різних точок зору та розуміння впливу медіа на формування світогляду. Загальний ефект цього механізму полягає у зміцненні резистентності суспільства до дезінформації та забезпеченні його інформаційної безпеки, що є важливим для збереження стабільності в суспільстві.

Не менш важливим є механізм, який передбачає співпрацю державних структур з громадськими організаціями, приватним сектором та міжнародними партнерами для обміну досвідом і ресурсами. Основна мета цього механізму полягає в забезпеченні координації дій та використанні спільних зусиль у протидії дезінформації. Співпраця з громадськими організаціями дозволяє залучити до процесу широкі шари населення та експертну громадськість. Співпраця з приватним сектором передбачає залучення технологічних компаній, соціальних мереж та інших приватних підприємств до спільних ініціатив з розробки та впровадження інноваційних рішень для виявлення та протидії дезінформації в інтернеті та соціальних мережах. Співпраця з міжнародними партнерами включає обмін найкращими практиками, технологіями та експертними знаннями, що дозволяє використовувати глобальний підхід до проблеми дезінформації та розробляти спільні стратегії та механізми протидії.

Організація інформаційних кампаній та заходів з протидії дезінформації передбачає проведення систематичних та цілеспрямованих заходів, які можуть включати розміщення відповідних матеріалів у медіа, соціальних мережах та на вулицях міст, проведення публічних заходів, таких як семінари, тренінги, конференції, вебінари, а також розповсюдження інформаційних матеріалів через засоби масової інформації.

Метою створення інституційних механізмів координації дій між різними відомствами та органами влади є забезпечення спільного підходу до проблеми дезінформації. Це передбачає розробку спільних стратегій, планів дій та протоколів взаємодії, а також обмін інформацією та ресурсами. Для цього може бути здійснене створення спеціальних міжвідомчих комісій,

робочих груп або центрів, які відповідають за вироблення та впровадження стратегій протидії дезінформації.

Від розгляду факторів, принципів, методів та механізмів переходимо до аналізу ресурсів, необхідних для ефективної реалізації моделі інституціонального механізму вироблення державної політики у сфері протидії дезінформації, оскільки її успішна реалізація значною мірою залежить від достатнього фінансування, наявності кваліфікованого персоналу та технічних можливостей.

На рисунку нижче (рис. 2.5) наведено перелік основних ресурсів, необхідних для забезпечення функціонування інституціонального механізму вироблення державної політики у сфері протидії дезінформації. Фінансові ресурси забезпечують фінансування програм, досліджень, розробок та проведення заходів. Людські ресурси включають кваліфікований персонал, який здійснює аналіз, розробки та впровадження стратегій, а також фахівців, які забезпечують консультації та експертну підтримку. Технічні ресурси охоплюють доступ до сучасних технологій, програмного забезпечення, баз даних та інші технічні засоби, необхідні для ефективного виконання завдань з протидії дезінформації. Такий організований підхід до ресурсного забезпечення сприяє ефективній реалізації інституційної моделі та досягненню поставлених цілей у протидії дезінформацією.

Рис 2.4. Ресурси, необхідні для забезпечення функціонування інституціонального механізму вироблення державної політики у сфері протидії дезінформації.

Джерело: складено автором.

Для ефективної реалізації державної політики у сфері протидії дезінформації використовуються різні джерела фінансування, що використовуються в різних напрямах . Бюджетні асигнування, виділені з державного бюджету, спеціально призначені для програм та заходів з протидії дезінформації. Гранти та субсидії, які надаються як з державних, так і з міжнародних фондів, фінансово підтримують програми та ініціативи у цій сфері. Інвестиції в інформаційні технології сприяють розробці та впровадженню систем для протидії дезінформації. Освітні та тренінгові

програми фінансують проведення навчальних заходів для підвищення медіаграмотності громадян. Рекламні та інформаційні кампанії фінансуються з метою популяризації істинної інформації та усвідомлення загрози дезінформації. Дослідження та аналіз фінансуються для здійснення наукових досліджень щодо поширення дезінформації. Міжнародне співробітництво фінансує проекти та програми міжнародного рівня. Технічна інфраструктура фінансується для забезпечення захисту від дезінформації.

Фінансування для ефективної реалізації державної політики у сфері протидії дезінформації має ключове значення, але також важливо мати належний кадровий потенціал та технічні засоби. Експерти з аналітики та досліджень, які мають необхідні навички та знання для виявлення дезінформації, грають важливу роль у зборі, аналізі та інтерпретації інформації. Комунікаційні стратеги та медіа експерти відповідають за розробку та розповсюдження ефективних комунікаційних стратегій щодо дезінформації. Юристи та правозахисники забезпечують правову підтримку та надають консультації з правових аспектів боротьби з дезінформацією. Експерти з інформаційної безпеки вирішують технічні аспекти кіберзахисту та захисту від кібератак. Експерти з освіти та тренінгів розробляють та проводять освітні програми для підвищення медіаграмотності. Дослідники та науковці здійснюють наукові дослідження в області дезінформації. Громадські активісти та волонтери активно долучаються до протидії дезінформації. Державні службовці відповідають за розробку та впровадження державної політики з протидії дезінформації на різних рівнях.

Технічні ресурси, у свою чергу, охоплюють різноманітні інструменти та технології. Серед них, зокрема, системи моніторингу інформаційного простору, які є важливим інструментом для виявлення та аналізу дезінформаційних кампаній і тенденцій у медіа та соціальних мережах. Ці системи дозволяють вчасно виявляти та реагувати на поширення дезінформації, що є важливим етапом у боротьбі з нею. Також значну роль відіграють аналітичні інструменти та програми, які спрямовані на обробку та

аналіз великих обсягів даних для виявлення та розуміння змісту дезінформації. Ці інструменти допомагають експертам у виявленні шаблонів та тенденцій, що можуть вказувати на поширення шкідливої інформації. До інших важливих технічних ресурсів можна віднести інформаційно-аналітичні бази даних, що надають доступ до необхідної інформації для проведення наукових досліджень та аналізу дезінформації, а також інструменти для захисту від кібератак та забезпечення інформаційної безпеки, що є важливим аспектом у відверненні загроз кібербезпеки та захисту від кіберманіпуляцій.

Паралельно з матеріальними та людськими ресурсами для ефективної реалізації державної політики у сфері протидії дезінформації необхідна мобілізація всіх інститутів, що працюють у цій сфері, включаючи не лише державні структури, а й громадські організації, незалежні дослідницькі центри, міжнародних партнерів та приватний сектор.

Таблиця, наведена нижче (табл.2.3) демонструє взаємодію різних інститутів на стратегічному, тактичному та операційному рівнях державної політики протидії дезінформації.

Таблиця 2.3

Інституційна взаємодія на трьох рівнях концепції протидії дезінформації

Інститути	**Концепція протидії дезінформації**		
	Стратегічний рівень	**Тактичний рівень**	**Операційний рівень**
Державні органи та відомства	Формулювання стратегічних цілей та розроблення стратегічних ініціатив. Координація дій між різними органами та відомствами щодо впровадження цих ініціатив.	Розробка та реалізація програм та заходів. Забезпечення аналізу та оцінки поточних дезінформаційних загроз.	Впровадження заходів протидії дезінформаціїі. Моніторинг та аналіз інформаційного простору для виявлення дезінформаційних атак та реагування на них.
Наукові та дослідницькі установи	Дослідження та аналіз для стратегічної протидії дезінформації. Розробка концепцій протидії дезінформації. Експертна підтримка оцінки ефективності заходів протидії дезінформації.	Розроблення методик та інструментів для аналізу дезінформації та ідентифікації її джерел її поширення. Дослідження ефективності методів протидії дезінформації та розроблення рекомендацій щодо їх впровадження	Підтримка в реалізації ініціатив протидії дезінформації та надання наукових консультацій.

Продовження таблиці 2.3

Міжнародні організації та фонди	Участь у формулюванні стратегій та завдань на міжнародному рівні. Спільне розроблення та впровадження проектів та програм з підвищення інформаційної стійкості суспільства та інших ініціатив, спрямованих на протидію дезінформації.	Надання технічної та фінансової підтримки для впровадження заходів захисту. Спільна аналітична робота для виявлення поточних загроз та протидії їм.	Практична реалізація спільних проектів та програм протидії дезінформації. Співпраця з Центром протидії дезінформації щодо моніторингу та аналізу інформаційного простору та реалізації контрзаходів.
Приватний сектор	Участь у формулюванні загальних стратегічних підходів до протидії дезінформації. Участь у визначенні найбільш критичних загроз та розробці стратегій захисту.	Виявлення поточних загроз та вироблення тактичних підходів до їх протидії. Спільні ініціативи з розробки контрзаходів.	Розробка та використання інструментів виявлення дезінформації та впровадження технічних заходів захисту від неї. Практична реалізація контрзаходів.
Громадські організації та медіа	Участь у формулюванні загальних стратегій протидії дезінформації. Ініціативи з підвищення інформаційної стійкості суспільства.	Співпраця у розробці заходів захисту від поточних дезінформаційних загроз. Спільні аналітичні проекти з розробки контрзаходів.	Моніторинг інфопростору, фактчекінг та розміщення відповідного контенту на власних інтернет-ресурсах. Участь у спільних проектах та програмах з підвищення інформаційної стійкості суспільства.

Джерело: складено автором.

Як бачимо, у сфері протидії дезінформації діють різні зацікавлені сторони, і їх зусилля вимагають ефективної координації та взаємодії. Це необхідно для забезпечення ефективності та результативності заходів з протидії дезінформації, забезпечення взаємодоповнення різних ініціатив та ресурсів, а також зменшення можливих дублювань та прогалин у виявленні та протидії дезінформаційним загрозам. Тож є очевидною необхідність розробки чітких механізмів співпраці та координації дій між усіма зацікавленими сторонами.

На рис. 2.5 наведені механізми партнерської взаємодії між різними стейкхолдерами та ключові цінності, на яких ці механізми базуються.

Рис. 2.5. Базові цінності механізмів партнерської взаємодії

Джерело: складено автором

Механізм партнерських програм з громадянським суспільством полягає в укладанні партнерських угод або домовленостей між урядовими структурами та неприбутковими організаціями, громадськими об'єднаннями або іншими представниками громадянського суспільства. Цей механізм базується на взаємній користі для обох сторін. Урядові структури можуть отримати доступ до додаткових ресурсів, експертної підтримки та ширшого спектру знань і досвіду, які можуть надати такі організації. У свою чергу, громадянське суспільство має можливість впливати на вироблення державної

політики, співвизначати пріоритети та пропонувати інноваційні рішення. Партнерські програми також передбачають відкритий обмін інформацією та активну співпрацю між усіма учасниками. Це сприяє покращенню розуміння проблеми дезінформації, виробленню ефективних стратегій та забезпеченню взаємодоповнення ресурсів та ініціатив. Крім того, партнерські програми можуть бути адаптовані до змінних потреб та умов, що виникають у сфері протидії дезінформації. Це дозволяє оперативно реагувати на нові виклики та інноваційні можливості. Важливо зауважити, що учасники партнерських програм ділять відповідальність за досягнення спільних цілей у протидії дезінформації. Це вимагає взаємної довіри, відкритості та відповідальності за власні дії та результати.

Такий механізм партнерської взаємодії, як міжнародні проекти, відображає співпрацю між різними країнами, міжнародними організаціями та представниками громадянського суспільства у реалізації спільних ініціатив з протидії дезінформації. Ключові базові цінності цього механізму охоплюють залучення учасників з різних країн та регіонів для вирішення загальних проблем, пов'язаних з дезінформацією, що дозволяє обмінюватися досвідом, найкращими практиками та ресурсами між різними культурами і контекстами. Залучення урядового, громадського та приватного секторів для спільної реалізації заходів з протидії дезінформації що створює можливості для комбінування різних видів ресурсів, експертизи та підходів для досягнення більш ефективних результатів. Також міжнародні проекти дозволяють поєднувати зусилля учасників для створення синергії та взаємодоповнення різних ініціатив, що дозволяє зменшити дублювання зусиль, оптимізувати використання ресурсів та підвищити вплив на протидію дезінформації. Крім того, міжнародні проекти часто стимулюють розвиток та впровадження новаторських рішень і технологій для протидії дезінформації, що сприяє залученню нових ідей, досліджень та розробок у глобальному масштабі. Також міжнародні проекти є важливим механізмом партнерської

взаємодії у сфері протидії дезінформації, сприяючи об'єднанню зусиль для забезпечення інформаційної безпеки та захисту демократії.

У свою чергу, публічно-приватні партнерства (ППП) передбачають співпрацю між урядовими структурами та приватним сектором для спільного вирішення різних проблем. Основні риси публічно-приватних партнерств в контексті протидії дезінформації охоплюють: ресурсну ефективність (ППП дозволяють об'єднати ресурси та експертизу урядових і приватних суб'єктів для реалізації спільних заходів з протидії дезінформації, що може включати фінансові вкладення, технічну підтримку та доступ до новітніх технологій); швидкість реакції (ППП можуть допомогти в уникненні бюрократичних затримок та швидко реагувати на нові дезінформаційні загрози); технологічний розвиток (приватний сектор зазвичай має доступ до передових технологій та інновацій, які можуть бути використані для виявлення та протидії дезінформації); залучення експертів (партнерство з приватним сектором дозволяє залучити експертів з різних галузей, таких як технології, медіа та комунікації, для спільного вироблення та впровадження стратегій протидії дезінформації; гнучкість та інновації (ППП можуть бути більш гнучкими та інноваційними у порівнянні з традиційними урядовими програмами, що дозволяє більш швидко реагувати на змінні потреби та виклики, пов'язані з дезінформацією).

Механізм партнерської взаємодії, що передбачає консультації з експертами, полягає в залученні висококваліфікованих фахівців та спеціалістів із різних сфер для надання консультаційної підтримки у розробці та впровадженні стратегій протидії дезінформації. Основні характеристики цього механізму включають допомогу професіоналів, які можуть мати глибокі знання у сферах комунікацій, медіа, технологій, політики тощо. Консультанти можуть представляти як урядові органи, так і приватний сектор, академічні установи, громадські організації тощо. Експертиза залучених консультантів дозволяє провести об'єктивний аналіз ситуації та розробити індивідуалізовані рекомендації щодо заходів протидії. Вони

можуть допомогти визначити ключові проблеми, ідентифікувати потенційні загрози та розробити стратегії їх подолання. Крім того, участь у консультаціях з експертами сприяє обміну знань та навичками між різними зацікавленими сторонами.

Форуми та робочі групи також є важливим механізмом партнерської взаємодії у сфері протидії дезінформації. Передовсім, форуми та робочі групи надають можливість представникам різних інститутів – урядових органів, громадських організацій, приватного сектору, наукових установ тощо – зібратися разом для обговорення актуальних питань щодо протидії дезінформації. Такі зустрічі сприяють обміну кращими практиками, ідеями та досвідом. Учасники можуть висловлювати свої точки зору та взаємно навчатися одне від одного. Також під час форумів та засідань робочих груп можуть бути розглянуті конкретні питання та проблеми, що стосуються дезінформації. У результаті обговорень можуть бути розроблені спільні стратегії та прийняті конкретні рішення для подальшої реалізації.

Механізм звітності і взаємодії сприяє активній комунікації між усіма стейкхолдерами, які беруть участь у протидії дезінформації. Це може включати обмін інформацією, обговорення найбільш актуальних питань та спільне прийняття рішень. Учасники систематично оприлюднюють дані про проведені заходи, досягнуті результати, витрачені ресурси та інші важливі аспекти. Це сприяє створенню відкритого та прозорого середовища, де учасники вільно обмінюються інформацією та діляться результатами своєї діяльності, що сприяє підвищенню довіри між стейкхолдерами та покращує ефективність спільних зусиль. Механізм звітності і взаємодії також допомагає виявляти проблеми та труднощі у реалізації заходів протидії дезінформації та спільно шукати шляхи їх вирішення.

Узагальнюючи вищевикладене, можемо констатувати, що механізми партнерської взаємодії в моделі інституціонального механізму вироблення державної політики протидії дезінформації є важливим інструментом для досягнення ефективності та результативності діяльності у цій сфері. Вони

сприяють зближенню різних зацікавлених сторін, забезпечують координацію та співпрацю між ними, а також сприяють обміну інформацією та досвідом. Завдяки цим механізмам стейкхолдери можуть ефективніше протидіяти дезінформаційним загрозам, максимізувати використання ресурсів та досягати спільних цілей. Такий підхід сприяє створенню кооперативного середовища, де різні учасники здійснюють синергію своїх зусиль для ефективного протидії дезінформації та зміцнення інформаційної безпеки суспільства.

Партнерська взаємодія значною мірою впливає на процес прийняття рішень у сфері протидії дезінформації державними структурами. Цей процес охоплює розподіл відповідальності між усіма учасниками, включаючи різні групи інтересів, а також ухвалення рішень урядом та парламент. Результатом цього процесу є реалізація конкретних виконавчих заходів для протидії дезінформації. У другому розділу нами була розроблена концепція протидії дезінформації (рис. 2.1) , а наведена нижче таблиця (табл. 2.4) демонструє розподіл відповідальності між різними суб'єктами взаємодії в процесі реалізації цієї концепції.

Таблиця 2.4

Розподіл відповідальності між різними суб'єктами взаємодії в процесі реалізації виконавчих заходів з реалізації Концепції протидії дезінформації

Функція	Захід	Суб'єкти взаємодії	Виконавчі заходи
Стратегічний рівень			
Ідентифікація загроз	Аналіз тенденцій та потенційних джерел загроз	Наукові установи	Проведення наукових досліджень щодо тенденцій у сфері дезінформації та виявлення потенційних джерел загроз
		Державні органи	Моніторинг інформаційного простору для аналізу тенденцій та виявлення нових загроз
	Розробка методів оцінки впливу дезінформації	Наукові установи	Розробка науково обґрунтованих методик оцінки впливу дезінформації на суспільство та державу
		Державні органи	Використання цих методик для оцінки загроз і визначення стратегій протидії

Продовження таблиці 2.4

Вироблення стратегій	Визначення пріоритетів та ключових напрямків дій	Державні органи	Визначення стратегічних пріоритетів у протидії дезінформації та визначення ключових напрямків дій
		Наукові установи	Надання наукових рекомендацій для визначення пріоритетів та напрямків дій на основі аналізу даних
	Вироблення стратегії державної політики	Державні органи	Розробка та узгодження стратегій державної політики щодо протидії дезінформації
		Наукові установи	Надання наукових доказів та експертної підтримки для формулювання та реалізації стратегій
	Вироблення методик ефективного впровадження	Державні органи	Розробка методик та механізмів для ефективного впровадження стратегій протидії дезінформації
		Приватні айті-компанії	Розробка та впровадження інноваційних технологій для боротьби з дезінформацією в інтернеті та соціальних мережах.
Координація та співпраця	Встановлення механізмів міжсекторальної взаємодії	Державні органи	Управління та координація процесу встановлення механізмів міжсекторальної взаємодії з метою забезпечення спільної дії у протидії дезінформації
		Громадські організації	Активна участь у розробці та впровадженні механізмів міжсекторальної взаємодії для забезпечення включеності та представленості різних груп суспільства
		Наукові установи	Надання експертної підтримки та консультування у процесі встановлення механізмів міжсекторальної взаємодії на основі наукових досліджень та аналізу
	Співпраця з міжнародними партнерами	Державні органи	Укладання та виконання міжнародних угод та спільних ініціатив у сфері протидії дезінформації
		Міжнародні організації	Надання технічної та фінансової підтримки, обмін досвідом та найкращими практиками у сфері протидії дезінформації
		Громадські організації	Участь у міжнародних форумах та платформах для обміну досвідом та координації спільних дій з іншими країнами
	Координація дій між різними галузями	Державні органи	Координація та спрямування зусиль різних галузей у впровадженні стратегій протидії дезінформації
		Приватний сектор	Участь у реалізації спільних проектів та програм із протидії дезінформації на рівні підприємств та бізнес-структур
		Громадські організації	Мобілізація ресурсів громадянського суспільства та координація їх дій у протидії дезінформації
Моніторинг та аналіз ефективності	Постійний моніторинг та аналіз впливу	Державні органи	Здійснення постійного моніторингу дезінформаційних загроз та аналіз їхнього впливу на суспільство
		Наукові установи	Виконання наукових досліджень щодо виявлення та оцінки впливу дезінформа формації на суспільство та розробка рекомендацій щодо протидії цим загрозам
	Оцінка ефективності стратегій	Державні органи	Оцінка ефективності стратегій, що розроблені і впроваджені на державному рівні.
		Наукові установи	
		Міжнародні партнери	Участь в оцінці ефективності стратегій, що мають міжнародний аспект або впливають на міжнародну спільноту

Продовження таблиці 2.4

	Регулярні оціночні заходи	Наукові установи	Проведення регулярних оціночних заходів для оцінки ефективності стратегій на основі наукових досліджень та аналізу даних.
		Державні органи	Координація цього процесу та забезпечення зв'язку з іншими зацікавленими сторонами.
		Міжнародні партнери	Сприяння проведенню таких оціночних заходів на міжнародному рівні та обміну досвідом.
Тактичний рівень			
Захист від дезінформаційних інцидентів	Розробка та впровадження стратегій інформаційного контрзаходу	Державні органи	Організація та координація робіт з розробки та впровадження стратегій
		Приватні айті-компанії	Розробка та впровадження технічних рішень для захисту інформаційного простору
	Створення системи моніторингу та реагування	Державні органи	Організація та підтримка системи моніторингу
		Наукові установи	Проведення аналізу даних та розробка методів реагування
	Запровадження інструментів та технологій фільтрації	Приватні айті-компанії	Розробка та впровадження технологій фільтрації на платформах та в мережах
		Державні органи	Контроль за впровадженням та регуляція використання таких інструментів
Сприяння виявленню та аналізу дезінформаційних загроз	Залучення експертів та використання аналітичних інструментів для аналізу загроз	Наукові установи	Проведення аналізу даних та розробка методів протидії дезінформації
		Державні органи	Залучення експертів для аналізу конкретних ситуацій та розробки стратегій протидії
	Розробка стратегій контрдії та співпраця з медіа	Державні органи	Розробка стратегій та співпраця з медіа в області контрдії дезінформації
		Громадські організації	Проведення освітніх заходів та інших ініціатив для протидії дезінформації
	Розвиток інформаційної стійкості суспільства	Громадські організації	Організація та проведення освітніх та інформаційних заходів для підвищення стійкості суспільства
		Державні органи	Розробка програм та стратегій з цієї сфери
Впровадження контрдій	Розробка та впровадження стратегій контрдії дезінформації	Державні органи	Визначення конкретних заходів та стратегій національного рівня
		Громадські організації	Розробка та реалізація освітніх та інформаційних кампаній для боротьби з дезінформацією
	Співпраця з медіа та іншими сторонами для нейтралізації дезінформації	Державні органи	Встановлення зв'язків з журналістами та медіа для розповсюдження достовірної інформації
		Громадські організації	Організація спільних проєктів та ініціатив з медіа для збільшення обізнаності про дезінформацію
	Розвиток медіаграмотності та критичного мислення серед населення	Освітні установи	Включення курсів про медіаграмотність та критичне мислення в навчальні програми
		Громадські організації	Проведення тренінгів та семінарів для розвитку навичок критичного мислення серед населення
Постмоніторинг та аналіз результатів	Оцінка ефективності заходів та виявлення слабких місц	Державні органи	Проведення аналізу результатів імплементації стратегій та виявлення недоліків
		Приватні айті-компанії:	Забезпечення інструментів для моніторингу та відстеження ефективності заходів зі своєї сторони.
Операційний рівень			
Моніторинг інформаційного простору	Створення моніторингових груп	Наукові установи	Організація та проведення аналізу даних для виявлення дезінформаційних загроз
		Державні органи	Координація та підтримка роботи моніторингових груп

Продовження таблиці 2.4

	Забезпечення системи сповіщень та тривожних сигналів	Приватні айті-компанії:	Розробка та впровадження технічних рішень для швидкого реагування на тривожні сигнали
		Державні органи	Організація та підтримка системи сповіщень та тривожних сигналів на національному рівні
	Проведення аналізу попередніх дезінформаційних інцидентів	Наукові установи	Аналіз попередніх інцидентів та розробка рекомендацій для запобігання майбутнім
		Державні органи	Забезпечення доступу до необхідних даних та ресурсів для аналізу
	Залучення експертів для оцінки інформації	Наукові установи	Залучення фахівців для оцінки достовірності інформації та потенційного впливу
		Громадські організації	Залучення експертів для оцінки рівня впливу дезінформації на громадську думку
	Регулярне оновлення методів моніторингу	Приватні айті-компанії	Розробка та вдосконалення технологій для моніторингу дезінформації
		Наукові установи	Проведення наукових досліджень та апробація нових методів моніторингу.
Виявлення та ідентифікація дезінформа-ційних інцидентів	Аналіз джерел інформації	Державні органи	Забезпечення доступу до ресурсів та інструментів для аналізу джерел інформації
		Наукові установи	Проведення досліджень щодо джерел поширення дезінформації та їх впливу
	Використання алгоритмів для автоматичного виявлення дезінформаці	Приватні айті-компанії	Розробка та вдосконалення алгоритмів для автоматичного виявлення дезінформації на платформах та соціальних мережах
		Наукові установи	Дослідження нових методів та алгоритмів для ефективного виявлення шаблонів та ознак дезінформації
	Співпраця з експертами для підтвердження інцидентів	Державні органи	Встановлення механізмів співпраці з експертами для підтвердження дезінформаційних інцидентів та їх аналізу.
		Громадські організації	Мобілізація експертів для швидкого підтвердження або спростування дезінформації
	Підвищення кваліфікації персоналу	Державні органи	Організація навчань та семінарів для персоналу, що займається протидією дезінформації
		Приватні айті-компанії	Надання доступу до спеціалізованих курсів та онлайн-навчань для свого персоналу.
Вплив на дезінформа-ційний інцидент	Аналіз розповсюдження дезінформації	Наукові установи	Проведення досліджень щодо механізмів та шляхів розповсюдження дезінформації в мережі
		Приватні айті-компанії	Аналіз даних та моніторинг платформ для виявлення та вивчення патернів поширення дезінформації
	Розробка стратегій контрдії дезінформації	Державні органи	Відповідальні за розробку загальнодержавних стратегій та політики щодо протидії дезінформації
		Громадські організації	Розробка та впровадження стратегій контрдії на рівні громадськості та цивільного суспільства
	Залучення громадських організацій та засобів масової інформації	Громадські організації	Активна участь у впровадженні стратегій протидії дезінформації та розповсюдженні правдивої інформації
		Медіа	Співпраця з урядовими та неприбутковими організаціями для розповсюдження достовірної інформації та нейтралізації дезінформації.
	Співпраця з міжнародними інституціями	Державні органи	Участь у міжнародних ініціативах та обмін досвідом з іншими країнами у сфері протидії дезінформації
		Міжнародні організації	Співпраця з державами та міжнародними партнерами для розробки та впровадження спільних стратегій протидії дезінформації

Продовження таблиці 2.4

Постмоні-торинг та аналіз результатів	Оцінка ефективності застосованих стратегій	Державні органи	Моніторинг та аналіз результатів впроваджених стратегій та програм для оцінки їх ефективності
		Наукові установи	Дослідження ефективності різних методів протидії дезінформації та розробка рекомендацій для подальших заходів.
	Аналіз поширення дезінформаційних матеріалів	Приватні айті-компанії	Моніторинг та аналіз поширення дезінформаційних матеріалів на платформах та соціальних мережах
		Наукові установи	Дослідження впливу дезінформаційних матеріалів на громадську думку та розробка стратегій протидії їх поширенню.
	Виявлення слабких місць у системі протидії дезінформації	Державні органи	Аналіз системи протидії дезінформації для виявлення недоліків та слабких місць
		Приватні айті-компанії	Оцінка ефективності застосованих технологій та ідентифікація можливих вразливостей в системах фільтрації
	Формулювання рекомендацій для майбутніх заходів	Наукові установи	Аналіз досвіду та даних для розробки рекомендацій щодо подальших заходів у протидії дезінформації
		Державні органи	Використання рекомендацій наукових експертів для формулювання стратегій та політики протидії дезінформації

Джерело: складено автором.

Процес прийняття рішень у сфері протидії дезінформації відображає складні механізми взаємодії державних структур, наукових установ,міжнародних партнерів, громадських організацій та приватного сектора. При цьому, кожен інститут має свої унікальні функції та компетенції, які визначають його роль у реалізації Концепції протидії дезінформації на різних рівнях (табл. 2.5).

В контексті розподілу відповідальності також важливо відзначити роль парламенту в реалізації державної політики у сфері протидії дезінформації. Верховна Рада України як законодавчий орган має компетенцію створення нормативно-правової бази для протидії дезінформації. Вона розробляє та приймає законодавчі акти, регулюючи діяльність у сфері інформаційної безпеки та визначаючи правові механізми для протидії дезінформації.

Уряд, у свою чергу, відповідає за практичне впровадження рішень, прийнятих парламентом. Він координує роботу державних органів, забезпечуючи виконання законів та програм дій у сфері протидії дезінформації.

Таблиця 2.5

Задіяність суб'єктів впливу на різних рівнях реалізації концепції протидії дезінформації

ФУНКЦІЇ		ДЕРЖАВНІ СТРУКТУРИ	НАУКОВІ УСТАНОВИ	МІЖНАРОДНІ ПАРТНЕРИ	ГРОМАДСЬКІ ОРГАНІЗАЦІЇ	ПРИВАТНИЙ СЕКТОР
СТРАТЕГІЧНИЙ рівень	Визначення	висока	висока	середня	низька	низька
ТАКТИЧНИЙ рівень	Захист	висока	середня	висока	середня	висока
	Виявлення	висока	низька	середня	висока	висока
ОПЕРАЦІЙНИЙ рівень	Реагування	висока	низька	середня	висока	середня
	Відновлення	висока	середня	висока	середня	низька

Джерело: складено автором.

Наукові установи забезпечують інформаційну базу для розроблення стратегій та прийняття рішень у сфері протидії дезінформації. Вони проводять дослідження, аналізують тенденції та ідентифікують дезінформаційні загрози, що допомагає у формулюванні науково обґрунтованих підходів до протидії цьому явищу.

Міжнародні партнери відіграють важливу роль у формуванні міжнародного виміру стратегій протидії дезінформації. Співпраця з міжнародними організаціями дозволяє обмінюватися досвідом та ресурсами, що веде до спільних ініціатив та реалізації спільних проектів у цій сфері.

Громадські організації та приватний сектор також активно залучаються до протидії дезінформації. Вони можуть організовувати інформаційні кампанії, розробляти та впроваджувати технологічні рішення для в забезпечення інформаційної безпеки, а також здійснювати моніторинг та аналіз інформаційного простору з метою виявлення дезінформаційних інцидентів та вжиття контзаходів.

Кожен із цих суб'єктів має свої можливості, ресурси та компетенції, які вони використовують на різних етапах та рівнях реалізації концепції протидії дезінформації. Це створює комплексний підхід до протидії дезінформації та забезпечує успішну реалізацію стратегій у цій сфері.

Розглянувши розподіл відповідальності між суб’єктами впливу в процесі реалізації концепції протидії дезінформації, важливо також звернутися до аспекту оцінки результатів цієї діяльності. Така оцінка дозволяє зрозуміти, наскільки ефективними є загальна стратегія і ті виконавчі заходи, які реалізують учасники процесу кожен на своєму рівні..

Оцінка результатів у сфері протидії дезінформації може здійснюватися різними органами, кожен з яких виконує визначені функції та має свої компетенції (рис. 2.6).

Рис. 2.6. Оцінка ефективності заходів у сфері протидії дезінформації

Джерело: складено автором.

Аналітичні підрозділи державних структур відіграють ключову роль у цьому процесі. Вони збирають, аналізують та інтерпретують дані щодо ефективності застосованих стратегій та заходів у боротьбі з дезінформацією.

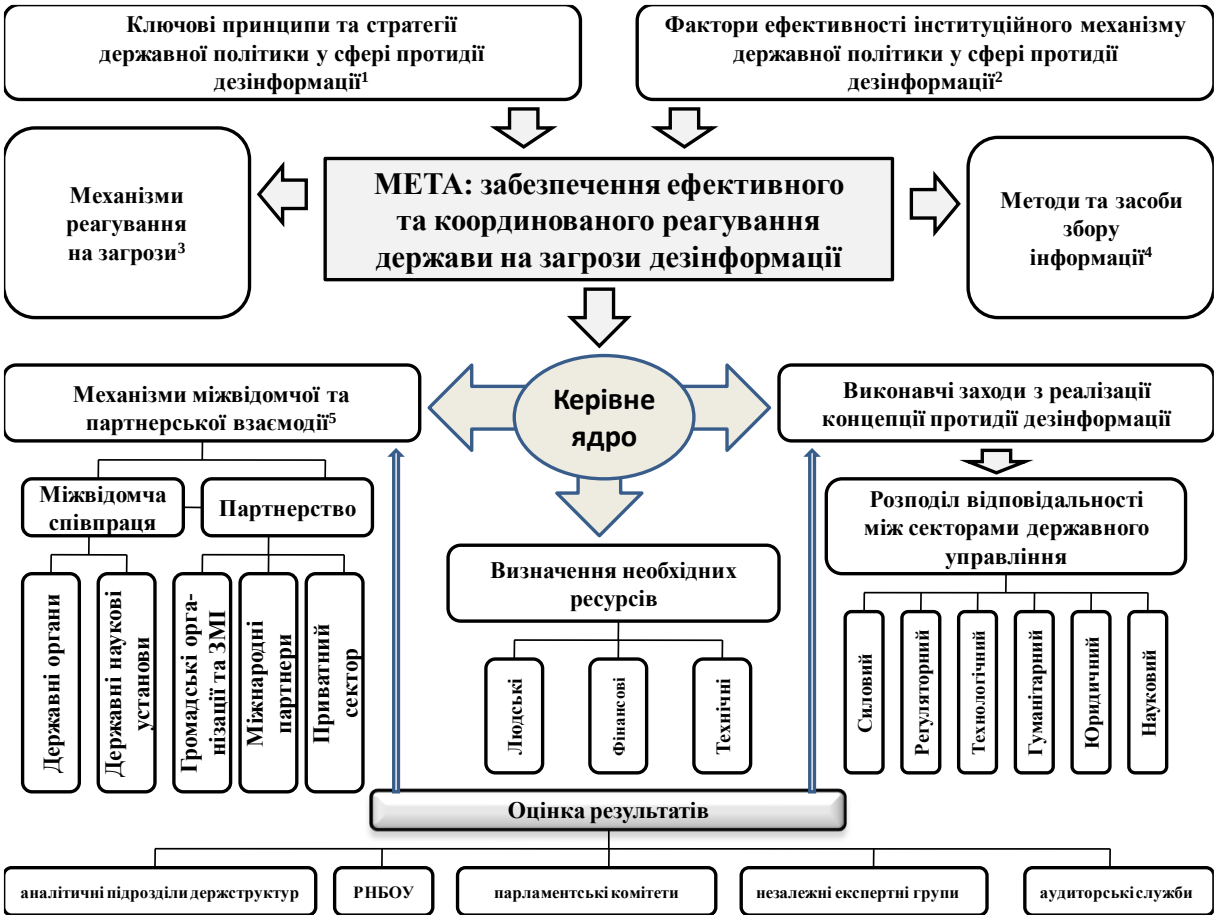
Крім того, для об'єктивного оцінювання результатів. до цього процесу можна залучати комісії та ради з питань інформаційної безпеки, які спеціалізуються на координації дій у сфері інформаційної безпеки та незалежні експертні групи. Парламентські комітети та аудиторські служби можуть також проводити аналіз ефективності заходів у сфері протидії дезінформації. Їхні оцінки і рекомендації можуть відігравати важливу роль у формуванні державної політики у цій сфері.

Розглянувши всі складові державної політики у сфері протидії дезінформації, ми можемо запропонувати інституційну модель вироблення механізмів державної політики у цій сфері. Запропонована модель подана на рисунку 2.7.

Отже, взаємозв'язки між складовими елементами інституційного механізму вироблення державної політики у сфері протидії дезінформації розглядаються нами як динамічні процеси впливу та взаємодії.

Ключові принципи та стратегії державної політики у сфері протидії дезінформації, а також основні фактори, що впливають на ефективність інституційного механізму цієї політики, визначають загальну мету.

Мета визначає стратегічний вибір механізмів протидії дезінформації та підходи до використання методів і засобів збору та аналізу інформації.



Примітка:

[1]ефективні заходи захисту; ефективний моніторинг і аналіз; швидка реакція та оперативні контрдії; принцип доказової основи; співпраця і координація дій; прозорість та відкритість; задіяність різних зацікавлених сторін; активна комунікація з цільовими групами; оцінювання результатів

[2]політичний контекст; інформаційна культура; технологічний розвиток; роль громадянського суспільства; вплив медіа; міжнародна співпраця; фінансові ресурси; стратегічне партнерство

[3]моніторинг медіа та соціальних мереж; аналітичні інструменти; експертна оцінка; публічні кампанії; спеціальні комісії та агентства; міжнародне співробітництво; законодавчі заходи

[4]стратегічне планування; аналітичні дослідження; нормативне регулювання; інформаційний моніторинг; освітні програми; партнерська співпраця; інформаційна мобілізація; координаційні заходи

[5]міжвідомча співпраця: робочі групи і комітети, регулярні наради, обмін інформацією, спільні програми і проекти, кризова координація, розробка спільних стратегій; партнерська взаємодія: партнерські програми з громадянським суспільством, міжнародні проекти, публічно-приватні партнерства, консультації з експертами, форуми та робочі групи, звітність та взаємодія.

Рис. 2.7. Модель інституціонального механізму вироблення державної політики у сфері протидії дезінформації

Джерело: складено автором.

Крім того, мета спрямовує дії керівного ядра, яке виконує три ключові функції: 1) забезпечує ефективність виконавчих заходів з реалізації концепції протидії дезінформації з розподілом відповідальності між усіма секторами державного управління; 2) визначає фінансові, людські і технічні ресурси,

необхідні для ефективної протидії дезінформації; 3) забезпечує координацію та узгодження дій між суб'єктами взаємодії у сфері протидії дезінформації, що охоплює не лише міжвідомчу співпрацю державних структур, а й партнерські програми з громадянським суспільством, публічно-приватні партнерства та міжнародні проекти. Така взаємодія сприяє обміну досвідом, ресурсами та інформацією, що сприяє підвищенню ефективності та швидкості реагування на дезінформаційні загрози.

Завершальним етапом у цьому процесі є оцінка результатів виконавчих заходів та взаємодії всіх учасників процесу. Таке оцінювання можуть проводити, наприклад, аналітичні підрозділи держструктур, Рада національної безпеки і оборони України, парламентські комітети, незалежні експертні групи та аудиторські служби. Ця функція дозволяє зрозуміти ефективність застосованих стратегій та механізмів протидії дезінформації та вносити відповідні корективи у подальшу діяльність.

Висновки до розділу 2.

У другому розділі розглянуто основні підходи до вироблення державної політики у сфері протидії дезінформації в США та Європейському Союзі, а також можливість їх адаптації до умов України. Встановлено, що в країнах з розвинутою демократією державна політика базується на партнерстві між урядом, громадськістю та приватним сектором. Це партнерство проявляється у створенні механізмів саморегулювання для медіа-організацій, активній взаємодії з фактчекінковими організаціями, сприянні розвитку медійної грамотності серед населення, підтримці наукових досліджень у галузі протидії дезінформації та розробці нових технологій для виявлення недостовірної і маніпулятивної інформації та запобігання її поширенню.

Також визначено сутність поняття «інформаційна війна» як основного джерела загрози інформаційній безпеці України. Досліджено еволюцію підходів до понять «інформаційна війна» та «спеціальні

інформаційні операції» у нормативно-правових актах держави. Встановлено, що термін «інформаційна війна» охоплює більш широкий спектр діяльності, пов’язаної з використанням інформаційних засобів і методів для досягнення певної стратегічної мети, ніж термін «спеціальні інформаційні операції». Запропоновано термінологічне визначення поняття «інформаційна війна» як протяжного в часі процесу використання інформаційних технологій та медіа-ресурсів з метою впливу на інформаційну безпеку та соціальну стабільність країни, проти якої така війна ведеться. Рекомендовано використовувати термін «інформаційна війна» в нормативно-правових актах держави для опису загального контексту в інформаційному просторі, а термін «спеціальні інформаційні операції» – для конкретних дій, обмежених у часі і цілях.

Також встановлено чинники (фактори), що впливають на збільшення швидкості поширення дезінформації комунікативними каналами у публічній сфері, а саме: здатність емоційно зарядженого й контраверсійного контенту активно розповсюджуватися подібно до поширення вірусу в біологічній системі; вплив когнітивного спотворення, прагнення підтвердження власних переконань, емоційна залежність психіки людини від соціальних мереж; таргетування (алгоритми рекомендацій) соціальних мереж, що впливають на відображення певного контенту в новинній стрічці користувачів; використання анонімних (псевдоанонімних) фейкових акаунтів та ботів.

Запропоновано алгоритм протидії дезінформації в умовах розвитку цифрових трансформацій, який складається з п’яти основних етапів:

1. Визначення потенційних загроз та вироблення стратегії державної політики протидії дезінформації.

2. Захист від поточних загроз шляхом впровадження механізмів фільтрації та перевірки інформації, підвищення інформаційної грамотності та вдосконалення заходів захисту від кібератак

3. Виявлення дезінформаційних інцидентів в режимі реального часу.

4. Оперативне та ефективне реагування на такі інциденти.

5. Здійснення заходів з відновлення стабільності та оцінка результатів.

Впровадження такого алгоритму протидії дезінформації в державну політику дасть змогу ефективно протистояти дезінформаційним загрозам та сприятиме підвищенню рівня інформаційної безпеки держави.

Розроблено модель інституціонального механізму вироблення державної політики у сфері протидії дезінформації на стратегічному, тактичному та операційному рівнях для забезпечення ефективного та координованого реагування підрозділів органів влади на маніпулятивні та фальсифікативні загрози, що базується на взаємодії суб'єктів публічного управління (стратегічних, регуляторних, комунікативних, гуманітарних; юридичних, наукових) у процесі реалізації комплексу організаційно-функціональних заходів згідно зон їх відповідальності на основі:

– факторів (політичний контекст; інформаційна культура; технологічний розвиток; роль громадянського суспільства; вплив медіа; міжнародна співпраця; фінансові ресурси; стратегічне партнерство);

– стратегій (реалізації заходів захисту; здійснення моніторингу, аналізу та оцінювання ризиків; реагування та здійснення контрдій);

– принципів (комунікативності, захищеності, координованості, доказовості, прозорості, відкритості, задіяності та адаптивності);

– методів/засобів збору та поширення контенту (моніторингу медіа та соціальних мереж; аналітичних інструментів; експертної оцінки; публічних кампаній; спеціальних комісій та агентств; міжнародного співробітництва; законодавчих ініціатив);

– інструментів реагування на загрози (стратегічне планування; аналітичні дослідження; нормативне регулювання; інформаційний моніторинг; освітні програми; партнерська співпраця; інформаційна мобілізація; координаційні заходи);

– співпраці (формування спеціалізованих робочих груп та комітетів; проведення регулярних нарад; здійснення обміну інформацією; створення

спільних програм і проєктів; здійснення кризової координації; розробка спільних стратегій) та партнерської взаємодії (залучення партнерських програм з громадянським суспільством та міжнародних проєктів; застосування публічно-приватного партнерства; проведення консультацій з експертами; організація форумів та робочих група); ресурсів (фінансових, людських і технічних).

Запропоновано шляхи розвитку інституціонального механізму вироблення державної політики у сфері протидії дезінформації, зокрема через:

– поліпшення координації дій між Центром протидії дезінформації при РНБО України і профільними органами державної влади та іншими зацікавленими суб'єктами публічного управління;

– оптимізацію використання фінансових, людських і технічних ресурсів із залученням партнерської взаємодії з громадськими організаціями, приватним сектором та міжнародними партнерами для спільної реалізації проектів і програм;

– оновлення нормативно-правової бази з урахуванням сучасних викликів, загроз, ризиків та впливу цифрових технологій у сфері протидії дезінформації;

– забезпечення широкого доступу громадськості до достовірної інформації та підвищення інформаційної грамотності населення.

Основні результати розділу 2 опубліковано в наукових працях автора: *[49, 51, 53, 54, 55, 85]*.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

3.1. Аналіз плану заходів Стратегії інформаційної безпеки в контексті протидії дезінформації та рекомендації щодо його вдосконалення

Метою цього розділу є проведення аналізу Плану заходів уряду з реалізації Стратегії інформаційної безпеки на період до 2025 року [184] з фокусом на аспектах протидії дезінформації.

Зосереджуючи увагу на позитивних аспектах Плану заходів, необхідно відзначити, що документ охоплює різні напрями протидії дезінформації, включаючи розвиток медійної грамотності населення, співпрацю з міжнародними організаціями та налагодження успішної взаємодії з громадянським суспільством. Зокрема, у розділі, присвяченому підвищенню рівня медіакультури та медіаграмотності, чітко і фахово викладені заплановані заходи, які належним чином відображають важливість розвитку критичного мислення та навичок аналізу інформації. Проте, багато заходів сформульовано в загальному форматі, що ускладнює практичне застосування та контроль за їх виконанням.

Так, першим завданням, визначеним у Стратегії, є «створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам». Є очевидним, що створення такої системи – це складний і тривалий процес, що передбачає ряд етапів, включаючи розробку та впровадження нових технологій, вдосконалення законодавства, підготовку кадрів та інше, проте для його виконання урядом заплановано лише заходи з аналізу даних, одержаних в результаті медіа-моніторингу, що явно не відповідає масштабу завдання.

Також виникає обґрунтована дискусія стосовно підходу, за якого завдання з моніторингу інформаційного простору з метою виявлення дезінформації покладаються одночасно на Міністерство культури та інформаційної політики, Центр протидії дезінформації при РНБО, інформаційне агентство «Укрінформ», Службу безпеки України, Службу зовнішньої розвідки, Міністерство оборони, Міністерство внутрішніх справ, Міністерство зовнішніх справ та Національну раду з питань телебачення і радіомовлення зі складанням відповідних звітів.

Очевидно, передбачається, що певні теми можуть прямо стосуватися діяльності конкретних організацій. Однак, у такому разі залишається нез'ясованим, як саме різні структури, відповідальні за моніторинг інформаційного простору, будуть визначати "свою" та "не свою" дезінформацію, яку вони фіксуватимуть або ігноруватимуть. Наприклад, невідомо, в чому конкретно буде полягати відмінність між моніторингом інформаційного простору, який здійснюватиме Міністерство культури, і моніторингом, який буде проводити Центр протидії дезінформації чи «Укрінформ». Здається, що ці структури виконуватимуть аналогічну роботу. На наш погляд, було б доцільніше зосередити функції з моніторингу дезінформації в одному спеціалізованому центрі, обладнаному сучасною технікоюта новітнім програмним забезпеченням, який має висококваліфікованих фахівців з відповідною підготовкою у галузі виявлення дезінформації. Це дозволить оптимізувати використання ресурсів та постійно вдосконалювати технології та методики виявлення дезінформації, що є важливим аспектом у швидкозмінному інформаційному середовищі.

По-друге, хоча підготовка звітів за результатами моніторингу є важливою складовою процесу протидії дезінформації, сама їх наявність не є свідченням того, що захід був успішно виконаний. Наприклад, звіти можуть бути недостатньо деталізованими, неповними або необ'єктивними, що може спотворювати справжню картину результатів моніторингу. Тому

було б корисно мати більш детальні та конкретні індикатори успішності. Наприклад, можна було б виміряти кількість виявлених загроз та їх серйозність, кількість виявлених шаблонів і трендів, кількість розроблених стратегій та рекомендацій щодо запобігання загрозам, часовий вимір у годинах чи хвилинах від розпізнавання загроз до розробки та впровадження заходів з їх запобігання та багато іншого. Крім того, важливо зазначити, що виконання запропонованих заходів потребує залучення значних коштів та інших матеріальних засобів, й основним проблемним питанням може стати недостатнє фінансування, однак цей фактор зовсім не враховується.

Переходячи до другого завдання, визначеного в Стратегії інформаційної безпеки, зазначимо, що його реалізація передбачає виконання заходів, спрямованих на протидію поширенню дезінформації та деструктивної пропаганди, пов’язаної з європейською та євроатлантичною інтеграцією України. Проте аналіз запланованих урядом заходів не спонукає до оптимізму. Перш за все, звертають на себе увагу загальні формулювання, використані для опису заходів, які мають завершувати досягнення цілей: «забезпечення співпраці із закордонними партнерами», «сприяння реалізації та захисту національним інтересам», «протидія дезінформації та спеціальним інформаційним операціям», «підготовка та внесення пропозицій», «підготовка та поширення інформаційних матеріалів», «організація та проведення публічних заходів», тоді як важливо зосередитися на конкретних вимірюваних діях та результативності замість загальних фраз, які можуть трактуватися по-різному. Планування заходів передбачає моніторинг та оцінку їх ефективності, але це неможливо здійснити, якщо в якості індикаторів виконання поставлених завдань вказуються такі загальні показники, як «здійснено виявлення та протидію зовнішнім інформаційним загрозам» та наводиться часова рамка дедлайну: «протягом 2023—2025 років».

Ускладнення об'єктивної оцінки виконання ряду заходів також виникає через включення широкого кола завдань у їхню структуру без конкретизації очікуваних результатів. Наприклад, запланований захід з «протидії дезінформації та спеціальним інформаційним операціям, спрямованим на підрив конституційного ладу, суверенітету і територіальної цілісності України, а також дискредитацію євроатлантичного та європейського стратегічного курсу держави» передбачає участь широкого кола виконавців, включаючи МКІП, МЗС, МВС, Міноборони, Держспецзв'язок, СБУ, ЦПД РНБОУ, а індикатор виконання сформульовано як «проведено заходи з протидії дезінформації та спеціальним інформаційним операціям».

Стосовно наступного заходу, який передбачає налагодження співпраці із закордонними партнерами, виникає сумнів щодо коректності самої постановки цього питання, оскільки таке взаємодія вже існує. Ймовірно, мається на увазі не створення співпраці з нуля, а розвиток і поглиблення вже встановлених зв'язків та пошук нових можливостей для співпраці. Це свідчить про несистемний або поверхневий підхід до планування заходів без чіткої спрямованості на досягнення вагомих результатів у зазначеному напрямі.

Наступний захід, який був обраний для аналізу, полягає у підготовці та внесенні пропозицій щодо застосування персональних санкцій до фізичних та юридичних осіб, що підтримали збройну агресію Російської Федерації проти України та поширюють дезінформацію. Застосування санкцій щодо таких осіб справді може сприяти зменшенню їх впливу на інформаційне середовище та здатності впливати на громадську думку. Проте, недостатність інформації про процедуру визначення осіб, що підпадають під санкції, може породжувати недовіру до цього процесу та спричиняти ситуації, коли окремі особи, фактично підпадаючи під санкції, уникають їх застосування через недостатню прозорість відповідних механізмів. Крім того, відсутність чітких критеріїв для визначення осіб, що

підпадають під санкції, може призвести до суб'єктивних оцінок та викликати спірність щодо цього питання.

Ще одним важливим аспектом протидії дезінформації є розвиток спроможностей складових сил оборони України у протидії загрозам в інформаційному просторі. Можна логічно припустити, що для досягнення зазначеної стратегічної цілі необхідне впровадження інноваційних технологій та методик, які забезпечать ефективну протидію дезінформаційній агресії, яка в цифрову епоху «вийшла на новий рівень» [188]. З огляду на це, виникає потреба в спеціальному виокремленні в силах оборони аналітичної складової і побудови цілісної підсистеми стратегічного аналізу, заснованої на використанні сучасних аналітичних технологій» [189]. Але про такий крок в Плані заходів не йдеться. Крім того, при визначенні функцій новостворених підрозділів акцент зроблено лише на зовнішніх чинниках і не враховується ширший спектр потенційних загроз, що можуть мати внутрішнє походження та суттєво впливати на стан інформаційної безпеки у воєнній сфері, сприяючи розповсюдженню антиукраїнського інформаційного контенту [109, С. 15].

Ще одним із заходів, спрямованих на розвиток спроможностей складових сил оборони у протидії загрозам в інформаційному просторі, є забезпечення військових медіа необхідними ресурсами. Слід зазначити, що протягом останніх кількох років у системі комунікацій Міністерства оборони України відбувалися значні трансформаційні процеси, що призвели до створення нових інформаційних засобів. Зокрема, у грудні 2018 року було засноване інформаційне агентство «АрміяINFORM», яке замінило собою ліквідовані друковані видання [130]. Також активізовано діяльність «Військового телебачення України» [129] та військового радіо «Армія FM» [128] як структурних підрозділів Центральної телерадіостудії МОУ, та YouTube-каналу «Бриз». Також було засновано науково-практичний та науково-теоретичний журнал «Наука і Оборона», хоча на період проведення нашого дослідження він не функціонував [127].

Важливо відзначити велику значущість військових корпоративних видань для цільової аудиторії. Згідно з результатами анкетування, близько 40% військовослужбовців використовують військові медіа як основне джерело інформації (це найвищий показник, за винятком специфічної внутрішньої комунікації, яка відіграє провідну роль у задоволенні інформаційних потреб особового складу. При цьому найчастіше в якості головних джерел інформації респонденти називали офіційний сайт МОУ (57,3%) та сторінку власної військової частини у соцмережах (48,3 %). Також високою популярністю серед військових користуються радіо «Армія FM» (39,3 %) та сайт Збройних сил України (37,1 %) [165]. Ці дані в цілому корелюються з результатами, отриманими в ході загальнонаціональних досліджень, що проводилися Київським міжнародним інститутом соціології, Фондом «Демократичні ініціативи імені Ілька Кучеріва» та соціологічною службою Центру Разумкова [165].

Отже, на основі наведених даних можна зробити висновок, що військові ЗМІ виконують важливу комунікаційну функцію, сприяючи підвищенню обізнаності військовослужбовців та їх родин щодо військових питань, а також задовольняючи гостру потребу широкої громадськості в достовірній інформації з надійних джерел у період війни. Однак, для подальшого розвитку військових медіа необхідне виділення додаткових ресурсів, про що в Плані уряду не згадується.

Переходячи до розгляду наступного пакету запланованих заходів, зазначимо, що наша особлива увага була зосереджена на пункті, що стосується «посилення відповідальності за поширення недостовірної інформації (дезінформації)». Відповідно до Плану заходів МКІП спільно з СБУ мають розробити пропозиції, спрямовані на посилення відповідальності за поширення недостовірної інформації (дезінформації) стосовно намірів та дій держави-агресора. Зауважимо, що в умовах війни проблематика протидії шкідливим формам впливу на громадську думку є надзвичайно актуальною, ознак у сформульованому урядом завданні

відбулося змішування понять пропаганди і дезінформації, які хоча й схожі за метою, але відрізняються за формою. Зокрема, пропаганда передбачає використання різних форм комунікації і може містити як правдиву, так і неправдиву інформацію з метою зміни думки або поведінки людей. Водночас, дезінформація завжди передбачає поширення неправдивої інформації, замаскованої під правдиву, з метою формування у об'єкта впливу викривленого сприйняття дійсності. Отже, можемо зробити висновок, що пропаганда і дезінформація переслідують спільну мету – вплив на громадську думку, але вони відрізняються за формою такого впливу. Змішування схожих, але не взаємозамінних понять може створювати недостатньо ясність щодо того, що саме потрібно контролювати та регулювати.

Крім того, є очевидним некоректне ототожнення термінів «недостовірна інформація» і «дезінформація», які хоч і пов'язані між собою, але не є ідентичними. Це має важливе значення, оскільки доведення факту поширення будь-якої інформації вимагає певної кількості доказів і аналізу контексту.

Дезінформація завжди передбачає навмисну діяльність, тому при встановленні винуватості необхідно довести умисел особи припоширенні неправдивої інформації. Для цього необхідно встановити конкретні факти, що свідчать про те, що особа усвідомлювала неправдивий характер інформації, яку вона поширила, та можливі наслідки своїх дій.

Недостовірна інформація так само може бути використана з різною метою, включаючи політичні маніпуляції та спроби вплинути на громадську думк. Однак при вставленні факту поширення такої інформації не потрібно доводити наявність умислу, оскільки недостовірність може бути несвідомою.

Іншими словами, дезінформація є однією з форм недостовірної інформації, проте не всі випадки недостовірної інформації можна віднести до дезінформації. Ці два поняття взаємопов'язані як частина і ціле.

Важливо враховувати, що в Україні досі немає офіційного визначення терміну «дезінформація» через його специфічний зміст та відсутність узгодженого підходу між усіма галузями та органами влади щодо того, що саме вважається дезінформацією та як її визначати. Тому, з метою уніфікації термінології та забезпечення посилення відповідальності за поширення шкідливого контенту, ми пропонуємо використовувати ширший термін "недостовірна інформація".

У контексті інших вагомих заходів протидії дезінформації важливо відзначити ефективне науково-аналітичне та експертне супроводження цього процесу, що дозволяє раціонально визначати пріоритети, розробляти теоретично обґрунтовані стратегії та тактику протидії інформаційній агресії, а також оцінювати ефективність вжитих заходів. Проте індикатор виконання заходу, зазначений як «підготовлені інформаційні матеріали» не відображає всіх аспектів роботи, необхідних для забезпечення наукового супроводження вироблення державної політики у сфері протидії дезінформації. Для більш конкретної оцінки успішності можуть бути використані інші показники, такі як, проведені наукові дослідження та наукові експертизи, опубліковані наукові статті та інших наукові матеріали із зазначеної тематики, кількість проведених заходів та інші ревалентні параметри.

Отже, підсумовуючи результати проведеного аналізу, зазначимо, що для ефективної взаємодії у сфері протидії дезінформації передовсім необхідно чітко розмежувати функції Центру протидії дезінформації при Раді національної безпеки і оборони України (ЦПД РНБОУ) та Міністерства культури та інформаційної політики України (МКІП), оскільки, хоча ці два відомства спільно спрямовані на забезпечення інформаційної безпеки та захисту суспільства від дезінформації, але мають різні функції і обов'язки.

ЦПД РНБОУ відповідає за моніторинг, аналіз та реагування на стратегічні гібридні загрози та поточні дезінформаційні інциденти, а також забезпечує стратегічну координацію урядових структур у сфері запобігання

та протидії дезінформації. Натомість, МКІП відповідає за формування та реалізацію державної політики в інформаційній сфері, що включає розвиток медійного простору, підтримку культурних ініціатив, інформаційну безпеку тощо.

Виходячи з цього, ЦПД РНБОУ швидко реагує на виявлені загрози та спрямовує ресурси на забезпечення інформаційної безпеки, тоді як МКІП займається переважно регулюванням медіа та інформаційного простору, встановленням стандартів якості та обмежень для медійних засобів. Отже, хоча обидва організми працюють у сфері інформаційної безпеки, їх функції мають бути чітко відмежовані і не повинні дублюватися чи пересікатися.

Крім того, важливим кроком для забезпечення ефективної співпраці та координації між різними організаціями, установами або відомствами є розроблення протоколів обміну інформацією та узгодження спільних дій є. Ось чому це важливо:

– через розроблення протоколів обміну інформацією можна уникнути дублювання робіт та марнування ресурсів на однакові завдання; встановлення чітких правил обміну інформацією дозволить оптимізувати використання людських, фінансових та матеріальних ресурсів;

– правильно налаштовані протоколи обміну інформацією дозволять швидко реагувати на надзвичайні та кризові ситуації або загрози;

– встановлення протоколів узгодження спільних дій дозволить різним організаціям або відомствам працювати разом в одному напрямку, діяти узгоджено та вирішувати спільні завдання. що забезпечить більшу ефективність і результативність діяльності;

– якщо у всіх учасників процесу буде чітке розуміння їх ролей, обов'язків та очікувань, це сприятиме підвищенню довіри між ними, і як наслідок – більш ефективній та продуктивній співпраці.

Також у сучасному цифровому середовищі критично важливим є забезпечення державних структур сучасними технологіями та аналітичними інструментами, що дозволяють швидко виявляти та аналізувати інформацію

про дезінформаційні загрози. інциденти. Зокрема, сучасні технології аналізу даних (наприклад, штучний інтелект та машинне навчання) дозволяють обробляти великі обсяги інформації та швидко виділяти патерни та тренди, що можуть вказувати на поширення дезінформації. Також сучасні технології дозволяють автоматизувати процес моніторингу соціальних медіа та інших онлайн-платформ для виявлення дезінформації та негативних впливів. Крім того, аналітичні інструменти дозволяють створювати прогностичні моделі для передбачення можливих сценаріїв розвитку ситуацій та виявлення потенційних джерел дезінформації. Нарешті, сучасні технології сприяють поліпшенню координації та співпраці між різними державними структурами, організаціями та міжнародними партнерами у сфері протидії дезінформації.

Одним з ключових елементів успішної стратегії протидії дезінформації є партнерська взаємодія з активним залученням громадянського суспільства, академічної спільноти та приватного сектора. З огляду на те, що ці інституції представляють різноманітні джерела інформації та експертного аналізу, їх залучення розширює спектр джерел, з яких можна отримати об'єктивну та надійну інформацію. Крім того, академічна спільнота та приватний сектор мають доступ до спеціалізованого експертного знання і аналітичних інструментів, які можуть допомогти виявляти та аналізувати дезінформацію. Також громадянське суспільство має потенціал для підвищення обізнаності людей щодо розпізнавання та усвідомлення дезінформації. Активне залучення громадян до процесів протидії може сприяти створенню інформованого та критичного суспільства. Крім іншого, приватний сектор, зокрема соціальні мережі та інші технологічні компанії, мають можливості для моніторингу та реагування на дезінформацію в онлайн-середовищі. Їхні технічні ресурси та експертність також можуть бути використані для протидії поширенню патогенної інформації. Також важливо зауважити, що залучення громадянського суспільства та приватного сектора до процесів протидії дезінформації сприяє підвищенню довіри громадян до заходів, які приймаються урядом та іншими органами влади.

Нарешті, для ефективної протидії дезінформації критично важливим є впровадження ефективних механізмів контролю та оцінки. Це не лише допомагає адаптувати стратегії, виявляти успішні практики та оптимізувати використання ресурсів, а й сприяє постійному вдосконаленню загального алгоритму дій. Зокрема, механізми контролю та оцінки дозволяють визначити результативність вжитих заходів протидії дезінформації, ідентифікувати успішні підходи та стратегії, а також виявляти прогалини і слабкі місця, що потребують додаткових заходів.

Крім того, зважаючи на постійну еволюцію методів та технологій дезінформації, механізми контролю та оцінки дозволяють оперативно виявляти нові потенційні загрози та адаптувати стратегії протидії.

Поміж іншого, оцінка ефективності допомагає визначити найбільш ефективні способи використання ресурсів у протидії дезінформації. Це дозволяє ефективніше розподіляти бюджетні кошти та інші ресурси для досягнення максимального впливу Крім того, через оцінку дієвості заходів з протидії дезінформації можна виявити кращі практики та передавати їх іншим учасникам, що сприяє вдосконаленню комунікації та координації між різними органами та відомствами.

Підсумовуючи, можемо констатувати, що необхідним є розроблення удосконаленого плану протидії дезінформації з врахуванням останніх трендів, технологій та методів дезінформації, що дозволить ідентифікувати найбільш ефективні підходи та оптимізувати використання ресурсів, чітко визначити ролі та відповідальність різних учасників у протидії дезінформації, а також наблизитися до максимально інформованого та відповідального суспільства. Лише за умови спільних зусиль державних органів, громадянського суспільства, академічної спільноти та приватного сектора можливо створити ресурсоміцну та ефективну систему протидії дезінформації, що буде відповідати сучасним викликам і допоможе забезпечити стабільність та добробут суспільства.

3.2. Створення законопроекту про виявлення дезінформації та запобігання її поширенню: аналіз міжнародного досвіду та рекомендації для України

Аналіз стану протидії дезінформації в Україні підтверджує, що цей напрям є одним з пріоритетних у державній політиці на сучасному етапі. Проте існуюче законодавство не забезпечує достатнього рівня захисту від дезінформації та не враховує особливостей сучасних технологій та інформаційних потоків. У зв'язку з цим розробка законопроекту про протидію дезінформації в Україні стає актуальним завданням, що вимагає негайної уваги.

Для забезпечення ефективності такого законопроекту та його відповідності міжнародним стандартам необхідно врахувати досвід інших країн. В цьому контексті можна виокремити Німеччину, Францію та Італію, які стали першими серед країн-членів Європейського Союзу, що ухвалили законодавчі акти, спрямовані на протидію дезінформації. Варто зазначити, що кожна з цих країн розробляє власне законодавство, враховуючи свої потреби та особливі умови.

Наприклад, у Німеччині з 2017 року діє закон про мережеві інформаційні послуги (NetzDG) [295], спрямований на протидію фейкам, дифамації та мові ворожнечі у соціальних мережах. Відповідно до цього закону, великі соціальні мережі, які мають понад два мільйони користувачів з Німеччини, зобов'язані видаляти очевидно незаконний контент протягом 24 годин з моменту отримання відповідної скарги від користувачів. Термін може бути подовжений до семи днів, якщо незаконність контенту складно визначити відразу.

Крім того, провайдери телемедійних послуг, які керують соціальними платформами в Інтернеті, зобов’язанідвічі на рік публікувати звіти про кількість отриманих запитів на видалення протизаконної

інформації, рівень їх задоволення та загальні дані про способи і правила видалення контенту.

У разі порушення соціальними мережами та платформами вимог закону NetzDG, передбачені адміністративні штрафи, які можуть сягати до 50 мільйонів євро. Крім того, закон відкриває можливість порушення кримінальної справи проти керівництва соціальної мережі або платформи у разі систематичного та грубого порушення закону NetzDG.

Однак, слід зауважити, що незважаючи на включення поширення фейків до переліку незаконного контенту, закон NetzDG не забезпечує повного охоплення всіх аспектів дезінформації в Інтернеті через відсутність її визначення, тоді як поняття «фейк» є дуже широким і включає багатоформ недостовірної інформації.

Звичайні користувачі, як правило, не несуть відповідальності за поширення незаконного контенту на платформах соціальних мереж та інших онлайн-сервісах. Проте, якщо користувач публікує матеріали, що містять ознаки екстремізму,расизму, пропаганди насилля, сексуальних домагань тощо, він може бути притягнутий до кримінальної відповідальності згідно зі статтями 86-91 і 126-129 Кримінального кодексу Німеччини за злочини проти державної безпеки та злочини екстремістської спрямованості.

Таким чином, можна стверджувати, що законодавство Німеччини в основному регулює традиційний незаконний контент і не повністю враховує сучасні явища, пов’язані з дезінформацією в Інтернеті.

Французький закон «Про боротьбу з маніпуляційною інформацією» [294], також відомий як «закон проти фейків», був ухвалений у грудні 2018 року з метою встановлення механізмів протидії дезінформації перед виборами. Цей закон накладає обов’язкина великі інтернет-платформи, такі як Facebook і Twitter для запобігання поширенню незаконного контенту на їхніх платформах.

Зокрема, закон вимагає, щоб платформи розкривати інформацію про спонсорів політичних рекламних матеріалів, встановлювали маркуванняконтенту, пов’язаного з політикою, та впроваджували процедури швидкого видалення незаконного контенту.

Стаття L. 163-1 цього закону встановлює кримінальну відповідальність за порушення, пов'язані з поширенням неправдивої інформації в період виборів. За такі порушення передбачено покаранняу вигляді позбавлення волі на один рік та штрафу у розмірі 75 000 євро. Юридичні особи, визнані винними у порушенні закону, також несуть відповідальність згідно з відповідними статтями Кримінального кодексу Франції. Зокрема, їм може бути накладено заборону здійснювати будь-яку професійну діяльність з максимальним терміном до п’яти років за поширення або сприяння поширенню маніпулятивної інформації.

Проте, слід зазначити, що закон «Про боротьбу з маніпуляційною інформацією» має свої обмеження. Наприклад, він не забезпечує повного охоплення всіх аспектів дезінформації через відсутність єдиного та чіткого визначення цього терміну. Поняття "маніпулятивна інформація" також може бути широким і неоднозначним, що створює виклики при визначенні його меж.

Однак, французький закон відображає зусилля країни боротися з поширенням дезінформації та маніпулятивної інформації в Інтернеті. Його введення в життя сприяє підвищенню відповідальності платформ та захисту громадян від незаконного та шкідливого контенту.

Закони, подібні до вищезгаданих, були також прийняті в деяких інших країнах Європи. Наприклад, у 2020 році литовський парламент затвердив закон про захист інформації, який включає положення щодо боротьби з дезінформацією. Згідно з цим законом, особи, що розповсюджують дезінформацію, можуть бути покарані штрафом або позбавлені волі на термін до трьох років. Більш того, закон встановлює заходи протидії дезінформації в Інтернеті, включаючи обов'язкову

ідентифікацію користувачів соціальних мереж, а також обов'язкове розміщення попереджень про можливу дезінформацію на новинних веб-сайтах.

В Італії у 2018 році був ухвалений «Закон про заходи щодо боротьби з явищами виникнення, поширення та посилення неправдивої інформації в Інтернеті», який встановив відповідальність за створення та розповсюдження неправдивої інформації, зокрема стосовно кандидатів на виборах.Закон також вимагає від соціальних мереж більш активних заходів, спрямованих на протидію дезінформації, зокрема шляхом встановлення механізмів швидкого зупинення розповсюдження недостовірної інформації та повідомлення користувачів про її неправдивий характер.

Згадані вище законодавчі ініціативи вказують на зростаюче усвідомлення в ЄС необхідності регулювання поширення дезінформації в Інтернеті з метою виявлення, блокування та зниження реальних і потенційних шкідливих наслідків цього явища.

На сучасному етапі протидії дезінформації у світі виділяються два підходи до регулювання інформаційного простору: західна та східна моделі. Західна модель ґрунтуєтьсяна демократичних принципах та наголошує на значенні свободи слова як основного права. Зі свого боку, східна модель заснована на визначальному державному контролі.

Наприклад, в Китайській Народній Республіці (КНР) діє система жорсткого державного контролю над ЗМІ, включаючи Інтернет та соціальні мережі. Китайський уряд встановлює цензуру на контент, який вважається шкідливим або небажаним. Крім того, в країні діє законодавство, згідно з яким електронні ЗМІ зобов’язані реєструватися та надавати владі доступ до даних про користувачів. Згідно з Кримінальним кодексом Китаю, поширення неправдивої інформації може бути визнане злочинм, за який передбачається штрафвід 5000 до 500 000 юанів (орієнтовно, від $750 до $75 000), абопозбавлення волі терміном від трьох

до семи років. Крім того, у Китаї діє система фільтраціїї "Great Firewall" (Золотий щит), яка блокує доступ до заборонених іноземних веб-сайтів та контенту, який, на думку китайського уряду, завдає шкоди національним інтересам КНР. Варто зазначити, що країна загалом не дотримується принципу свободи слова та може трактувати терміни, пов’язані з регулюванням інформаційного простору, по-різному.

В Росії дезінформацію визначають як поширення неправдивої інформації, яка може завдатишкоди правам та інтересах громадян або суспільства. Згідно з таким широким визначенням, дезінформація є протиправним діянням і може тягнути за собою юридичну відповідальність. Зокрема, з 2014 року в РФ діє законодавча норма, яка передбачає обов’язкову реєстрацію блогерівз понад трьома тисячами користувачів у Федеральній службі з нагляду у сфері зв’язку, інформаційних технологій і масових комунікацій. У 2019 році був також прийнятий закон про адміністративні правопорушення, який передбачаєдиференційовані штрафи за поширення недостовірної інформації в Інтернеті для фізичних осіб, юридичних осіб та посадовців. З квітня 2023 року в РФ набули чинностідві норми: одна стосується відповідальності за дискредитацію використання російських збройних сил за кордоном і передбачає до семи років позбавлення волі, а друга стосується поширення «завідомо неправдивої інформації" про ці формування з терміном покарання до 15 років позбавлення волі. Крім того, ще в березні 2022 року в Росії у судовому порядку було визнано Meta «екстремістською організацією» і заблоковано доступ доFacebook та Instagram.

Хоча не можна однозначно стверджувати, що авторитарні країни мають більш розмите визначення дезінформаціїта суворіше покарання за її поширення, проте авторитарні режими можуть використовувати широкі та нечіткі визначення дезінформації для виправдання політично мотивованих переслідувань опозиційних голосів та критиків уряду.

У демократичних країнах також існують закони, що забороняють поширення дезінформації, проте вони частіше мають більш конкретне визначення дезінформації та використовують менш жорсткі заходи покарання, такіяк штрафи або призупинення діяльності, у порівнянніз більш суворими заходами, такими як арешт або ув'язнення, що передбачені в авторитарних режимах.

При створенні законопроекту про протидію дезінформації необхідно враховувати примат свободи слова та поширення інформації, що є важливою умовою демократії та захисту прав людини. Згідно з Міжнародним пактом про громадянські і політичні права [120], кожен має право на свободу думки, совісті тавираження своїх поглядів у всіх формах, включаючи пресу, мирні збори та асоціації. Однак, це право може бути обмежене з метою захисту інших прав та інтересів.

Європейська конвенція з прав людини (ЄКПЛ) [95], прийнята у 1950 році, визнає свободу висловлювання та свободу інформації як основні права (стаття 10). Згідно з Конвенцією, кожна людина має право на свободу думок, совісті та вираження своїх поглядів, незалежно від того, чи є вони образливими або несприятливими, а також право на створення та поширення інформації без втручання державних органів та незалежно від кордонів. Однак, Конверція визнає, що це право може бути обмежене, якщо це необхідно для захисту національної безпеки, громадського порядку, здоров'я та моралі. Важливо зауважити, що такі обмеження повинні бути зрозумілими, передбачуваними та пропорційними.

За два роки до прийняття ЄКПЛ, Генеральна Асамблея ООН ухвалила і проголосила резолюцію 217 А (III) від 10 грудня 1948 року, відому як Загальна декларація прав людини [57]. Стаття 19 цієї Декларації гарантує свободу вираження думок та інформації як одне з основних прав людини, але також передбачає обмеження цього права, якщо це необхідно для захисту прав та інтересів інших.

у 1976 році Європейський суд з прав людини (ЄСПЛ) ухвалив рішення у справі "Handyside проти Великої Британії" [276], яке вважається визначальним у встановленні стандартів щодо свободи слова в Європі. В цьому рішенні ЄСПЛ визнав свободу висловлювання однією з фундаментальних складових демократії,при цьому обмеження цієї свободи можуть бути виправданими лише в обмеженому числі випадків, коли вони є необхідними для захисту інших прав або інтересів, таких як національна безпека, громадський порядок або мораль. Рішення також наголосило, що обмеження свободи слова повинні бути пропорційними та необхідними в рамках демократичного суспільства. Рішення у справі Handyside відіграло значну роль у формуванн стандартів свободи слова в Європі та вплинуло на законодавство багатьох країн.

Таким чином, баланс між свободою слова та національними інтересами є складною проблемою, яка вимагає врахування різних факторів та узгодженого підходу. З одного боку, свобода слова є однією з основних цінностей демократичного суспільства і гарантує право людей на вільне висловлювання своїх поглядів та думок. Вільне слово є необхідним для розвитку науки, культури, журналістики та інших сфер, які забезпечують прогрес та інновації в суспільстві.

З іншого боку, інтереси національної безпеки та інтереси держави не завжди збігаються зі свободою слова. В деяких випадках, така свобода може поставити під загрозу національну безпеку, створити загрозу громадському порядку та спричинити шкоду інтересам держави [50].

Аналізуючи міжнародний досвід, Україна активно займається розробкою власних стратегій протидії дезінформації. Варто відзначити, що в межах наявного нормативно-правового поля в державі вже існують статті адміністративної та кримінальної відповідальності за поширення неправдивої інформації. З цього приводу, деякі експерти рекомендують обмежитися застосуванням вже наявних норм у судовій практиці. Однак, ми не можемо погодитись з таким підходом, оскільки, по-перше, ці норми

є застарілими та не відповідають вимогам сучасності. А головне,закон про протидію дезінформації має охоплювати не лише точкову відповідальність та покарання за окремі прояви дезінформації, а й передбачати системні заходи, спрямовані на запобігання поширення дезінформації та забезпечення інформаційної безпеки суспільства. Враховуючи складну природу проблеми та широкий спектр її проявів, необхідно розробити комплексну стратегію, яка включатиме правові, технологічні та освітні заходи.

При дослідженні дезінформації як правової категорії важливо враховувати три основні аспекти: інституціональний, ознаковий та змістовий.

Інституціональний аспект охоплює систему державних органів та законодавчі акти, що регулюють протидію дезінформації. Він також передбачає розробку правових механізмів для запобігання дезінформації, включаючи профілактичні заходи та співпрацю зі ЗМІ, громадськими організаціями та міжнародними партнерами.

Ознаковий аспект дезінформації визначається її позитивними та негативними ознаками з правової точки зору. Вона може бути розглянута як свобода висловлювання або як загроза національним інтересам, що вимагає встановлення відповідальності та механізмів реагування відповідно до законодавства та міжнародних стандартів прав людини.

Змістовий аспект дезінформації пов'язаний з визначенням самого поняття і включає характеристики шкідливості, небезпеки, масштабів та наслідків дезінформації. Правове визначення зазвичай є більш конкретним і спрямованим на законодавчі акти та юридичні процедури.

У першому розділі дисертації ми сформулювали визначення терміну «дезінформація». Згідно з ним, дезінформація – це створення та поширення з політичною чи іншою стратегічною метою завідомо хибної чи свідомо модифікованої інформації як істинної для інформаційно-психологічного впливу на об’єкт з метою формування в нього

помилкового уявлення про реальність та підштовхування до певних дій чи бездіяльності.

Це визначення описує ключові ознаки дезінформації, але не враховує деякі важливі аспекти для правового аналізу. Наприклад, не вказується, хто є об'єктом дезінформації, що може мати значення для її кваліфікації як злочину чи правопорушення. Також не уточнюється, як доводяться наміри створення дезінформації. Крім того, не пояснюється, якоцінюється інформаційно-психологічний вплив та щовважається небажаними або небезпечними діями. Така невизначеність може призвести до необґрунтованих обмежень свободи слова. Тому необхідно розширити визначення дезінформації з урахуванням зазначених аспектів, щоб забезпечити більш точний та повний правовий аналіз.

Таким чином, визначення дезінформації як правової категорії може мати такий вигляд: дезінформація – це процес створення та/або поширення неправдивої інформації, яка містить вигадані відомості або приховує чи спотворює факти з метою завдання шкоди інтересам людини, суспільства та держави.

Проте, таке загальне визначення потребує уточнень. Важливо скласти список видів недостовірної інформації та встановити критерії, за якими недостовірна інформація може бути визнана дезінформацією.

Отже, основні види недостовірної інформації (список не є вичерпним) включають:

1. Фейки – вигадки та міфи, створені з метою з обману аудиторії про події чи факти, які ніби-то існували/існують насправді.

2. Безпідставні звинувачення (наклеп) –поширення завідомо неправдивих відомостей, що ганьблять честь і гідність іншої особи.

3. Некоректна інформація (misinformation) – неточна інформація, поширена без наміру спричинити негативні наслідки.

4. Неперевірена інформація (чутки та плітки) – неверифікованідані, отримані з ненадійних джерел (включаючи так звані анонімні джерела ЗМІ), поширені усно або через канали масової комунікації.

5. «Теорії змови» - непідтверджені або спростовані інформаційні матеріали про приховані домовленості між організаціями, групами людей або державами.

6. Підміна фактуоціночним судженням –некоректне викладення суб'єктивних суджень про факт, що може призвести до неправильного розуміння самого факту як об'єктивної реальності та спричинити недостовірні висновки про нього.

7. Зловживання статистикою (маніпуляція статистикою) – використання вибіркових або неправильних методів аналізу для підтвердження певного аргументу або думки.

8. Маніпулятивна інформація (спотворена інформація) – інформаційні матеріали, навмисно змінені або вирвані з контексту для створення хибного враження про їх первісний зміст.

9. Упередженість інформації – твердження, що базуються на особистих переконаннях, стереотипах або політичних поглядах, що можуть призвести до недостовірних висновків.

10. Анонімний акаунт – обліковий запис або профіль в Інтернеті, який приховує або маскує ідентичність користувача, не розкриваючи справжню інформацію про нього.

11. Підробний веб-сайт, профіль або акаунт – інтернет-ресурс, який неправомірно претендує на ідентичність або підробляє ідентичність когось іншого.

Для встановлення факту дезінформації пропонуємо скористатися таким визначенням: недостовірна інформація стає дезінформацією, якщо відповідає чотирьом критеріям: має недостовірний зміст; навмисно створена або спотворена; поширена з певною метою; може вплинути на громадську думку.

Вислів «має недостовірний зміст» вказує на те, що інформація містить неточності, помилки, вигадки, довільну інтерпретацію фактів, подій або даних і є об’єктивно хибною.

Вислів «навмисно створена або спотворена» вказує на те , що особа або група осіб, які створили дезінформацію, діяли усвідомлено шляхом вигадування неіснуючих фактів або викривлення існуючих.

Навмисно створена або спотворена інформація може включати, але не обмежується такими елементами:

– помилкові або спотворені відомості, які навмисно суперечать фактам, подіям, статистичним даним, висловленим позиціям або науковим доказам;

– маніпулятивне використання фотографій, відеозаписів, аудіозаписів або інших візуальних чи звукових матеріалів з метою створення ілюзії чи спотворення подій;

– фальсифікація джерел інформації або неправомірне використання авторитетних імен, організацій чи медіа-ресурсів для підтримки недостовірних тверджень;

– використання ботів, автоматизованих систем чи інших технологій для автоматичної генерації чи розповсюдження дезінформації.

Поширення (розповсюдження) дезінформації в рамках цього законопроекту визначається як будь-який один із пунктів:

1. Цілеспрямоване поширення недостовірної інформації для введення в оману громадськості, створення хибного враження для досягнення політичних, комерційних або інших цілей.
2. Організована діяльність, спрямована на масове розповсюдження дезінформації з використанням мережевих ресурсів, соціальних медіа, платформ та інших засобів інформаційних комунікацій.
3. Створення і підтримка штучних спільнот, груп, акаунтів або профілів з метою широкого розповсюдження дезінформації та маніпуляції громадською думкою.

4. Фінансування або організація діяльності, спрямованої на розповсюдження дезінформації або маніпуляцію інформацією з метою досягнення певних політичних, економічних чи інших інтересів.

Під метою поширення дезінформації в рамках цього законопроекту розуміється активне поширення або обмін інформацією з використанням будь-яких інформаційних ресурсів для досягнення певних цілей, зокрема, але не обмежуючись наступними:

– завдання шкоди національній безпеці України шляхом розпалювання міжнаціональної або міжетнічної ворожнечі, підбурювання до насильства, тероризму, екстремізму або ксенофобії;

– нав'язування суспільству певних цінностей, ідеологій, релігійних переконань або світогляду для впливу на громадську думку;

– розповсюдження недостовірної інформації з метою дискредитації або підваження ділової репутації державних органів, приватних компаній, громадських діячів та інших суб'єктів правових відносин;

– використання засобів масової інформації для здійснення пропаганди, включаючи пропаганду насильства, війни або агресії, а також пропаганду наркотиків, алкоголю, тютюну або інших речовин, здатних завдати шкоди здоров'ю.

Під інформаційним ресурсом в контексті цього законопроекту розуміється будь-який засіб для зберігання, обробки та передачі інформації. Це може бути пристрій, програма, система або технологія– комп'ютер, мобільний телефон, сховище даних, мережевий комунікаційний засіб, база даних, програма для обробки інформації тощо.

Інші терміни у цьому законопроекті вживаються в такому значенні:

1. Спроба впливу на громадську думку – навмисні дії з використанням різних засобів та методів інформаційно-психологічного маніпулювання, спрямовані на формування, зміну або зміцнення переконань, думок та оцінок громадськості з метою досягнення певних

результатів, таких як дестабілізація політичної обстановки, дискредитація державних інституцій, організацій, громадських діячів або інших суб'єктів правових відносин.

2. Суб'єкт поширення дезінформації – будь-яка фізична або юридична особа, яка навмисно створює, спотворює або поширює інформацію з метою введення в оману, маніпулювання громадською думкою або нав'язування певних переконань.

Суб'єкт поширення дезінформації може включати, але не обмежується такими категоріями:

– фізичні або юридичні особи, що публікують або поширюють дезінформацію через засоби масової інформації, такі як друковані видання, телебачення, радіо, онлайн-портали та соціальні мережі.

– власники або адміністратори веб-сайтів, форумів або блогів, де систематично розміщується дезінформація.

–особи, що активно діють у соціальних мережах, публікують та поширюють дезінформацію серед широкої аудиторії.

–організації або структури, що фінансують або організовують поширення дезінформації з метою задоволення політичних, економічних або інших інтересів.

3. Об'єкт дезінформації – окрема особа або група осіб, спільнота чи організація, на яку спрямована дезінформація з метою впливу на їх свідомість, поведінку, думки або рішення, в тому числі в інтересах третіх осіб, що суперечать суспільним інтересам або принципам права і моралі.

Об'єкти дезінформації можуть включати, але не обмежуються наступними категоріями:

– окремі особи, зокрема державні службовці, політичні діячі, громадські лідери та інші публічні особи, які стають мішенню дезінформації з метою дискредитації, компрометації, формування негативного іміджу або зміни їх сприйняття громадськістю;

– різноманітні спільноти, групи або організації, такі як етнічні або релігійні громади, соціальні або професійні групи, студентські або молодіжні організації, на які спрямована дезінформація з метою розпалювання міжетнічної ворожнечі, релігійних конфліктів, політичної нестабільності або дестабілізації суспільної гармонії;

– спільноти, які використовують інтернет-платформи, соціальні мережі, форуми або інші засоби комунікації, які стають об'єктами дезінформації, спрямованої на формування певних переконань, маніпулювання громадською думкою або створення ворожої атмосфери;

– державні інтереси. Дезінформація може спрямовуватись на дискредитацію, маніпуляцію або спотворення інформації, що стосується державних інтересів. Це може включати поширення недостовірних чи спотворених даних про політичні рішення, міжнародні відносини, економічну ситуацію та інші аспекти, які мають важливе значення для держави.

4. Канали поширення дезінформації – засоби масової інформації, платформи, соціальні мережі, месенджери, електронна пошта та будь-які інші канали, які можуть використовуватися для передачі інформації незалежно від формату та носія.

Канали поширення дезінформації можуть включати, але не обмежуються наступними прикладами:

– засоби масової інформації, такі як телебачення, радіо, газети, журнали, новинні агентства та інші друковані та електронні ЗМІ, які використовуються для поширення дезінформації.

– інтернет-платформи, включаючи соціальні мережі, відеохостинги, блог-платформи, форуми, месенджери та інші онлайн-сервіси, які використовуються для масштабного поширення дезінформації.

– веб-сайти, блоги або інтернет-портали, спеціально створені або використовувані для публікації та поширення дезінформації.

– тролл-фабрики, бот-мережі або інші автоматизовані системи, які використовуються для масового створення та поширення дезінформації через соціальні мережі та інші онлайн-платформи.

– оффлайн-канали зв'язку, такі як друковані матеріали, листівки, плакати, лекції або презентації, які використовуються для поширення дезінформації серед широкої аудиторії.

Визначення ефективних механізмів є наступним необхідним етапом у розробці законопроекту після встановлення термінології. Наведені нижче можливі механізми сприяють ідентифікації дезінформаційних матеріалів та їх джерел, а також вилученню дезінформації з інформаційного простору та запобіганню її поширенню.

Перший механізм передбачає розвиток Центру протидії дезінформації при РНБО (далі - Центр). Вже зараз Центр виконує важливу роботу з моніторингу та аналізу інформаційного простору. Однак, для більш ефективної протидії дезінформації, яка включає кілька напрямків, необхідно розширити його повноваження та матеріально-технічну базу.

Перш за все, варто зміцнити роль Центр в координації діяльності державних структур з протидії дезінформації шляхом надання йому додаткових повноважень, ресурсів і технічних засобів. Важливо встановити активну співпрацю Центру з академічними та науковими установами, а також з незалежними експертами, які спеціалізуються на виявленні дезінформації та запобіганні її поширенню. Також варто налагодити партнерські взаємовідносини з громадськими організаціями та медіа.

Другий напрям вдосконалення діяльності Центру передбачає розвиток системи моніторингу та аналізу дезінформації. Необхідно створити ефективну систему автоматичного моніторингу та аналізу інформаційного простору, включаючи застосування передових технологій та алгоритмів машинного навчання. Це дозволить швидко виявляти нові форми дезінформації та оперативно реагувати на них. Для реалізації такої

системи необхідно залучати фахівців у галузі штучного інтелекту та аналізу даних.Також варто розвивати експертний аналіз дезінформації з участю фахівців з інформаційної безпеки, журналістів та дослідників. Це дозволить Центру проводити більш глибокий аналіз дезінформаційних кампаній, ідентифікувати джерела та поширювачів дезінформації, а також аналізувати їх вплив на громадську думку та політичні процеси.

Третій напрям полягає у створенні механізмів оперативної реакції на дезінформацію, зокрема: розширення функцій Центру шляхом створення відділу аналітики та експертизи;відкриття для громадськості та сторонніх організацій бази даних Центру про дезінформацію; встановлення механізмів співпраці та обміну інформацією із соціальними мережами, платформами та провайдерами послуг з метою забезпечення оперативного видалення та блокування дезінформаційного контенту; створення мережі регіональних державних центрів протидії дезінформації, які будуть взаємодіяти з центральним офісом.

Дія другого механізму має бути спрямована на розвиток критичного мислення та медіаграмотності серед населення.

Цей аспект повинен бути врахований у системі освіти, зокрема на початковому рівні. Для досягнення цієї мети до Закону України "Про освіту"необхідно внести зміни, які б унормували впровадження відповідних заходів. Нижче наведено приклад окремої статті, яка могла б бути включена до цього закону:

Стаття 2. Розвиток критичного мислення та медіаграмотності населення

2.1. Держава забезпечує розвиток критичного мислення та медіаграмотності населення шляхом створення необхідних умов для їх освоєння в процесі навчання в освітніх закладах.

2.2. Освітні заклади зобов'язані включати до навчального плану модулі, курси та програми, спрямовані на навчання критичному мисленню та медіаграмотності.

2.3. Навчання критичному мисленню та медіаграмотності передбачає такі елементи:

2.3.1. Вивчення теорії інформації та основ медіакомпетентності.

2.3.2. Аналіз та оцінка інформації, отриманої через різні медіа-канали, з урахуванням можливої дезінформації та спотворень.

2.3.3. Навчання навичкам пошуку, аналізу та перевірки інформації в Інтернеті, включаючи використання спеціальних інструментів та ресурсів для протидії дезінформації.

2.4. Держава зобов'язується підтримувати розвиток та вдосконалення освітніх програм, курсів та модулів, пов'язаних з критичним мисленням та медіаграмотністю. Це включає постійне оновлення матеріалів і методик, а також забезпечення доступу до актуальних досліджень та ресурсів у цій галузі.

2.5. Для забезпечення ефективного розвитку критичного мислення та медіаграмотності, держава сприяє підвищенню кваліфікації педагогічних працівників, які мають навички та знання у цій сфері. Зокрема, проводяться тренінги, семінари та інші заходи, спрямовані на підвищення професійної компетентності вчителів.

2.6. Державні і недержавні організації, медійні установи та громадські організації сприяють розробці та поширенню інформаційних матеріалів, які сприяють розвитку критичного мислення та медіаграмотності. Вони проводять інформаційно-освітні кампанії, організовують тренінги та дискусії з метою підвищення рівня обізнаності населення щодо проблем дезінформації та шкідливого впливу медіа.

2.7. Забезпечення розвитку критичного мислення та медіаграмотності включає активну співпрацю між освітніми установами, медійними організаціями, родинами та громадськістю. Це може бути досягнуто через організацію спільних проектів, партнерство та обмін досвідом у галузі розвитку медіаграмотності.

2.8. Держава сприяє створенню спеціалізованих дослідницьких центрів та лабораторій з метою проведення наукових досліджень в галузі критичного мислення та медіаграмотності. Ці установи забезпечують наукову підтримку і експертні рекомендації для розвитку ефективних стратегій протидії дезінформації та підвищення рівня медіаграмотності.

Крім того, на законодавчому рівні необхідно передбачити механізми підтримки проектів та програм, що спрямовані на розвиток критичного мислення та медіаосвіти серед дорослого населення. Основні механізми підтримки таких ініціатив можуть включати фінансування проектів та програм з боку держави або місцевих органів влади, спрямованих на розвиток критичного мислення та медіаосвіти,надання податкових пільг організаціям, що займаються розвитком критичного мислення та медіаосвіти, наприклад, журналістським школам та курсам з медіаосвіти тощо.

Третій механізм – встановлення міри відповідальності за поширення дезінформації, що є ключовим аспектом в будь-якій системі, спрямованій на регулювання поведінки людей, адже «значна кількість онлайн-медіа і незалежних блогерів працює без належного контролю над розповсюдженням контенту, що дозволяє вільно поширювати дезінформацію без будь-яких обмежень» [54]. Але забезпечення відповідальності за поширення дезінформації повинно базуватись на відповідних правових нормах і бути пропорційним ступеню наслідків.

У рамках законопроекту щодо протидії дезінформації можуть бути передбачені такі заходи адміністративної відповідальності для осіб та організацій:

1. Застосування штрафів у розмірі від 50 до 100 мінімальних заробітних плат за поширення дезінформації, яка може завдати шкоди національним інтересам держави або суспільству. Розмір штрафів диференціюється залежно від характеру та масштабу поширеної дезінформації.

2. У разі системного та умисного поширення дезінформації щодо порушника може прийматися рішення про заборону на певну діяльність, пов'язану з медіа чи інформаційними ресурсами.

3. Якщо ліцензовані медіаорганізації систематично поширюють дезінформацію, може прийматися рішення про відкликання їх ліцензії на здійснення медіадіяльності.

4. За незначні порушення вимог закону щодо протидії дезінформації може застосовуватися попередження, винесене у письмовій або усній формі, з метою запобігання подальшому поширенню дезінформації.

5. Застосування адміністративного виключення із соціальних мереж та месенджерів на термін до 3 місяців за поширення дезінформації, яка спричинила порушення громадського порядку або порушення прав та свобод громадян.

6. Ліквідація юридичної особи за систематичне поширення дезінформації, яка призвела до порушення законодавства та інтересів суспільства.

У кожному конкретному випадку застосування заходів адміністративної відповідальності повинно бути обґрунтоване та відповідати вимогам закону.

Кримінальна відповідальність за поширення дезінформації може включати такі заходи:

1. Умовне засудження, що передбачає можливість уникнення реального ув'язнення за умови дотримання певних умов, встановлених судом.

2. Покарання у вигляді позбавлення волі яке є найбільш серйозним заходом кримінальної відповідальності і може бути застосоване у випадках, коли поширення дезінформації завдає значної шкоди суспільству або державі.

3. Конфіскація майна, що може бути застосована у разі, коли поширення дезінформації здійснювалося з метою отримання незаконної

вигоди. Суд може прийняти рішення про конфіскацію майна, яке було набуте внаслідок таких дій.

4. Примусові заходи, що можуть бути застосовані у окремих випадках. Суд може вирішити застосувати примусові заходи до особи, яка поширює дезінформацію, наприклад, примусову державну або громадську допомогу.

Крім того, Кримінальний кодекс України може містити конкретні статті, що стосуються поширення дезінформації і встановлюють відповідні санкції. Наприклад, статтю щодо розповсюдження завідомо неправдивої інформації, згідно з якою неправомірний доступ до комп'ютерної інформації карається штрафом від 50 до 500 неоподатковуваних мінімумів доходів громадян або обмеженням волі до двох років, або позбавлення волі на такий само термін. Втручання у роботу електронної обчислювальної машини, обчислювальної або телекомунікаційної мережевої ресурсу карається штрафом від 100 до 500 неоподатковуваних мінімумів доходів громадян або позбавленням волі на термін до двох років. Організація масових безладів в результаті розповсюдження завідомо неправдивої інформації може передбачати позбавлення волі на термін до п'яти років. Використання засобів масової інформації для розповсюдження завідомо неправдивої інформації може передбачати штраф або позбавлення волі на термін до трьох років.

Четвертим механізмом законодавчого врегулювання протидії поширенню дезінформації може бути встановлення зобов’язань для провайдерів інформаційних послуг, включаючи соціальні мережі та пошукові системи. Відповідний розділ законопроекту може передбачати:

1. Обов'язкове видалення недостовірної інформації:

– провайдери інформаційних послуг зобов'язані вживати заходів щодо видалення неправдивої інформації, яка може завдати шкоди приватним особам, організаціям або державним інституціям;

– провайдери інформаційних послуг повинні розробити та надати користувачам механізми для подання скарг та розгляду звернень, пов'язаних з поширенням неправдивої інформації;

– провайдери інформаційних послуг зобов'язані швидко й ефективно реагувати на скарги та видаляти неправдиву інформацію протягом розумного строку після отримання відповідного звернення.

2. Надання інформації про поширювачів дезінформації:

– провайдери інформаційних послуг зобов'язані надавати інформацію про поширювачів дезінформації, які використовують їх сервіси для розповсюдження хибної інформації;

–провайдери інформаційних послуг повинні надавати інформацію про поширювачів дезінформації компетентним органам за запитом;

– провайдери інформаційних послуг не повинні розкривати особисту інформацію користувачів, за винятком випадків, передбачених законодавством.

3. Забезпечення прозорості:

– провайдери інформаційних послуг зобов'язані забезпечувати прозорість щодо своїх механізмів боротьби з поширенням дезінформації;

– провайдери інформаційних послуг повинні регулярно публікувати звіти про свої заходи щодо боротьби з поширенням дезінформації та про ефективність цих заходів;

– провайдери інформаційних послуг зобов'язані надавати користувачам можливість оскарження рішень, пов'язаних з видаленням інформації.

4. Санкції за порушення:

– у разі систематичного або умисного порушення зобов'язань провайдерами інформаційних послуг, пов'язаних з боротьбою з поширенням дезінформації, можуть бути застосовані адміністративні, цивільно-правові або кримінальні санкції відповідно до законодавства;

– розмір санкцій має бути пропорційним характеру та масштабу порушень з урахуванням впливу поширення дезінформації на громадський порядок, безпеку та інтереси громадян;

– застосування санкцій повинно здійснюватись з дотриманням принципів справедливості, пропорційності та прав людини і свободи слова.

Законодавче врегулювання накладених зобов'язань на провайдерів інформаційних послуг може стати ефективним четвертим механізмом для стримування поширення дезінформації та забезпечення ефективнішого контролю над інформаційними матеріалами, що поширюються в мережі.

В якості п’ятого механізму законодавчого врегулювання протидії поширенню дезінформаціїдоцільно розглянути можливість створення посади уповноваженого із захисту інформації, який матиме повноваження подавати позови до суду щодо притягнення до відповідальності за поширення дезінформації. Уповноважений із захисту інформації, як незалежний орган з доступом до інформації, аналітичних ресурсів та професійних експертів, зможе оперативно виявляти випадки поширення дезінформації та вживати заходів щодо її припинення. Такий орган зможе діяти швидше та ефективніше, ніж державні органи, які можуть бути зайняті вирішенням інших завдань.

Крім того, уповноважений із захисту інформації матиме значно більше можливостей для застосування правових важелів щодо поширювачів дезінформації. Окрім того, що він зможе звертатися до суду з позовами на видалення недостовірної інформації та відшкодування шкоди, заподіяної дезінформацією, такий орган також зможе працювати над розробкою та удосконаленням законодавства, спрямованого на протидію дезінформації.

Однак, перед введенням посади уповноваженого із захисту інформації необхідно врахувати такі фактори:

1. Юридична компетенція. Для ефективної роботи інституту уповноваженого із захисту інформації необхідно забезпечити наявність

юридичних знань та досвіду у сфері захисту інформації та правової відповідальності за поширення дезінформації в самого уповноваженого та працівників його апарату.

2.Фінансування. Слід враховувати фінансові витрати на створення та підтримання посади уповноваженого із захисту інформації, включаючи оплату праці, юридичну підтримку та інші витрати.

3. Взаємодія з іншими органами. Уповноважений із захисту інформації має співпрацювати з іншими структурами, такими як правоохоронні органи та суди, для забезпечення ефективності роботи з протидії дезінформації.

4. Розмежування повноважень. Слід чітко визначити межі повноважень уповноваженого із захисту інформації та не допускати їх перекриття з повноваженнями інших структур, задіяних у сфері протидії дезінформації.

В цілому, установлення посади уповноваженого з захисту інформації може стати ефективним механізмом для протидії дезінформації та захисту суспільства від негативного впливу недостовірної інформації.

Узагальнюючи вищевикладене, можемо підсумувати, що процес розробки законопроекту про протидію дезінформації включає кілька етапів.

Першим етапом є аналіз світових практик, що дозволяє визначити успішні підходи та ефективні механізми протидії дезінформації, а також уникнути помилок, що були зроблені в інших країнах. Цей етап сприяє накопиченню знань та досвіду, необхідних для розробки якісного та збалансованого законопроекту.

Другим етапом євизначення основних понять та термінів, що забезпечує юридичну точність та чіткість законопроекту, а також уникнення неоднозначності та розбіжностей у трактуванні понять. Це важливий аспект, оскільки належна формулювання термінології сприятиме узгодженості та однозначному розумінню положень закону.

Третій етап передбачає розроблення законодавчих механізмів виявлення дезінформації та запобігання її поширенню. Це охоплює розробку ефективних методів моніторингу та аналізу інформації, розвиток критичного мислення та медіаграмотності, встановлення міри відповідальності за поширення дезінформації, зобов'язання для провайдерів інформаційних послуг,та введення інституту уповноваженого з захисту інформації.

Ці рекомендації сприятимуть формуванню законопроекту, що забезпечить ефективну протидію дезінформації та запобігання її поширенню з збереженням балансу між свободою слова та захистом національних інтересів держави.

3.3. Цифрові інструменти для реалізації державної політики у сфері протидії дезінформації:вибір та оцінка ефективності

Вироблення практичних рекомендацій щодо використання цифрових інструментів у сфері протидії дезінформації є завершальним етапом нашого дослідження. На підставі проведеного аналізу механізмів вироблення державної політики у цій сфері можна зробити висновок, що використання цифрових інструментів може суттєво підвищити ефективність виявлення дезінформації та сприяти успішній реалізації заходів, спрямованих на запобігання її поширенню.

З метою порівняльного аналізу ефективності цифрових інструментів вважаємо за доцільне провести загальний огляд застосування таких інструментів у деяких європейських країнах та США. Це дозволить дослідити підходи та методи використання цифрових інструментів для протидії дезінформації та надати практичні рекомендації щодо їх використання.

Першою з країн, що була досліджена, є Франція, де уряд використовує різні цифрові інструменти, включаючи алгоритми

машинного навчання для виявлення дезінформації в соціальних мережах та інших цифрових медіа.

У Франції також діють кілька онлайн-платформ для боротьби з недостовірною інформацією, зокрема,платформа CrossCheck, що була створена для перевірки фактів і протидії дезінформації під час виборів у Франції. Однак проект виявився настільки успішним, що продовжив свою роботу і після виборів. Платформа об’єднує кілька медіа-організацій та незалежних журналістів, які перевіряють інформацію та діляться результатами своїх досліджень.

Окрім платформи CrossCheck, існують інші цифрові інструменти, що допомагають боротися з дезінформацією у Франції. Онлайнова база даних Decodex, створена газетою "Le Monde", містить список сайтів, що поширюють неправдиву та неточну інформацію, та допомагає читачам перевіряти джерела новин.

Крім того, уряд Франції створив онлайн-платформу Signalement, що доступна для широкої громадськості та дозволяє повідомляти про контент, що може містити дезінформацію або інші неприйнятні матеріали.

Ще одним цифровим інструментом є платформа Nouvelles de France, створена для протидії дезінформації в режимі реального часу. Ця платформа використовує штучний інтелект та алгоритми машинного навчання для аналізу новин та виявлення інформації, які може бути неточною або маніпулятивною.

Додатково, уряд Франції співпрацює з провайдерами соціальних мереж, такими як Facebook, Twitter та Google, з метою протидії дезінформації. Наприклад, у 2018 році Франція спільно з Google запустила програму боротьби з дезінформацією перед президентськими виборами.

Інші європейські країни також використовують різні цифрові інструменти для протидії дезінформації. Наприклад, уряд Іспанії створив інтернет-портал Maldito Bulo, який призначений для перевірки фактів та боротьби з фейками в Інтернеті.

Уряд Німеччини фінансує програму "Фортеця демократії" ("Demokratie stärken"), яка спрямована на фінансову підтримку організацій, що займаються розробкою інструментів протидії дезінформації. Серед таких організацій можуть бути фактчекери, медійні організації, наукові інститути та інші групи, які забезпечують свободу слова та борються з дезінформацією. Відбір отримувачів грантів здійснюється на конкурсній основі, де кандидати подають детальний опис проектів та бізнес-планів з описом очікуваних результатів. Заявки оцінює комісія експертів, яка вирішує, які проекти будуть фінансовані.

Додатково уряд Німеччини фінансує програму "Förderprogramm für innovative Maßnahmen zur Stärkung der Medienkompetenz" (Програма фінансування інноваційних заходів щодо зміцнення медійної грамотності). Метою програми є підтримка інноваційних ідей, які можуть допомогти підвищити медійну грамотність та зміцнити протидію дезінформації. Конкретні цілі програми включають розробку інструментів та сервісів для перевірки фактів та спростування дезінформації в онлайн-середовищі; створення та поширення освітніх матеріалів та ресурсів, які допомагають розвивати медійну грамотність та критичне мислення; підтримку та розвиток незалежних медіа, які є надійними джерелами інформації; розробку інструментів та сервісів для моніторингу та аналізу дезінформації в інформаційному просторі.

У свою чергу, італійський уряд у відповідь на високий рівень дезінформації розробив онлайн-інструмент Pagella Politica, що використовується командою професійних журналістів і фактчекерів для незалежної оцінки новин та подій, ґрунтуючись на фактах.

У Великобританії створено кілька незалежних організацій, таких як Full Fact і BBC Reality Check, які займаються перевіркою фактів та боротьбою з дезінформацією. Ці об’єднані організації використовують цифрові інструменти і технології, зокрема автоматичну обробку природної мови та машинне навчання, для автоматичної перевірки фактів та

виявлення дезінформації у великих обсягах текстових та відеоматеріалів. Крім того, вони надають громадськості ряд інструментів та ресурсів для розвитку медіаграмотності та протидії дезінформації, таких як довідники з перевірки фактів, курси навчання та інформаційні матеріали.

У Швеції одним із позитивних прикладів використання цифрових інструментів для боротьби з дезінформацією є проект Viralgranskaren, що був запущений газетою Expressen. Проект являє собою незалежну команду журналістів, які перевіряють вірусні новини та інформацію, що містить помилки, в соціальних мережах. Результати роботи команди публікуються в газеті та на веб-сайті проекту.

У США також використовуються цифрові інструменти для протидії дезінформації. Зокрема, Національний центр боротьби з дезінформацією (NCDCM) збирає та аналізує дані про дезінформацію і маніпуляції у ЗМІ та соціальних мережах, а також надає інформацію та рекомендації державним органам і громадськості. Також успішно функціонує Центр боротьби з кіберзлочинністю (CCU), який бореться з кіберманіпуляціями та дезінформацією на національному і міжнародному рівнях.У свою чергу, Комісія зі свободи преси (FPC) проводить дослідження та аналізує ситуацію зі свободою преси, розробляє рекомендації та рішення для зміцнення свободи слова та боротьби з дезінформацією. Крім того, Інформаційний центр США (USA.gov) у вигляді офіційного урядового веб-сайту забезпечує доступ широкій громадськості до інформації та ресурсів з різних питань, в тому числі з питань протидії дезінформації. USA.gov публікує новини та статті про дезінформацію, поради з перевірки фактів, рекомендації щодо використання безпечних та достовірних джерел інформації, а також посилання на інші ресурси та інструменти.

Також у США діє програма протидії дезінформації, створена Конгресом США. В рамках цієї програми фінансуються дослідження та розробка цифрових інструментів для боротьби з дезінформацією, а також проводяться навчальні заходи для журналістів та громадськості.

Крім того, уряд США співпрацює із соціальними мережами та іншими онлайн-платформами з метою виявлення та вилучення дезінформаційного контенту, який може загрожувати національній безпеці.

Оскільки не лише США, а й багато інших країн співпрацюють із платформами соціальних мереж з метою виявлення та блокування дезінформаційних повідомлень та акаунтів, доцільним є дослідження цифрових інструментів, що використовуються цими мережами.

Зокрема, Facebook використовує кілька цифрових інструментів для боротьби з дезінформацією на своїй платформі, включаючи алгоритми машинного навчання для автоматичного виявлення та вилучення недобросовісного контенту; використання перевірених даних, одержаних від незалежних організацій, які спеціалізуються на фактчекінгу, для ідентифікації неправдивої інформації з подальшим її вилученням; рейтингову систему для оцінки якості контенту та надійності джерел; співпрацю з організаціями та експертами з дезінформації для отримання рекомендацій та порад щодо боротьби з дезінформацією на своїй платформі; навчальні програми та курси для користувачів, щоб вони могли краще розуміти, як розпізнавати фейки та не піддаватися дезінформації.

Зазначимо, що Facebook відносить до ненадійного контенту не лише дезінформацію. Зокрема, йдеться про систему виявлення підбурювання: Facebook використовує алгоритми для пошуку та видалення контенту, який може призвести до насильства та порушень громадської безпеки. Крім того, використовується система розпізнавання та видалення посилань, які можуть містити віруси, фішингові атаки та інші шкідливі програми. Також Facebook використовує цифрові інструменти для виявлення ненадійних оголошень, які можуть містити шахрайські схеми, фальшиві товари та інші ненадійні практики.

Щодо співпраці з фактчекерами, то Facebook співпрацює на платній основі з фактчекерськими проектами відомих новинних агенцій, таких як Reuters, Associated Press (AP), Agence France-Presse (AFP), а також з

незалежними фактчекерськими організаціями: PolitiFact (США), Maldita (Іспанія), Correctiv (Німеччина) та іншими. Українська версія Facebook співпрацює з фактчекерськими платформами VoxCheck та StopFake. Всі ці організації мають доступ до інструментів Facebook для перевірки фактів та допомагають ідентифікувати і помітити спеціальним знаком неправдиву інформацію на платформі.

Ще одним популярним цифровим інструментом, який допомагає визначати надійність та достовірність облікового запису на Facebook, є рейтингова система. Ця система ґрунтується на алгоритмах машинного навчання, які аналізують поведінку користувачів на платформі та виявляють ознаки недобросовісних дій.

Контент з високим рейтингом вважається більш надійним та буде частіше відображатись у стрічці новин користувачів. Одночасно контент з низьким рейтингом може бути позначений як недостовірний та прихований від більшості користувачів. Негативно на рейтинг можуть вплинути такі фактори, як повторне порушення правил Facebook або використання автоматизованих інструментів (ботів та скриптів).

Варто зазначити, що рейтингова система не є визначальним фактором при видаленні контенту або блокуванні користувачів, але може допомогти Facebook краще розуміти їх поведінку на платформі та вживати заходів для запобігання недобросовісних дій.

Крім того, Facebook пропонує кілька навчальних програм та курсів для користувачів, спрямованих на краще розуміння того, як розпізнавати фейки та боротися з дезінформацією. Зокрема, це створений спільно з університетом Стенфорд та онлайн-платформою edX безкоштовний курс "Стратегії новинної грамотності",що включає модулі з аналізу новинних джерел, визначення фейків та перевірки фактів; онлайновий центр інформаційної грамотності Facebook, який також надає корисні матеріали та ресурси для розпізнавання фейків та дезінформації; бібліотека фото- та відеоматеріалів, яка надає користувачам ресурси, що допомагають

розпізнавати фейкові фотографії та відео; навчальні курси для журналістів та медіа-спеціалістів, що допомагають їм використовувати платформу Facebook для поширення достовірної інформації; регулярні інформаційні кампанії, спрямовані на підвищення рівня інформаційної грамотності користувачів (включають рекламні оголошення, статті та інші матеріали, які допомагають розпізнавати фейки та боротися з дезінформацією; співпраця з урядами, некомерційними організаціями та іншими зацікавленими сторонами для протидії дезінформації та підвищення рівня інформаційної грамотності населення.

Багато з перерахованих цифрових інструментів активно використовуються іншими платформами. Наприклад, відеохостинг YouTube використовує різноманітні алгоритми машинного навчання для виявлення та видалення недобросовісного контенту, включаючи аналіз метаданих, таких як заголовки, описи та теги, щоб визначити, чи містить відео потенційно недостовірну інформацію; використання алгоритмів розпізнавання зображень та мови для аналізу змісту відео- та аудіоконтенту, щоб визначити його добросовісність; аналіз кількості переглядів, коментарів та лайків, що допомагає визначити, наскільки відео може бути популярним та потенційно небезпечним; порівняння відео з базою даних відомих недобросовісних контентів, щоб визначити, чи містить воно потенційно небезпечну інформацію; використання нейронних мереж та алгоритмів класифікації для навчання своїх алгоритмів на основі великих обсягів даних.

Крім цього, YouTube співпрацює із зовнішніми перевіреними фактчекерами, такими як Snopes, FactCheck.org та PolitiFact, які можуть перевіряти та розміщувати інформацію на сторінках з результатами пошуку, якщо відео або зміст на каналі були спростовані. Якщо відео містить суперечливий контент, то YouTube може запропонувати користувачеві посилання на фактчекера для більш детальної інформації. Крім того, самі користувачі можуть повідомляти YouTube про контент,

який може містити дезінформацію та формувати запитати його перевірки, використовуючи функцію "Поскаржитися" (Report) під відео.

Серед інших заходів протидії дезінформації, YouTube також посилив правила розміщення реклами на своїй платформі, щоб уникнути її появи поруч з недостовірним контентом. Крім того, YouTube надає інструменти, які дозволяють рекламодавцям керувати тим, де буде розміщена їх реклама, щоб захистити свої бренди від небажаних асоціацій з ненадійним контентом.

Рекламодавці можуть скористатися функцією "Управління площинами" (site exclusion) на платформі YouTube, щоб вилучити зі списку допустимих ресурсів певні канали, відео або категорії відео, на яких вони не бажають розміщувати свою рекламу.

Таким чином, можна стверджувати, що алгоритми машинного навчання є важливою частиною системи боротьби з дезінформацією та недобросовісним контентом на онлайн-платформах. Наприклад, у звіті Facebook за 2020 рік було відзначено, що за допомогою автоматичного виявлення вдалося видалити більше 95% недобросовісного контенту до того, як користувачі змогли його помітити та повідомити про це. Аналогічні показники були відзначені і на YouTube.

Використання алгоритмів машинного навчання також може значно підвищити ефективність державних структур, задіяних у моніторингу інформаційного простору з метою виявлення та аналізу дезінформації для запобігання її поширенню.

Наприклад, розвиток технологій машинного навчання та штучного інтелекту надав нові можливості для створення ефективних алгоритмів, здатних автоматично виявляти дезінформацію в текстах, зображеннях та відео. Це дозволяє значно зменшити час і зусилля, що необхідні для ручного аналізу та видалення дезінформації. Зазначимо, що найбільш поширеним та ефективним методом машинного навчання є нейронні мережі. Вони імітують роботу нервової системи людини і складаються з

багатьох взаємопов'язаних "нейронів", які обробляють інформацію та передають її далі по мережі.

Нейронні мережі використовуються для обробки та аналізу даних, включаючи текст, зображення та звук. Вони можуть бути навчені виявляти залежності та шаблони в даних, а потім використовувати ці знання для вирішення завдань.

Одним з типів нейронних мереж, які можуть бути використані для виявлення дезінформації, є рекурентні нейронні мережі (RNN). Вони особливо добре підходять для аналізу тексту, оскільки дозволяють враховувати контекст та послідовність слів у реченні або абзаці.

Проте, як і будь-який інший метод виявлення дезінформації, нейронні мережі також мають свої обмеження. Вони можуть допускати помилки та надавати хибні результати, особливо якщо навчені на недостатньо великому та різноманітному наборі даних. Крім того, вони не можуть враховувати контекст поза текстом, зокрема, контекст соціального середовища або політичної обстановки.

Для більш точного виявлення дезінформації можна використовувати аналізатор соціальних мереж. Це програмне забезпечення дозволяє автоматично збирати, обробляти та аналізувати дані, пов'язані з поведінкою користувачів у соціальних мережах. Воно використовується для вивчення настроїв у суспільстві, автоматичного відстеження тенденцій щодо формування громадської думки у соціальних мережах та інших подібних завдань.

У свою чергу, аналітика даних також може відігравати важливу роль у боротьбі з дезінформацією. Аналіз даних може показати, які теми та повідомлення привертають найбільшу увагу в Інтернеті та соціальних мережах, що може допомогти державним органам краще зрозуміти, як дезінформація поширюється, та що можна зробити, щоб запобігти цьому.

Розглянемо згадані інструменти детальніше.

Одним з найпоширеніших підходів для виявлення дезінформації є аналіз контенту на наявність певних характеристик. Наприклад, деякі ознаки можуть свідчити про те, що стаття або пост з великою вірогідністю містить дезінформацію.

Зокрема, на це може вказувати використання заголовків-приманок. Під ними розуміються такі заголовки новинних статей, які спонукають читача перейти на сторінку з новиною, але насправді не відповідають її змісту. Такі заголовки можуть бути використані для поширення дезінформації, оскільки вони привертають увагу користувачів та можуть змусити їх повірити неправдивій інформації.

Алгоритми машинного навчання можуть бути використані для виявлення таких заголовків-приманок. Спеціальна програма може аналізувати структуру та зміст заголовків, порівнювати їх зі змістом статті та виділяти неправдиві заголовки. Для цього можуть використовуватись такі методи, як аналіз тональності, семантичний аналіз та порівняння змісту заголовка зі змістом статті.

Однак варто пам'ятати, що хоча виявлення заголовків-приманок є важливим завданням для боротьби з дезінформацією, використання алгоритмів машинного навчання для їх виявлення не є універсальним рішенням і має поєднуватися з іншими методами. Так, серед головних ознак дезінформації необхідно виділити наявність певних ключових слів або фраз.

Деякі ключові слова або фрази можуть використовуватися для виявлення дезінформації шляхом аналізу текстового контенту. Аналізатор може використовувати алгоритми машинного навчання або правила для пошуку цих ключових слів або фраз в тексті.

У свою чергу, ключові слова можуть бути пов'язані з певними темами, подіями або джерелами дезінформації. Наприклад, під час військового конфлікту певні слова та фрази, пов'язані з політичною пропагандою, можуть використовуватися для виявлення дезінформації, яка

намагається маніпулювати громадською думкою щодо доцільності проведення бойових дій для захисту своєї території.

Однак визначення ключових слів і фраз для виявлення дезінформації може бути складним процесом, який вимагає детального аналізу теми, подій або контексту. Ось кілька рекомендацій, які можуть допомогти правильно визначити ключові слова та фрази для виявлення дезінформації: 1) Вивчайте тему, подію або контекст, щоб зрозуміти, які ключові слова та фрази можуть бути пов'язані з дезінформацією. Це може передбачати вивчення новин, соціальних медіа, форумів та інших джерел. 2) Складіть список слів та фраз, які можуть бути пов'язані з дезінформацією. Це можуть бути слова та фрази, які використовують дезінформатори для обману цільової аудиторії. 3) Використовуйте інструменти аналізу даних та машинного навчання, щоб виявити найбільш вживані слова та фрази, пов'язані з темою, подією або контекстом. Такі інструменти можуть забезпечити більш точне визначення ключових слів та фраз. 4) Оновлюйте список ключових слів та фраз, щоб відповідати новим тенденціям та методам дезінформації. Це допоможе покращити точність виявлення дезінформації.5) Працюйте з експертами в конкретній області, щоб отримувати їх поради та рекомендації щодо визначення ключових слів та фраз для виявлення дезінформації. Це може включати співпрацю з дослідниками, журналістами, правозахисниками та іншими експертами в галузі інформаційної безпеки. 6) Враховуйте контексти. Деякі ключові фрази та слова можуть бути менш ефективними, якщо їх використовувати відокремлено від контексту. Тому важливо враховувати їх взаємодію зі словами, які йдуть перед або після них. 7) Аналізуйте дані про попередні випадки дезінформації, що може допомогти виявити найбільш ефективні ключові слова та фрази, які використовувалися раніше. Це допоможе визначити тенденції та зміни в використанні мови дезінформації та оновлювати набір ключових слів та фраз відповідним чином.

В цілому, правильне визначення ключових слів та фраз для виявлення дезінформації – це мистецтво, яке потребує як технічної, так й інтуїтивної експертизи. Водночас, це процес, який вимагає постійного оновлення та вдосконалення, оскільки дезінформація постійно еволюціонує, і нові способи її поширення можуть з'являтися щодня [50].

Крім того, використання ключових слів та фраз для пошуку дезінформації може бути обмежене у зв'язку з тим, що неправдива та маніпулятивна інформація може поширюватися у різних формах та не завжди містить явні ключові слова або фрази. Тому крім прямих ключовиків також необхідно звертати увагу на наявність у новинних повідомленнях певних формулювань. Побудовані певним чином окремі фрази та загальні стилі письма можуть використовуватися для виявлення дезінформації, особливо в контенті, що поширюється в соціальних мережах. Для цього можна використовувати методи аналізу тональності тексту, аналізу емоційного забарвлення, аналізу лексики та граматики.

Наприклад, дезінформаційні тексти часто містять твердження, що не підтверджуються фактами, але написані яскраво-емоційним способом з використанням провокаційних заголовків. Такі тексти також можуть використовувати різні лінгвістичні трюки, такі як використання слів з подвійним значенням або гіперболічних висловлювань, щоб викликати у читача певні почуття та переконати його прийняти недостовірну інформацію. Це може включати в себе використання сильних емоційних слів, таких як "жахливий", "жахаючий", "шокуючий" тощо, які можуть створювати неправильне враження про серйозність джерела та призводити до поширення дезінформації. Тому при аналізі тексту слід звертати увагу на використання емоційних слів та оцінювати, як вони можуть впливати на сприйняття інформації.У процесі навчання алгоритми можуть використовувати велику кількість розмічених даних, щоб навчитися виявляти дезінформацію з високою точністю.

Ці методи можуть допомогти виявити приховані значення та підходи, які використовуються авторами дезінформації, хоча необхідно пам’ятати, що не всі тексти, написані в емоційному ключі, є дезінформацією. Тому для виявлення ознак дезінформації також використовуються методи машинного навчання, такі як алгоритми класифікації, які дозволяють розбивати набори даних на категорії або класи. Наприклад, вони можуть розподілити тексти на дві категорії: дезінформація та не-дезінформація. Класифікатор використовує ці дані для визначення, який клас належить новому тексту на основі його ознак, таких як наявність певних ключових слів або фраз, стиль письма тощо.

Прикладом алгоритмів класифікації, які можуть використовуватися для виявлення дезінформації є метод опорних векторів (SVM). Це один з найбільш поширених методів машинного навчання, який використовується для класифікації даних. Він використовує принцип розділення гіперплощиною багатовимірного простору, що дозволяє розбити вибірку на два класи.

Метод опорних векторів (SVM) будує гіперплощину, яка розташовується якомога далі від найближчих точок кожного класу (ці точки називаються опорними векторами). Для визначення оптимальної гіперплощини у SVM використовується метод оптимізації, що максимізує відстань між гіперплощиною та найближчими точками кожного класу.

SVM широко використовується для класифікації текстових даних у різних галузях та може бути застосований для виявлення дезінформації в текстових даних. Для цього необхідно попередньо обробити текст та вилучити з нього ознаки, які можна використовувати для класифікації, наприклад, наявність ключових слів, стилістика тощо.

SVM має декілька переваг, включаючи хорошу точність класифікації, здатність працювати з великими обсягами даних та обробляти дані з високою розмірністю. Однак, він також має деякі

недоліки, зокрема складність у налаштуванні параметрів та можливість перенавчання на певних типах даних.

Тож один з додаткових методів моніторингу інформаційного поля полягає у виявленні використання сумнівних джерел. Сумнівні джерела можуть допомогти виявити дезінформацію, оскільки часто інформація, що не відповідає дійсності, поширюється через неперевірені та ненадійні джерела, які можуть мати приховані мотиви або недостатній рівень експертизи. Дослідження таких джерел може виявити їх зв'язок з конкретними групами або інтересами.

Крім того, для підтвердження або спростування достовірності інформації можна провести додаткову перевірку альтернативних джерел. Якщо інформація не підтверджується іншими незалежними джерелами, це може свідчити про те, що вона є дезінформацією.

Серед інших підходів, які використовуються для виявлення дезінформації, можна виділити дослідження соціальних мереж. Цей метод базується на тому, що дезінформація часто поширюється через соціальні мережі, такі як Facebook, Twitter, Instagram, і може викликати певні реакції у користувачів. Наприклад, деякі люди можуть почати обговорювати і поширювати фейкові новини, що може призвести до певних паттернів активності в соціальній мережі.

Аналізатор соціальних мереж - це інструмент, який дозволяє аналізувати таку активність. Він може бути використаний в різних аспектах, таких як політичний маркетинг і реклама, пропагандистські кампанії, наукові дослідження тощо. Цей метод також широко використовується з комерційною метою – він може допомогти компанії дізнатися, як користувачі ставляться до її товарів і послуг, які теми і тренди обговорюються в соціальних мережах, які думки і відгуки публікують споживачі.

Водночас, аналізатор соціальних мереж може допомогти державним структурам відстежувати інформацію, яка поширюється в соціальних

мережах і потенційно може бути дезінформацією. За допомогою аналізу ключових слів, хештегів та інших факторів можна автоматично визначати повідомлення, які можуть містити дезінформацію.

Додатково, аналізатор соціальних мереж може допомогти оцінити масштаб дезінформації у соціальних мережах, щоб зрозуміти, наскільки вона поширена. Аналізатор може відслідковувати обсяг повідомлень, що містять певні ключові слова або фрази, і аналізувати їх зміст, щоб визначити, наскільки вони відповідають фактам.

Крім того, аналізатор може відстежувати повідомлення, які містять певні ключові слова, і аналізувати профілі користувачів, щоб визначити, хто їх публікує.

Спочатку необхідно отримати дані, наприклад, дані з соціальних мереж. Потім необхідно провести аналіз та визначити основні вузли мережі та їх взаємодії. У ролі вузлів можуть виступати користувачі соціальних мереж, групи, сторінки, а також хештеги, згадки та посилання.

Для аналізу мережевої структури можна використовувати метрики, такі як центральність, коефіцієнт кластеризації та діаметр графа. Наприклад, центральність може допомогти виділити ключових гравців в мережі, які можуть бути пов'язані з поширенням дезінформації.

Для виявлення дезінформації можна використовувати методи машинного навчання в поєднанні з SNA. Наприклад, можна використовувати класифікатори, такі як SVM, для визначення того, чи є певна інформація дезінформацією, чи ні. Потім можна використовувати SNA для аналізу мережевих зв'язків цих інформаційних елементів, щоб визначити джерела дезінформації та її поширювачів.

Це програмне забезпечення може допомогти державним структурам оцінити ефективність заходів, спрямованих на протидію дезінформації. Аналізатор може відстежувати обсяг повідомлень, що містять певні ключові слова, до та після проведення відповідних заходів, щоб визначити, наскільки вони були ефективними.

Необхідно зазначити, що в цілому метод аналізу соціальної мережі може бути дуже корисним, оскільки він дозволяє аналізувати інформаційну взаємодію та виявляти ключових гравців, пов'язаних з поширенням дезінформації. Однак аналізатор соціальних мереж, як і будь-який інший алгоритм машинного навчання, не є універсальним рішенням, оскільки він може допускати помилки та ложні спрацьовування, що може призвести до неправомірного блокування контенту.

Наприклад, алгоритми можуть неправомірно блокувати легітимний контент, який не є дезінформацією, але містить ключові слова або фрази, які алгоритм пов'язує з дезінформацією.

Окремою проблемою є блокування контенту через неможливість визначення чіткої межі між дезінформацією та свободою слова. Автори контенту можуть використовувати терміни, які можна розглядати і як дезінформацію, і як право на свободу висловлювання власних поглядів [55]. У таких випадках алгоритми можуть неправомірно блокувати контент.

Також алгоритми можуть блокувати контент на основі суб'єктивних оцінок. Наприклад, якщо алгоритм налаштований на блокування контенту, пов'язаного з політичними кампаніями, він може неправомірно блокувати контент, який не є дезінформацією, але пов'язаний з політикою.

Крім того, дезінформація може бути дуже тонко вибудуваною, що ускладнює її виявлення, оскільки існує багато різних способів передати хибну інформацію. Деякі форми спотвореної правди можуть бути дуже добре замасковані під правду, особливо якщо така інформація відповідає очікуванням або переконанням цільової аудиторії. Інші форми дезінформації можуть бути більш очевидними та використовувати явні маніпулятивні твердження, але все одно вони також можуть бути ефективними в намаганні дезінформаторів ввести людей в оману.

Крім того, будь-яка інформація може бути суб'єктивною, оскільки вона часто залежить від поглядів, переконань чи інтересів людей, які її

створюють та/або поширюють. Це означає, що одні й ті ж факти можуть тлумачитися по-різному залежно від того, хто їх надає, та з якою метою вони надаються й інтерпретуються. Тому виявлення дезінформації може потребувати не тільки аналізу тексту, а й врахування контексту, тональності та інших факторів, які не завжди можуть бути визначені коректно алгоритмами машинного навчання.

Таким чином, причиною помилкових спрацювань можуть бути недосконаліть алгоритмів та складність визначення межі між дезінформацією та легітимним контентом. Наприклад, деякі ключові слова чи фрази можуть використовуватись як в дезінформації, так і в легітимному контенті.

Крім того, помилкові спрацювання можуть бути спричинені зміною формату та стилю дезінформації. Деякі дезінформаційні кампанії можуть змінювати свої методи та стилі, щоб обійти алгоритми виявлення, що ще більш ускладнює протидію дезінформації.

Для зниження рівня помилкових спрацювань використовуються різні підходи. Одним з таких підходів є використання комбінації різних методів машинного навчання, таких як SVM (Support Vector Machines), керуючі (рішучі) дерева та нейронні мережі. Цей підхід, коли різні алгоритми об’єднуються в один, називається ансамблевим навчанням, що може допомогти підвищити точність класифікації та знизити кількість помилкових спрацювань.

Також важливо постійно покращувати алгоритми та методи виявлення дезінформації на основі нових даних та досвіду роботи з ними.

Необхідно зауважити, що сам вибір програмного забезпечення (ПЗ) для державних структур, що займаються протидією дезінформації, може бути складним процесом, оскільки вимоги до таких програмних засобів можуть відрізнятися в залежності від конкретної ситуації та завдань, які необхідно вирішити. Однак, при виборі програмного забезпечення для виявлення дезінформації рекомендується враховувати наступні фактори: 1)

Функціональність: необхідно вибрати ПЗ, яке підтримує аналіз великого обсягу даних з різних джерел, включаючи соціальні мережі, новинні сайти, форуми тощо. Важливо, щоб програма могла обробляти текстові дані на різних мовах. 2) Автоматизація: обов'язково потрібно вибрати програмне забезпечення, яке дозволяє автоматизувати процес виявлення дезінформації, щоб скоротити час аналізу та підвищити точність результатів. 3) Машинне навчання: важливо звернути увагу, чи використовує конкретне ПЗ методи машинного навчання для виявлення дезінформації. Це дозволить програмі автоматично знаходити нові ознаки дезінформації та з часом підвищувати свою точність. 4) Експертна оцінка: також потрібно переконатися, що ПЗ дозволяє включати експертну оцінку в процес аналізу для підвищення точності результатів.

Деякі з популярних програм для виявлення дезінформації включають Emergent, Hoaxy, Botometer та Factmata. Однак, перш ніж зробити вибір, важливо, щоб державна структура, крім перерахованих факторів, також визначила свої потреби та цілі у сфері протидії дезінформації. Наприклад, якщо основною метою є відстеження та аналіз соціальних мереж, то необхідно обирати ПЗ, яке спеціалізується на цьому виді діяльності.

Також необхідно переконатися, що обране програмне забезпечення може бути інтегроване з іншими системами та інструментами, що використовуються в роботі.

При виборі ПЗ для державних структур, необхідно враховувати питання безпеки та конфіденційності даних, тому важливо обирати програмні засоби, які забезпечують високий рівень безпеки та захисту даних [52].

Технічна підтримка є важливим критерієм при виборі програмного забезпечення. Державні структури повинні переконатися, що в обраного ПЗ є команда підтримки, яка може швидко реагувати на виниклі проблеми та запитання.

Крім того, при виборі програмного забезпечення слід враховувати фінансові можливості організації. Деякі рішення можуть бути дорогими та вимагати значних витрат на навчання персоналу, технічну підтримку й оновлення. Тому важливо визначити, які інструменти максимально відповідають бюджету та можливостям організації.

Отже, підсумовуючи все вищевикладене, можемо стверджувати, що в сучасному світі цифрові інструменти відіграють все більшу роль у боротьбі з недостовірною інформацією, особливо в контексті розробки державної політики у сфері протидії дезінформації.

Завдяки використанню цифрових інструментів можна значно пришвидшити та підвищити ефективність процесу виявлення й аналізу дезінформації та запобігання її поширенню. До таких інструментів належать, зокрема, машинне навчання, аналіз соціальних мереж, алгоритми класифікації та методи аналізу даних.

Однак, незважаючи на всі переваги використання цифрових інструментів, необхідно враховувати, що вони можуть допускати помилки, тому потрібен комплексний підхід, який включає експертну оцінку, аналіз соціально-політичного контексту та співпрацю з журналістами, громадськими організаціями та іншими зацікавленими сторонами. Це може допомогти збалансувати роботу алгоритмів та зменшити кількість помилкових сигналів.

Також варто зазначити, що використання цифрових інструментів потребує певних знань та навичок, а також доступу до необхідних даних. Тому при виборі програмного забезпечення та технологій необхідно враховувати фінансові можливості та вибирати ПЗ, яке найкращим чином відповідає потребам державних структур.

В цілому, можна зробити висновок, що використання цифрових інструментів є необхідним компонентом державної політики у сфері протидії дезінформації, оскільки їх правильне застосування може значно

удосконалити процес протидії цьому явищута бути корисним для розробки ефективних стратегій у цьому напряміу довгостроковій перспективі.

Висновки до розділу 3

В третьому розділі запропоновано конкретні заходи, спрямовані на вдосконалення механізмів вироблення державної політики у сфері протидії дезінформації в умовах цифровізації публічного управління.

Зокрема, розглянуто план заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року в контексті державної політики у сфері протидії дезінформації, що дало змогу виявити ряд недоліків, які полягають у загальності формулювання завдань та недостатній деталізації (конкретизації) заходів, необхідних для досягнення поставлених цілей, окрім цього визначено лише узагальнені показники реалізації та не встановлено точних строків (проміжних термінів) щодо окремих етапів їхнього виконання. Надано рекомендації щодо вдосконалення плану заходів з реалізації Стратегії інформаційної безпеки в контексті протидії дезінформації, що включають:

– деталізацію загальних завдань шляхом конкретизації дій та заходів, необхідних для досягнення поставлених цілей. Забезпечити ефективну координацію та співпрацю між різними державними структурами та організаціями, що залучені до виконання Плану заходів;

– розмежування функцій Центру протидії дезінформації при РНБО України, відповідального за стратегічну координацію комунікації урядових структур, і Міністерства культури та інформаційної політики України як центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері для здійснення ефективної координації та співпраці між різними суб’єктами публічного управління, що залучені до виконання Плану заходів;

– розроблення протоколів обміну інформацією та узгодження спільних дій і заходів, спрямованих на протидію інформаційним загрозам;

– встановлення показників успішності, які дозволять оцінити ефективність проведених заходів та виявити потребу у доопрацюваннях;

– впровадження механізмів постійного моніторингу, контролю та оцінювання результативності проведених заходів у сфері протидії дезінформації, що дозволить своєчасно виявляти потребу у внесенні змін, визначати успішні практики та проблемні аспекти, які потребують додаткової уваги;

– унормування (розроблення та затвердження) алгоритму протидії дезінформації в умовах розвитку цифрового суспільства з конкретизацією необхідних заходів, що сприятиме забезпеченню державних структур сучасними технологіями та аналітичними інструментами аналізу інформаційних загроз та запобігання їхнього впливу.

Також здійснено порівняльний аналіз концептуальних та практичних підходів в США та ЄС щодо розв’язання проблеми протидії дезінформації, а також розглянуто можливість їх адаптації в Україні. На основі проведеного аналізу та з урахуванням сучасних умов й потенціалу цифрового розвитку України розроблено рекомендації щодо удосконалення нормативно-правового забезпечення у сфері протидії дезінформації шляхом необхідності створення окремого законопроекту, в якому регулюватимуться процеси виявлення та запобігання її поширенню, а також передбачається: розширення повноважень та зміцнення матеріально-технічної бази Центру протидії дезінформації при РНБО України як керівного ядра інституціонального механізму вироблення державної політики у сфері протидії дезінформації; встановлення адміністративної та кримінальної відповідальності за створення та поширення дезінформації; запровадження інституту уповноваженого з питань інформації. Окрім цього рекомендовано нормативно врегулювати

запровадження навчальних модулів, курсів та програм з опануваннях нових знань, умінь та навичок з критичного мислення, медіаграмотності та цифрової гігієни.

Обґрунтовано необхідність застосування цифрових інструментів протидії дезінформації для забезпечення результативної співпраці суб'єктів публічного управління через створення єдиної системи раннього виявлення дезінформації та запобігання її поширенню, що сприяє інноваційним підходам та побудові ефективних взаємодій між усіма учасниками комунікативного процесу. Доведено, що у подальшому повсюдне використання цифрових інструментів дозволить виявляти, класифікувати та перевіряти (практично безперервно) в режимі онлайн великі обсяги даних та канали їх поширення, на основі цього рекомендовано:

– Міністерству культури та інформаційної політики України забезпечити розробку та реалізацію цілісної й координованої програми розвитку цифрових каналів управління стратегічними комунікаціями для оперативного забезпечення населення достовірною інформацією в достатньому обсязі, а також для налагодження взаємодії з міжнародними партнерами у сфері захисту національних інтересів в інформаційному просторі;

– Центру протидії дезінформації при РНБО України розвивати партнерські відносини з онлайн-медіа та провайдерами цифрових платформ з метою виявлення ними дезінформаційного контенту та його блокування;

– Міністерству цифрової трансформації України: створити та постійно оновлювати репозитарій цифрових інструментів (програмного забезпечення) з урахуванням потреб технологічного розвитку та актуальних методів поширення дезінформації, а також сформувати державну цифрову платформ для обміну даними між органами публічної влади, задіяними у боротьбі з поширенням дезінформації; забезпечити

співпрацю з технологічними компаніями, стартапами та інноваційними організаціями, що спеціалізуються на розробці алгоритмічних фільтрів та інших інструментів для виявлення та протидії дезінформації, що сприятиме появі нових технологій та інструментів у цій сфері;

– Міністерству освіти і науки України, вищим навчальним закладам: запровадити освітньо-професійні програми другого (магістерського) рівня освіти за спеціальністю 281 «Публічне управління та адміністрування» для опанування цифрових навичок з управління стратегічними комунікаціями, розробити та постійно проводити короткострокові курси підвищення кваліфікації та тренінги з питань протидії дезінформації для державних службовців та посадових осіб місцевого самоврядування.

Запропоновано органам влади на національному, регіональному та місцевому рівнях активно використовувати цифрові інструменти збору, аналізу та візуалізації даних щодо захисту інформаційного простору України, включаючи використання алгоритмів машинного навчання та штучного інтелекту з метою автоматизованого виявлення, класифікації та аналізу дезінформації.

Основні результати розділу 3 опубліковано в наукових працях автора: [50, 52, 54, 55].

ВИСНОВКИ

У дисертації вирішено нове наукове завдання, яке полягає в теоретичному обґрунтуванні механізмів вироблення державної політики у сфері протидії дезінформації та наданні практичних рекомендацій щодо їх вдосконалення в умовах цифровізації публічного управління. В результаті проведеної роботи досягнута її мета та розв'язані всі поставлені завдання, що дозволило зробити такі узагальнюючі висновки:

1. Уточнено понятійно-категорійний апарат науки державного управління у сфері протидії дезінформації, зокрема на основі виокремлених ознак (хибність, зловмисність, цілеспрямованість, наявність стратегічної мети та бажаний наслідок впливу) запропоновано авторське тлумачення дезінформації, під якою у подальших дослідженнях запропоновано розуміти створення та поширення з політичною чи іншою стратегічною метою завідомо хибної чи свідомо модифікованої інформації як істинної для інформаційно-психологічного впливу на об'єкт з метою формування в нього помилкового уявлення про реальність та підштовхування до певних дій чи бездіяльності з метою завдання шкоди інтересам людини, суспільства і держави. Констатовано, що до дезінформації слід відносити як самі хибні відомості, так і процес їх поширення, що може мати різні форми, методи та канали комунікації. На основі проведеного аналізу різних підходів до формулювання терміну «інформаційна війна» запропоновано його узагальнене визначення як процес використання інформаційних технологій та медіа-ресурсів з метою впливу на інформаційну безпеку та соціальну стабільність країни, проти якої така війна ведеться. Обґрунтовано недоцільність його заміни в офіційних документах на термін «спеціальні інформаційні операції», оскільки термін «інформаційна війна» охоплює більш широкий спектр діяльності, пов'язаної з використанням інформаційних засобів і методів для досягнення стратегічної мети. З урахуванням цього рекомендується

зберегти термін «інформаційна війна» для загального опису явищ в інформаційному просторі, тоді як термін «спеціальні інформаційні операції» можна використовувати для позначення конкретних дій, обмежених у часі і цілях. Доведено, доцільність подальшого використання зазначених дефініцій у нормативно-правових документах України, які регулюють інформаційну сферу, що дозволить встановити єдині правила і принципи дій для всіх учасників процесу, сприяти ефективній протидії дезінформації, а також стати основою для подальших наукових розробок, спрямованих на удосконалення механізмів вироблення державної політики у сфері протидії дезінформації.

2. Встановлено чинники (фактори), що впливають на збільшення швидкості поширення дезінформації комунікативними каналами у публічній сфері, а саме: здатність емоційно зарядженого й контраверсійного контенту активно розповсюджуватися подібно до поширення вірусу в біологічній системі; вплив когнітивного спотворення, прагнення підтвердження власних переконань, емоційна залежність психіки людини від соціальних мереж; таргетування (алгоритми рекомендацій) соціальних мереж, що впливають на відображення певного контенту в новинній стрічці користувачів; використання анонімних (псевдоанонімних) фейкових акаунтів та ботів. Запропоновано алгоритм протидії дезінформації в умовах розвитку цифрових трансформацій, який складається з п’яти основних етапів: визначення потенційних загроз та вироблення стратегії державної політики протидії дезінформації; захист від поточних загроз шляхом впровадження механізмів фільтрації та перевірки інформації, підвищення інформаційної грамотності та вдосконалення заходів захисту від кібератак; виявлення дезінформаційних інцидентів в режимі реального часу; оперативне та ефективне реагування на такі інциденти; здійснення заходів з відновлення стабільності та оцінка результатів.

Для удосконалення існуючих державних механізмів протидії швидкому поширенню дезінформації рекомендовано: досягти балансу між індивідуальними інформаційними свободами та захистом національних інтересів держави, зокрема, доцільно розглянути можливість врегулювання діяльності анонімних онлайн-ресурсів з метою ефективного припинення системного та безкарного поширення в інтернет-просторі недостовірної та маніпулятивної інформації, спрямованої проти національних інтересів України; сформувати правову базу, яка забезпечить ефективний захист від загроз в інформаційному просторі; створити інтегровану систему раннього виявлення загроз за допомогою технологій штучного інтелекту, машинного навчання, аналізу даних та цифрових сервісів; створити дієві механізми співпраці та обміну інформацією між різними суб'єктами провадження інформаційної безпеки (органами влади, громадськими організаціями і приватним сектором).

3. Розроблено модель інституціонального механізму вироблення державної політики у сфері протидії дезінформації на стратегічному, тактичному та операційному рівнях для забезпечення ефективного та координованого реагування підрозділів органів влади на маніпулятивні та фальсифікативні загрози, що базується на взаємодії суб’єктів публічного управління (стратегічних, регуляторних, комунікативних, гуманітарних; юридичних, наукових) у процесі реалізації комплексу організаційно-функціональних заходів згідно зон їх відповідальності на основі: *факторів* (політичний контекст; інформаційна культура; технологічний розвиток; роль громадянського суспільства; вплив медіа; міжнародна співпраця; фінансові ресурси; стратегічне партнерство); *стратегій* (реалізації заходів захисту; здійснення моніторингу, аналізу та оцінювання ризиків; реагування та здійснення контрдій); *принципів* (комунікативності, захищеності, координованості, доказовості, прозорості, відкритості, задіяності та адаптивності); *методів/засобів збору та поширення контенту* (моніторингу медіа та соціальних мереж; аналітичних

інструментів; експертної оцінки; публічних кампаній; спеціальних комісій та агентств; міжнародного співробітництва; законодавчих ініціатив); *інструментів реагування на загрози* (стратегічне планування; аналітичні дослідження; нормативне регулювання; інформаційний моніторинг; освітні програми; партнерська співпраця; інформаційна мобілізація; координаційні заходи); *співпраці* (формування спеціалізованих робочих груп та комітетів; проведення регулярних нарад; здійснення обміну інформацією; створення спільних програм і проєктів; здійснення кризової координації; розробка спільних стратегій) та *партнерської взаємодії* (залучення партнерських програм з громадянським суспільством та міжнародних проєктів; застосування публічно-приватного партнерства; проведення консультацій з експертами; організація форумів та робочих група); *ресурсів* (фінансових, людських і технічних).

Запропоновано шляхи розвитку інституціонального механізму вироблення державної політики у сфері протидії дезінформації, зокрема:

– поліпшення координації дій між Центром протидії дезінформації при РНБО України і профільними органами державної влади та іншими зацікавленими суб’єктами публічного управління;

– оптимізація використання фінансових, людських і технічних ресурсів із залученням партнерської взаємодії з громадськими організаціями, приватним сектором та міжнародними партнерами для спільної реалізації проектів і програм;

– оновлення нормативно-правової бази з урахуванням сучасних викликів, загроз, ризиків та впливу цифрових технологій у сфері протидії дезінформації;

– забезпечення широкого доступу громадськості до достовірної інформації та підвищення інформаційної грамотності населення.

4. Розглянуто план заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року в контексті державної політики у сфері

протидії дезінформації, що дало змогу виявити ряд недоліків, які полягають у загальності формулювання завдань та недостатній деталізації (конкретизації) заходів, необхідних для досягнення поставлених цілей, окрім цього визначено лише узагальнені показники реалізації та не встановлено точних строків (проміжних термінів) щодо окремих етапів їхнього виконання. Констатовано, що суттєва затримка у затвердженні Плану заходів негативно позначилася на повноті, ефективності та результативності виконання передбачених завдань. Надано рекомендації щодо вдосконалення плану заходів з реалізації Стратегії інформаційної безпеки в контексті протидії дезінформації, що включають:

– деталізацію загальних завдань шляхом конкретизації дій та заходів, необхідних для досягнення поставлених цілей. Забезпечити ефективну координацію та співпрацю між різними державними структурами та організаціями, що залучені до виконання Плану заходів;

– розмежування функцій Центру протидії дезінформації при РНБО України, відповідального за стратегічну координацію комунікації урядових структур, і Міністерства культури та інформаційної політики України як центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері для здійснення ефективної координації та співпраці між різними суб’єктами публічного управління, що залучені до виконання Плану заходів;

– розроблення протоколів обміну інформацією та узгодження спільних дій і заходів, спрямованих на протидію інформаційним загрозам;

– встановлення показників успішності, які дозволять оцінити ефективність проведених заходів та виявити потребу у доопрацюваннях;

– впровадження механізмів постійного моніторингу, контролю та оцінювання результативності проведених заходів у сфері протидії дезінформації, що дозволить своєчасно виявляти потребу у внесенні змін,

визначати успішні практики та проблемні аспекти, які потребують додаткової уваги;

– унормування (розроблення та затвердження) алгоритму протидії дезінформації в умовах розвитку цифрового суспільства з конкретизацією необхідних заходів, що сприятиме забезпеченню державних структур сучасними технологіями та аналітичними інструментами аналізу інформаційних загроз та запобігання їхнього впливу.

5. Здійснено порівняльний аналіз концептуальних та практичних підходів в США та ЄС щодо розв'язання проблеми протидії дезінформації, а також розглянуто можливість їх адаптації в Україні. Встановлено, що в країнах з розвинутою демократією державна політика у сфері протидії дезінформації базується на партнерстві між урядом, громадськістю та приватним сектором. Це партнерство проявляється у створенні механізмів саморегулювання для медіа-організацій, активній взаємодії з фактчекінковими організаціями, сприянні розвитку медійної грамотності серед населення, підтримці наукових досліджень у галузі інформаційного захисту та розробці нових цифрових технологій для виявлення недостовірної і маніпулятивної інформації та запобігання її поширенню. На основі проведеного аналізу та з урахуванням сучасних умов й потенціалу цифрового розвитку України розроблено рекомендації щодо удосконалення нормативно-правового забезпечення у сфері протидії дезінформації шляхом необхідності створення окремого законопроекту, в якому регулюватимуться процеси виявлення та запобігання її поширенню, а також передбачається: розширення повноважень та зміцнення матеріально-технічної бази Центру протидії дезінформації при РНБО України як керівного ядра інституціонального механізму вироблення державної політики у сфері протидії дезінформації; встановлення адміністративної та кримінальної відповідальності за створення та поширення дезінформації; запровадження інституту уповноваженого з питань інформації. Окрім цього рекомендовано нормативно врегулювати

запровадження навчальних модулів, курсів та програм з опануванняхнових знань, умінь та навичок з критичного мислення, медіаграмотності та цифрової гігієни.

Ці рекомендації спрямовані на вдосконалення державного управління у сфері протидії дезінформації через оновлення законодавства, що допоможе підвищити скоординованість та ефективність дій усіх зацікавлених сторін та забезпечити ефективне використання ресурсів, сприятиме покращенню захисту громадянських прав та свобод, а також зміцненню демократичних принципів функціонування інформаційного середовища.

6. Обґрунтовано необхідність застосування цифрових інструментів протидії дезінформації для забезпечення результативної співпраці суб'єктів публічного управління через створення єдиної системи раннього виявлення дезінформації та запобігання її поширенню, що сприяє інноваційним підходам та побудові ефективних взаємодій між усіма учасниками комунікативного процесу. Доведено, що у подальшому повсюдне використання цифрових інструментів дозволить виявляти, класифікувати та перевіряти (практично безперервно) в режимі онлайн великі обсяги даних та канали їх поширення, на основі цього рекомендовано органам державної влади у подальшому здійснювати такі практичні заходи як:

– *Міністерству культури та інформаційної політики України*: забезпечити розробку та реалізацію цілісної й координованої програми розвитку цифрових каналів управління стратегічними комунікаціями для оперативного забезпечення населення достовірною інформацією в достатньому обсязі, а також для налагодження взаємодії з міжнародними партнерами у сфері захисту національних інтересів в інформаційному просторі;

– *Центру протидії дезінформації при РНБО України*: розвивати партнерські відносини з онлайн-медіа та провайдерами цифрових

платформ з метою виявлення ними дезінформаційного контенту та його блокування;

– *Міністерству цифрової трансформації України:* створити та постійно оновлювати репозитарій цифрових інструментів (програмного забезпечення) з урахуванням потреб технологічного розвитку та актуальних методів поширення дезінформації, а також сформувати державну цифрову платформ для обміну даними між органами публічної влади, задіяними у боротьбі з поширенням дезінформації; забезпечити співпрацю з технологічними компаніями, стартапами та інноваційними організаціями, що спеціалізуються на розробці алгоритмічних фільтрів та інших інструментів для виявлення та протидії дезінформації, що сприятиме появі нових технологій та інструментів у цій сфері;

– *Міністерству освіти і науки України, вищим навчальним закладам:* запровадити освітньо-професійні програми другого (магістерського) рівня освіти за спеціальністю 281 «Публічне управління та адміністрування» для опанування цифрових навичок з управління стратегічними комунікаціями, розробити та постійно проводити короткострокові курси підвищення кваліфікації та тренінги з питань протидії дезінформації для державних службовців та посадових осіб місцевого самоврядування.

Запропоновано органам влади на національному, регіональному та місцевому рівнях активно використовувати цифрові інструменти збору, аналізу та візуалізації даних щодо захисту інформаційного простору України, включаючи використання алгоритмів машинного навчання та штучного інтелекту з метою автоматизованого виявлення, класифікації та аналізу дезінформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. **Бакуменко, В. Д. (2003). Теоретичні та організаційні засади державного управління. Київ: Міленіум. - 256 с. - С.35**
2. Баран, П. (1958). Логіка національної стратегії. The logic of national strategy. Washington, D.C.: National Defense University
3. Баришполець, О. (2007). Лжеінформація в комунікаційних процесах. Соціальна психологія: Український науково-практичний журнал, Спец. вип., 91-100.
4. Берлач, А.І. (2005). Адміністративне право України: навчальний посібник для дистанційного навчання. Київ: Університет Україна. - 472 с. - С. 75
5. Беспека, В. (2017). Аналогії в американо-російському інформаційному протиборстві в роки "холодних війн" XX та XXI ст. Науковий вісник Східноєвропейського національного університету ім. Лесі Українки. Серія: Історичні науки, 4(353), 103-107.
6. Бєляков, К.І. (2018). Законодавство в секторі інформаційної безпеки: технолого-правовий аналіз. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (с. 14-19). Київ.
7. Богданович, В. Ю., Семенченко, А. І., & Єжеєв, М. Ф. (2008). Методи державного управління забезпеченням національної безпеки у її визначальних сферах: навч. посіб. Київ: НАДУ. (40 с.)
8. Бодріяр, Ж. (2004). Симулякри і симуляція. Переклад з французької В. Ховхун. Київ: Видавництво Соломії Павличко "Основи". ISBN 966-500-189-2.
9. Брайчевський, С. М. (2011). Дезінформація як нелінійний ефект взаємодії інформаційних тематичних потоків. Інформація і право, (2), 91-97. URL: http://nbuv.gov.ua/UJRN/Infpr_2011_2_16.

10. Великий тлумачний словник сучасної мови. Дезінформація. URL: https://slovnyk.me/search?term=%D0%B4%D0%B5%D0%B7%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F
11. Вендлінг, М. (2018). Історія "фейкових новин". ВВС Україна. URL: https://www.bbc.com/ukrainian/features-42786093
12. Верголяс, О.О. (2020). Правове забезпечення спеціальних інформаційних операцій: дис. к.ю.н. : спеціальність 12.00.07. Київ: НДІІП НАПрН України
13. Вісник НАТО. (2021). Боротьба з дезінформацією: зміцнення цифрової стійкості Альянсу. URL: https://www.nato.int/docu/review/ru/articles/2021/08/12/bor-ba-s-dezinformatsiej-ukreplenie-tsifrovoj-ustojchivosti-severoatlanticheskogo-soyuza/index.html
14. Волошина, Н.М. (2010). Поняття "безпека інформації" та "інформаційна безпека" в сучасному науковому просторі. Сучасні інформаційні технології у сфері безпеки та оборони, № 2, 53-56.
15. Ганяк, В.Й. (2017). Політичні механізми у процесі вироблення державної політики у сфері свободи совісті й релігії: безпековий вимір. Інвестиції: практика та досвід, 7, 110.
16. Гібридна війна: in verbo et in praxi: монографія / під. заг. ред. проф. Р.О. Додонова. Вінниця: ТОВ «Нілан-ЛТД», 2017.
17. Гладун, Ю.Я., & Ліпенцев, А.В. (2016). Побудова типового центру забезпечення публічної безпеки на прикладі ситуаційного центру Головного Управління Національної поліції у Львівській області. Ефективність державного управління, 4, 119-128.
18. Глобальна та національна безпека: підручник / авт. кол. :В..І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та ін. / за заг. ред. Г.П.Ситника. – Київ : НАДУ, 2016. – 784 с. - С.109.

19.28. Гогвуд, Б.В., & Ган, Л.А. (2004). Аналіз політики для реального світу. К.: Вид-во Соломії Павличко "Основи".

20. Горбатюк, О.М. (1999). Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. Вісник Київського університету імені Т. Шевченка, Вип.14: Міжнародні відносини, 46-48.

21. Горбулін, В.П. (2009). Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. К.: Інтертехнологія.

22. Горбулін, В.П., & Качинський, А.П. (2009). Засади національної безпеки України. К.: Інтертехнологія.

23. Гребенюк, М.В., & Леонов, Б.Д. (2019). Проблеми протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів: аналіз досвіду ЄС. Інформація і право, № 2, 82-89. URL: http://nbuv.gov.ua/UJRN/Infpr_2019_2_11

24. Громадська організація “Інформаційно-аналітичний центр “Громадський Простір”. (2021). Протидія дезінформації: європейські підходи та стандарти [Онлайн-семінар]. Організовано спільно проєктом «Європейський Союз та Рада Європи працюють разом для підтримки свободи медіа в Україні» та Міністерством культури та інформаційної політики України. URL: http://www.prostir.ua/?news=protydiya-dezinformatsiji-jevropejski-pidhody-ta-standarty

25. Гурковський, В.І. (2004). Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: автореф. дис. ... канд. юрид. наук: 25.00.02. Національна академія державного управління при Президентові України, Київ.

26. Дай, Томас Р. (2005). Основи державної політики. Пер. з англійської Г.Є. Краснокутського; наук. ред. З.В. Балабаєва. Одеса: АО Бахва

27. Данильян, О., & Дзьобань, О. (2022). Сучасна війна: трансформація сенсу в епоху інформаційних технологій. Журнал "Інформація і право", (4 (43)), 9-22

28. Данилюк, О.В., & Данилюк, А.В. (2021). Методика раннього виявлення гібридних загроз в умовах агентурних заходів впливу РФ. Журнал "Актуальні проблеми політики", Вип. 67, 135-142.
29. Дацюк, С. (2022). Теперішнє покоління людей буде жити в матриці. URL:https://www.youtube.com/watch?v=pKNNAaFlf-U
30. Дем'янчук О.П. (2000). "Державна політика" та "публічна політика": варіант перехідного періоду. Наукові записки НаУКМА: Політичні науки, Т. 18, с. 31-36.
31. Дем'янчук, О. П. (2006). Відповідність нинішньої системи управління й вироблення державної політики вимогам суспільства знань. Наукові праці, 54, с. 182-186.
32. Державний комітет ядерного регулювання України. 2004 рік. Тлумачний словник. URL: https://snriu.gov.ua/storage/app/sites/1/docs/Mijnarodna%20diyalnist/%20%D1%82%D0%B0%20%D0%A4%D0%97%20%D1%82%D0%BB%D1%83%D0%BC%D0%B0%D1%87%D0%BD%D0%B8%D0%B9%20%D1%81%D0%BB%D0%BE%D0%B2%D0%BD%D0%B8%D0%BA.pdf
33. Детектор Медіа (2019). Джерела інформації, медіаграмотність і російська пропаганда: результати всеукраїнського опитування громадської думки. URL: https://detector.media/infospace/article/164308/2019-03-21-dzherelainformatsii-mediagramotnist-i-rosiiska-propaganda-rezultati-vseukrainskogoopituvannya-gromadskoi-dumki/
34. Детектор Медіа (2023). Новий Закон про медіа: питання і відповіді в рамках роботи Гарячої лінії Комісії з журналістської етики. URL: https://detector.media/infospace/article/206858/2023-01-10-novyy-zakon-pro-media-pytannya-i-vidpovidi-v-ramkakh-roboty-garyachoi-linii-kzhe/
35. Детектор Медіа. (2019). Кожен другий українець вважає, що здатен розпізнати фейк чи дезінформацію, – опитування КМІС. URL: https://detector.media/infospace/article/164315/2019-03-21-kozhendrugii-

ukrainets-vvazhae-shcho-zdaten-rozpiznati-feik-chi-dezinformatsiyuopituvannya-kmis/

36. Детектор Медіа. (2022). YouTube заблокував російські канали RT та Sputnik по всій Європі // https://detector.media/infospace/article/197062/2022-03-01-youtube-zablokuvav-rosiyski-kanaly-rt-ta-sputnik-po-vsiy-ievropi/
37. Детектор Медіа. Про нас. URL: https://go.detector.media/istoriya-go/
38. Дзьобань О.П., Пилипчук В.Г. (2011). Інформаційне насильство та безпека: світоглядно-правові аспекти. Монографія. Харків: Майдан.
39. Директива Європейського Парламенту та Ради Європейського Союзу 2016/1148/EU від 6 липня 2016 року "Про заходи щодо забезпечення високого рівня безпеки мереж і інформаційних систем в Європейському Союзі". URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text
40. Додонов А., Ланде Д., Циганок В. та ін. (2017). Розпізнавання інформаційних операцій. Київ: Инжиниринг.
41. Доктрина інформаційної безпеки України (втратила чинність), затверджена Указом Президента України від 8 липня 2009 року №514/2009. URL: https://zakon.rada.gov.ua/laws/show/514/2009#top
42. Доронін, І. М. (2020). Національна безпека України в інформаційну епоху: теоретико-правове дослідження. Київ.
43. Драпак, М. (2019). Міжцарство, або імітація реальності. MediaLab. URL: http://medialab.online/news/imitationofreality/
44. Дрешпак, В. М. (2013). Концептуальні основи періодизації державної інформаційної політики України. Аспекти публічного управління, (2), 41-47.
45. Дубов, Д. В., Баровська, А. В., Ісакова, Т. О., Коваль, І. О., & Горбулін, В. П. (2017). «Активні заходи» СРСР проти США: пролог до гібридної війни: аналіт. доп. Київ: НІСД.

46. Економіка та економічна безпека держави. Теорія та практика : навч. посіб. / С. Давиденко, О. Єгорова, В. Приходько та ін. Ужгород : РІК-У, 2017.
47. Європейська правда. (2017). Генсек Ради Європи: блокування сайтів суперечить свободі слова. URL: https://www.eurointegration.com.ua/news/2017/05/17/7065808/
48. Ємець, Н. А. (2021). Сучасні підходи до управління масовою свідомістю і поведінкою. Соціальні інновації в контексті реформаційних змін: зб. матеріалів Міжнар. наук.-практ. конф. (м. Чернігів, 21 листоп. 2021 р.). Чернігів: НУ «Чернігівська політехніка», с. 32-36.
49. Животова К. В. (2021). Інфодемія «Пандемія CoVID-19»: проблеми та перспективи організації реагування на поширення дезінформації. Соціогуманітарний вимір сучасних трансформацій. Збірник матеріалів Всеукраїнської науково-практичної конференції (м. Чернігів, 29 жовтня 2021 р.). Науково-освітній інноваційний центр суспільних трансформацій, м.Чернігів. Суми: ТОВ НВП «Росток А. В.Т.». 2021. 96 с. С. 12-14 URL: https://reicst.com.ua/asp/article/view/conf_gum_2021_03
50. Животова К. В. (2021). Особливості нормативно-правового регулювання сфери інформаційної безпеки: проблемні питання та термінологічні колізії в Україні. Демократичне врядування. 2021. №2 (28). URL: https://science.lpnu.ua/uk/dg/vsi-vypusky/vypusk-228-2021/osoblyvosti-normatyvno-pravovogo-regulyuvannya-sfery-informaciynoyi
51. Животова К. В., Пискун І. В. (2021). Інформаційна оборона органів влади як складова національної безпеки України. Інформаційно телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання. Матеріали науково-практичної конференції (м. Київ, 24-25 листопада 2021 р.). К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 316 с. С .22.

52. Животова К. В., Трофименко В. М. (2022). Боротьба з кіберзлочинністю в умовах дії воєнного стану: аналіз нових законодавчих норм. Кібербезпека державних інституцій та подолання кризових станів: Матеріали І Міжнародної науково-практичної конференції. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2022. 321 с. С. 294-295.
53. Животова К. В. (2023). Дезінформаційні кампанії РФ як спроба зірвати поставки зброї ВСУ та шляхи протидії з боку України. Політичні технології пропаганди та контрпропаганди у російсько-українській війні : зб. матеріалів Круглого столу з міжнар. участю, до річниці повномасштаб. вторгнення, м. Київ, 21 лютого 2023 р. / М-во освіти і науки України, Ком. з питань свободи слова Верховної Ради України [та ін.] ; [орг. ком.: Гапоненко В. А. та ін.]. Київ : КНЕУ, 2023. С. 133–136. URL: https://ir.kneu.edu.ua:443/handle/2010/40436
54. Животова К. В. (2023). Механізми протидії дезінформації в сучасному інформаційному середовищі: економічний аспект. Стратегія економічного розвитку України. № 52. С. 5-16. URL: https://doi.org/10.33111/sedu.2023.52.005.016
55. Животова К.В. (2023). Особливості використання цифрових інструментів в інформаційному протиборстві. Кібербезпека державних інституцій та подолання кризових станів. Матеріали ІІ Міжнародної науково-практичної конференції в 2 т. Том 2. Особливості діяльності органів державної влади в умовах кризи зб. Тез наук.доп. (Київ – Вроцлав. Травень 2023). [Електронне видання]. Київ : «Офіс цифрового врядування», 2023. Т.2. 148 с. С. 36-37.
56. Завада, А. А., Павленко, М. М., Наумчак, О. М., & Ратушний, С. А. (2019). Удосконалена функціональна схема автоматизованої системи виявлення та оцінювання деструктивного інформаційно-психологічного впливу в електронних засобах масової інформації. Проблеми створення, випробування, застосування та експлуатації

складних інформаційних систем, (17), 5-13. URL: http://znp.zvir.zt.ua/article/view/212712

57. Загальна декларація прав людини. (1948). Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
58. Закон України. (1992). Про інформацію. № 48 від 1992 року. Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650)URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
59. Закон України. (1998). Про концепцію Національної програми інформатизації. № 27-28 від 1998 року. Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст. 182 URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text
60. Закон України. (2007). Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Відомості Верховної Ради України (ВВР), 2007, № 12, ст. 102. URL: https://zakon.rada.gov.ua/laws/show/537-16#top
61. Закон України. (2018). Про засади внутрішньої і зовнішньої політики. 2411-VI від 08.07.2018. Відомості Верховної Ради України (ВВР), 2010, № 40, ст. 527. URL: https://zakon.rada.gov.ua/laws/show/2411-17#Text
62. Закон України. (2018). Про національну безпеку України, 2018 рік, № 31. Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
63. Закон України. (2018). Про основи національної безпеки України від 19.06.2003 р. (втратив чинність на підставі Закону № 2469-VIII від 21.06.2018). Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text
64. Закон України. (2018). Про санкції. Відомості Верховної Ради (ВВР), 2014, № 40, ст. 2018. URL: https://zakon.rada.gov.ua/laws/show/1644-18#Text

65. Закон України. (2022). «Про друковані засоби масової інформації (пресу) в Україні». Відомості Верховної Ради України (ВВР), 1993, № 1, ст. 1 (втратив чинність на підставі Закону № 2849-IX від 13.12.2022). URL: https://zakon.rada.gov.ua/laws/show/2782-12#Text
66. Закон України. (2022). Про медіа, 2849-IX від 13 грудня 2022. Відомості Верховної Ради України (ВВР), 2023, №№ 47-50, ст.120. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text
67. Захаренко К.В. (2018). Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі. Гуманітарний вісник Запорізької державної інженерної академії, (72), 44-52.
68. Зацерківна М. (2019). PR-технології у формуванні іміджу закладів вищої освіти сфери культури: дис. на здоб. наук. ступ. канд. наук із соц ком. Київський національний університет культури і мистецтв.
69. Звоздецька О. (2020). Протидія дезінформаційним впливам у національному просторі Республіки Польща. Історико-політичні проблеми сучасного світу, 42, 160-172.
70. Звоздецька О. (2022). Інституціональні механізми протидії дезінформації в ЄС: проблеми та здобутки. Медіафорум, 10, 107-122. URL: https://journals.chnu.edu.ua/index.php/mediaforum/article/view/307
71. Зелена книга протидії дезінформації. Упоряд. і заг. ред. С. Балан. ГО «Інститут інформаційної безпеки», К. (2022).
72. Зозуля, О. С. (2017). Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства [Дисертація кандидата наук з державного управління]. Національна академія державного управління при Президентові України.
73. Золотар, О. О. (2017). Особливості інформаційної безпеки людини в умовах гібридної війни. Інформація і право, (3), 124-131.
74. Золотар, О. О. (2018). Ґенеза суспільних відносин щодо інформаційної безпеки людини. Інформація і право, (1 (24)), 139-148.

75. Золотухін, Д. (2020). Дезінформація не є феномен медіа, це є спецоперації. URL: https://www.ukrinform.ua/rubric-society/3135957-dezinformacia-ne-e-fenomen-media-ce-e-specoperacii-zolotuhin.html
76. Івохін, Є. В., Махно, М. Ф., & Рець, В. О. (2022). Про один спосіб аналізу тональності текстів за допомогою штучних нейронних мереж. Системи управління, навігації та зв'язку. Збірник наукових праць, 3(69), 71-74. https://doi.org/10.26906/SUNZ.2022.3.071
77. Інститут журналістики. (2020). Актуальні проблеми медіапростору: матеріали ІІ Всеукраїнської науково-практичної конференції (Київ, 09 квітня 2020 р.). Київ: Інститут журналістики.
78. Інститут масової інформації. (2019). Методологія моніторингу фейків та російської дезінформації в українських онлайн-медіа. URL: https://imi.org.ua/monitorings/metodolohiia-monitorynhu-feykiv-ta-rosiys-koi-dezinformatsii-v-ukrains-kykh-onlayn-media-i28321
79. Інститут масової інформації. Про IMI. URL: https://imi.org.ua/about
80. Інститут соціальної та політичної психології Національної академії педагогічних наук України. Концепція впровадження медіаосвіти в Україні. URL:: http://www.ispp.org.ua/news_44.htm
81. Інтерньюз-Україна. Інформація про нас. URL: https://internews.ua/about
82. Інформаційне управління Апарату Верховної Ради України. (2020). ЄС розвінчав понад вісім тисяч кремлівських фейків. URL: https://www.rada.gov.ua/print/192178.html
83. Карпенко, О. (2015). Управлінські послуги як механізм реалізації державної політики. Актуальні проблеми державного управління, (1), 11.
84. Карпенко, О. В., & Арсенович, Л. А. (2020). Державна кіберосвіта та інструменти підвищення рівня цифрової компетентності населення України. Вісник НАДУ. Серія "Державне управління", 1(96), 95–102.
85. Карпенко, О., & Животова, К. (2022). Концептуальні підходи до формування інформаційних механізмів запобігання та розв'язання

міжнаціональних конфліктів. Аспекти публічного управління, 10(6), 14-18. URL: https://doi.org/10.15421/152238

86. Кілієвич, О. І., & Тертичка, В. В. (2009). Державна політика: аналіз та механізми її впровадження: метод. рек. Київ: НАДУ. С.32.

87. Кіца, М. Я. (2017). Особливості та методи виявлення фейкової інформації в українських ЗМІ. Вісник Національного університету «Львівська політехніка». Серія: Журналістські науки, (883), 28-32.

88. Ковальчук, А., & Гавловський, В. (2022). Інформаційно-психологічні впливи як засіб маніпуляції свідомістю, що застосовується організованими злочинними угрупуваннями. Інформація і право, (2 (41)), 94-98.

89. Ковбасюк, Ю. В. (2011). Енциклопедія державного управління: у 8 т. Т. 4: Галузеве управління. Київ: НАДУ.

90. Ковбасюк, Ю. В. (2013). Модернізація державного управління та європейська інтеграція України. Вісник Національної академії державного управління при Президентові України, (3), 5-10.

91. Ковбасюк, Ю. В., Ващенко, К. О., & Сурмін, Ю. П. (Ред.). (2014). Державна політика: підручник. Київ: НАДУ

92. Козлова, Л. В. (2011). Теоретико-методологічні засади механізму формування державної політики. Наукові праці [Чорноморського державного університету імені Петра Могили комплексу Києво-Могилянська академія]. Серія: Державне управління, (159, Вип. 147), 63-69.

93. Колбеч, Г. К. (2004). Політика: основні концепції в суспільних науках (Пер. з англ.). Київ: КМ Академія.

94. Колісник, О. Л. (2011). Психологічний аналіз проблеми дезінформації у міжособистісному спілкуванні у сучасних психологічних дослідженнях. Вісник Національної академії Державної прикордонної служби України, 2011, Вип. 2. URL: http://nbuv.gov.ua/UJRN/Vnadps_2011_2_28

95. Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) [Конвенцію ратифіковано Законом № 475/97-ВР від 17.07.97]. URL:: https://zakon.rada.gov.ua/laws/show/995_004#Text
96. Кондратюк, М. В. (2017). Комп'ютерна безпека України в системі національної безпеки: матеріали міжнародної науково-практичної конференції "Стан та перспективи реформування сектору безпеки і оборони України", м. Запоріжжя, 24 листопада 2017 року (Том 2, с. 67-69). Київ: Національна академія прокуратури України.
97. Кононенко, М. Ю. (2021). ЗМІ в політичній структурі суспільства. У Соціально-політичні проблеми сучасності: VI Всеукраїнська наукова конференція студентів і молодих вчених: тези доповідей, Дніпро, 25 березня 2021 року (с. 36). Дніпро: Університет імені Альфреда Нобеля.
98. Конституція України. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
99. Концепція інтегрованої системи оцінки інформаційних загроз та реагування на них. Проект. (2018). URL:: https://www.documentcloud.org/documents/20600270-kontseptsiia-isomizor
100. Копан, О. В., & Мельник, В. І. (2016). Інформаційно-психологічна війна як засіб маніпулювання людською свідомістю. Журнал "Інформація і право", (2), 92-98.
101. Кормич, Б. А. (2001). Співвідношення національної безпеки та національних інтересів. Вісник Харківського національного університету внутрішніх справ, (13), 71-76.
102. Кормич, Б. А. (2011). Інформаційне право: підручник. Харків: БУРУН і К.
103. Короткий філософський словник. Дезінформація. URL:: https://terme.ru/slovari/kratkii-filosofskii-slovar-2004.html
104. Крафт, М. Е., & Ферлонг, С. Р. (2019). Публічна політика: політика, аналіз та альтернативи. Cq Press.

105. Кресіна, І. О. (2006). Політика, право і влада в контексті трансформаційних процесів в Україні: [монографія]. Київ: Ін-т держави і права ім. В. М. Корецького НАН України.

106. Крикун, В. (2022). Поняття «маніпулювання»: сутність та контексти. Вісник Національного університету імені Ярослава Мудрого, серія: Філософія, філософія права, політологія, соціологія, 2(53). https://doi.org/10.21564/2663-5704.53.258162

107. Кротюк, В. А. (2021). Війни інформаційної епохи: міждисциплінарний дискурс. Харків: ФОП Федорко М. Ю.

108. Купрій, В. (2007). Процес творення державної політики як об'єкт наукових досліджень. Політичний менеджмент, (5), 15-32.

109. Левченко, О. В. (2021). Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування. Житомир: Видавець ПП "Євро-Волинь".

110. Левченко, О. В., Троцько, В. В., & Василенко, І. С. (2014). Уточнення понятійного апарату з питань оцінювання рівня воєнної загрози національній безпеці України. Наука і оборона, 2, 17.

111. Литвиненко, О. (1998). Інформація і безпека. Нова політика, (1), 47-49.

112. Ліпкан, В. А. (2003). Теоретичні основи та елементи національної безпеки України [Монографія]. Київ: Національна академія внутрішніх справ України.

113. Ліпкан, В. А., & Череповський, К. П. (2014). Інкорпорація інформаційного законодавства України [Монографія]. Київ: Ліпкан О. С.

114. Ліпкан, В. А., Максименко, Ю. Є., & Желіховський, В. М. (2006). Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ: КНТ.

115. Логінов, І. В. (2017). Місце кіберрозвідки у виконавчому механізмі розвідувальної діяльності. У Роль і місце національної

спецслужби в історії українського державотворення: матеріали всеукр. наук.-практ. конф., с. 76. Київ: ВПЦ “Київський Університет”.

116. Магда, Є. М. (2014). Інформаційна війна як складова гібридної загрози. У Д. В. Яковлев (Ред.), Чорноморські політологічні читання: матеріали третьої науково-практичної конференції (с. 120). Одеса: Національний університет «Одеська юридична академія»

117. Майк Вендлінг (2018) Історія "фейкових новин". https://www.bbc.com/ukrainian/features-42786093

118. Мануїлова, К. В. (2018). Міжнародно-правовий режим нерозповсюдження ядерної зброї в сучасному міжнародному праві. НАУКОВИЙ ВІСНИК МІЖНАРОДНОГО ГУМАНІТАРНОГО УНІВЕРСИТЕТУ, (106).

119. Міжнародне агентство «Missions Publiques». Термінологічний словник. URL: https://wetheinternet.org/uk/%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96-%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB%D0%B8/#1599825473523-b80474ee-f255

120. Міжнародний пакт про громадянські і політичні права. (1973). URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

121. Міністерство з питань реінтеграції тимчасово окупованих територій України. Управління інформаційної політики. URL: https://minre.gov.ua/diyalnist/osnovni-zavdannya-czili-ta-napryamky-diyalnosti-strukturnyh-pidrozdiliv/upravlinnya-informaczijnoyi-polityky/

122. Міністерство закордонних справ України (2023). Nations Against Disinformation: запуск нового креативного інструменту з протидії дезінформації. Retrieved from https://mfa.gov.ua/news/nations-against-disinformation-zapusk-novogo-kreativnogo-instrumentu-z-protidiyi-dezinformaciyi

123. Міністерство закордонних справ України. Телекомунікаційна стратегія Міністерства закордонних справ України. URL: https://mfa.gov.ua/storage/app/sites/1/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%97/communication-strategy.pdf

124. Міністерство культури та інформаційної політики України. (2022). Український інформаційний фронт: ключові напрямки, за якими працювало МКІП у 2022 році. URL: https://mkip.gov.ua/news/8350.html

125. Міністерство культури та інформаційної політики. (2021). МКІП презентував оновлений бренд національного проєкту з медіаграмотності ФІЛЬТР. URL: https://mkip.gov.ua/news/5830.html

126. Міністерство культури, молоді та спорту України. (2020). Презентація законопроекту «Про протидію дезінформації». URL: https://mkip.gov.ua/files/InformPolityka.pdf

127. Міністерство оборони України. Військові ЗМІ. URL: https://www.mil.gov.ua/multimedia/vijskovi-zmi.html

128. Міністерство оборони України. Військове радіо «Армія FM». Про нас. URL: https://www.armyfm.com.ua/about-us/

129. Міністерство оборони України. Військове телебачення України. Армія TV. URL: https://www.youtube.com/user/ctrsTVua/videos

130. Міністерство оборони України. Інформаційне агентство. АрміяINFORM. URL: https://armyinform.com.ua/about-us/

131. Міністерство освіти і науки України. (2021). МОН підтримує ініціативу Президента України щодо проведення уроків медіаграмотності в школах. URL: https://mon.gov.ua/ua/news/mon-pidtrimuye-iniciativu-prezidenta-ukrayini-shodo-provedennya-urokiv-mediagramotnosti-v-shkolah

132. Мороз, О. (2020). 54% українців в Facebook публікують фейки, маніпуляції та сайти-сміттярки: Всеукраїнське дослідження.

Українська правда. URL: https://www.pravda.com.ua/articles/2020/09/14/7266269/

133. Назаренко, Г. І. (2009). Інформаційні жанри журналістики: Навчальник посібник. Київ: НАУ

134. Національна рада України з питань телебачення і радіомовлення. (2022). Звіт. URL: file:///C:/Users/%D0%90%D0%B4%D0%BC%D0%B8%D0%BD%D1%96%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80/Downloads/REPORT-NC.pdf

135. Національна рада України з питань телебачення і радіомовлення. (2020). Відстеження дезінформації в медіа. URL: https://www.nrada.gov.ua/vidstezhennya-dezinformatsiyi-v-media/

136. Національний Інститут стратегічних досліджень. (2015). Аналітична доповідь до щорічного послання Президента України до Верховної Ради України "Про внутрішнє та зовнішнє становище України у 2015 році". Київ: НІСД. URL: https://niss.gov.ua/sites/default/files/2015-12/POSLANNYA-2015_giper_new-4af35.pdf

137. Національний Інститут стратегічних досліджень. (2016). Аналітична доповідь до щорічного послання Президента України до Верховної Ради України "Про внутрішнє та зовнішнє становище України у 2016 році". Київ: НІСД. Retrieved from https://niss.gov.ua/sites/default/files/2016-10/poslanya_new-cc2e3.pdf

138. Національний Інститут Стратегічних Досліджень. (2020). Фейки як інструмент впливу на вибори: Аналітична доповідь (С. 4). Київ: Центр безпекових досліджень, Школа політичної аналітики НАУКМА. URL: https://niss.gov.ua/sites/default/files/2020-01/fake_news_fin_full_clean.pdf

139. Національний інститут стратегічних досліджень. Головна сторінка. URL: http://www.niss.gov.ua

140. Національний інститут стратегічних досліджень. Про інститут. URL: https://niss.gov.ua/pro-instytut

141. Нашинець-Наумова, А. Ю. (2017). Інформаційна безпека: питання правового регулювання [Монографія]. Київ: Видавничий дім “Гельветика”.

142. Нижник, Н. Р., Ситник, Г. П., & Білоус, В. Т. (2000). Національна безпека України (методологічні аспекти, стан і тенденції розвитку). Ірпінь: Преса України.

143. Ніцше, Ф. (2023). Так казав Заратустра. Жадання влади. URL: https://worldinbooks.com.ua/wp-content/uploads/2022/11/nitsshe-fridrikh-tak-kazav-zaratustra3781.pdf

144. Ожеван, М. (2001). Маніпулятивні стратегії. Підприємництво в Україні, 9, 26-27.

145. Опанасенко, М., & Дзюба, Т. (2021). Розроблення паспорту загрози для системи раннього виявлення загроз національній безпеці України. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(12), 61-68.

146. Орбан-Лембрик, Л.Е. (2006). Психологія маніпулювання масовою свідомістю й поведінкою. Вісник Прикарпатського університету. Філософські і психологічні науки, Вип. VII, 135-151

147. Островська, К., & Печений, Д. (2022). Дослідження методів на основі нейронних мереж для аналізу тональності корпусу текстів. У 2022 International Conference on Innovative Solutions in Software Engineering (ICISSE) (с. 55).

148. Офіційний сайт ЄвропейськогоСоюзу. Запитання та відповіді про оперативну групу East StratCom. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en

149. Падалка, Г. М. (2021). Соціокультурна диференціація та динаміка цінностей у сучасному інформаційному суспільстві. Актуальні проблеми філософії та соціології, (32), 138-143.

150. Пазюк, А. Правовий аналіз Указу Президента за рішенням РНБО «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». URL: http://moepravo.com.ua/pravoviy-analiz-ukazu-prezidenta-shhodo-blokuvannya-dostupu-do-resursivinternetu/

151. Пал, Л.А. (1999). Аналіз державної політики. Пер. з англ. І. Дзюби. Київ: Основи.

152. Палагнюк, Ю. В. (2012). "Державна політика" та "публічна політика": теоретичний аспект. Наукові праці Чорноморського державного університету імені Петра Могили. Серія: Державне управління, (169), 63-67.

153. Палагнюк, Ю.В. (2014). Державна євроінтеграційна політика України: теорія, методологія, механізми. Миколаїв: Вид-во ЧДУ ім. Петра Могили.

154. Петрик, В. М. та ін. (2006). Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: навч. посіб. Київ: Росава.

155. Пирожков, С. (1992). Національні інтереси України: Концепція безпеки і сучасні реалії геополітичної ситуації в Європі. Віче, (11), 11-23.

156. Половинчак, Ю. (2014). Мобілізаційний та маніпулятивний потенціал дискурсу соціальних медіа в умовах перехідного суспільства. URL: http://nbuviap.gov.ua/index.php

157. Попова, Т. В., & Ліпкан, В. А. (2016). Стратегічні комунікації: словник. Київ: Дорадо-Друк.

158. Постанова Верховної Ради України. (1997). Про Концепцію (основи державної політики) національної безпеки України. URL: https://zakon.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80#Text

159. Постанова Верховної Ради України. (2003). Про Концепцію національної інформаційної політики. URL: https://zakon.rada.gov.ua/laws/show/687-15#Text

160. Почепцов, Г. (2018). "Фейк – від людини, дезінформація – від держави". URL: http://ms.detector.media/trends/1411978127/feyk_ot_cheloveka_dezinformatsiya_ot_gosudarstva/

161. Почепцов, Г. (2019). (Дез)информация. Київ: ПАЛИВОДА А. В.

162. Почепцов, Г.Г. (2001). Информация и дезинформация. Киев: Ника-Центр, Эльга.

163. Почепцов, Г.Г. (2004). Стратегический анализ для политики, бизнеса и военного дела. Львів: Дзвін.

164. Почепцов, Г.Г., & Чукут, С.А. (2006). Інформаційна політика: навчальний посібник. Київ: Знання.

165. Праута, М. (2022). Місце військових медіа серед джерел інформації для військовослужбовців ЗС України. Образ, 1 (38), 89-99. DOI: https://doi.org/10.21272/Obraz.2022.1(38)-89-99. URL: https://essuir.sumdu.edu.ua/handle/123456789/88005

166. Пригорницька, О. (2017). Фейкова інформація в соціальних медіа: виявлення, оцінка, протидія. Наукові праці Національної бібліотеки України імені В.І. Вернадського: збірник наукових праць, 48, 311-321.

167. Пристайко, В.В. (2019). Ситуаційні центри як ключовий інституціональний механізм державного антикризового управління: зарубіжний досвід. Вчені записки Тернопільського національного університету імені В.І. Вернадського. Серія: Державне управління, 30 (69), 138-142.

168. Проект Закону про інформаційний суверенітет та інформаційну безпеку України. (1999). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6670

169. Проект Закону про інформаційну безпеку України. (2004). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=5732&skl=5

170. Пухкал, О.Г., & Гомоляко, О.В. (2017). Публічна та державна політика: єдність та відмінності. Інвестиції: практика та досвід, (24), 106.

171. Рабінович, П.М. (Видання 5). Основи загальної теорії права та держави.

172. Рада національної безпеки і оборони України. (2014). Рішення про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. URL: https://zakon.rada.gov.ua/laws/show/n0004525-14#Text

173. Радіо Свобода. (2017). У НАТО погодилися, що блокування російських інтернет-ресурсів в Україні є питанням безпеки, а не свободи слова. URL: https://www.radiosvoboda.org/a/news/28492020.html

174. Радіо Свобода. (2019). ЄС: у протидії дезінформації і «фейкам» є прогрес, але зусилля слід подвоювати. Retrieved from https://www.radiosvoboda.org/a/eu-misinformation-fake/29740123.html

175. Радіо Свобода. (2022). Українське телебачення тепер є у «Дії» – Мінцифри. URL: https://www.radiosvoboda.org/a/news-diya-tv/31738630.html

176. Радченко, О.В. (2013). Родові ознаки категорії "механізм" в соціальних науках. У Публічне управління: теорія та практика: збірник наукових праць Асоціації докторів державного управління (№ 3 (15), с. 19–25). Харків: Видавництво АДНДУ.

177. Ребкало, В., & Тертичка, В. (Ред.). (2000). Державна політика: аналіз та механізми її впровадження в Україні [Навчальний посібник]. Київ: Видавництво Національної академії державного управління.

178. Резнікова, О.О. (2018). Паспорт сепаратистської загрози в Україні. Стратегічні пріоритети, 2, 12–24.

179. Резнікова, О.О. (2022). Національна стійкість в умовах мінливого безпекового середовища [Монографія]. Київ: Національний інститут стратегічних досліджень.

180. Резнікова, О.О., Войтовський, К.Є., & Лепіхов, А.В. (2020). Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України [Аналітичний допис]. Київ: Національний інститут стратегічних досліджень.

181. Рішення Конституційного суду України у справі щодо тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка). URL: https://zakon.rada.gov.ua/laws/show/v005p710-97#Text

182. Рішення Ради національної безпеки і оборони України "Про створення та забезпечення діяльності Головного ситуаційного центру України". URL: https://zakon.rada.gov.ua/laws/show/n0002525-15#Text

183. Розпорядження Кабінету Міністрів України. (2013). Про схвалення Стратегії розвитку інформаційного суспільства в Україні. № 386-р від 15 травня 2013 року. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#n8

184. Розпорядження Кабінету Міністрів України. (2023). Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. № 272-р від 30 березня 2023 року URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-z-realizatsii-str-a272r

185. Ротар, Н. (2021). Формування політики захисту електоральної моделі політичної участі від дезінформаційних впливів (на прикладі політики Європейського Союзу). Історико-політичні проблеми сучасного світу, 43, 179-193.

186. Русенко, Н. (2022). Державна та правова політика: порівняльний аналіз. Інформація і право, 4 (43), 165-174.

187. Садковий, В. П., Домбровська, С. М., Лопатченко, І. М., & Антонов, А. В. (2019). Державна політика: аналіз та механізми впровадження: конспект лекцій. Харків: НУЦЗУ.

188. Самчинська, О. А. (2022). Дезінформація: поняття та сутність. Адміністративне право і процес, 3 (38), 32-45. https://ela.kpi.ua/handle/123456789/49917

189. Свєшніков, С., Бочарніков, В., Прима, А., & Дергільова, О. (2021). Чинники безпекового середовища, важливі для розвитку сил оборони України. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, 25-32.

190. Сінґер, Р. (2019). Війна лайків. Зброя в руках соціальних мереж. Х : Клуб сімейного дозвілля

191. Рішення Конституційного суду України у справі щодо тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка). URL: https://zakon.rada.gov.ua/laws/show/v005p710-97#Text

192. Рішення Ради національної безпеки і оборони України "Про створення та забезпечення діяльності Головного ситуаційного центру України". URL: https://zakon.rada.gov.ua/laws/show/n0002525-15#Text

193. Розпорядження Кабінету Міністрів України. (2013). Про схвалення Стратегії розвитку інформаційного суспільства в Україні. № 386-р від 15 травня 2013 року. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#n8

194. Розпорядження Кабінету Міністрів України. (2023). Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. № 272-р від 30 березня 2023 року URL:

https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-z-realizatsii-str-a272r

195. Ротар, Н. (2021). Формування політики захисту електоральної моделі політичної участі від дезінформаційних впливів (на прикладі політики Європейського Союзу). Історико-політичні проблеми сучасного світу, 43, 179-193.

196. Русенко, Н. (2022). Державна та правова політика: порівняльний аналіз. Інформація і право, 4 (43), 165-174.

197. Садковий, В. П., Домбровська, С. М., Лопатченко, І. М., & Антонов, А. В. (2019). Державна політика: аналіз та механізми впровадження: конспект лекцій. Харків: НУЦЗУ.

198. Самчинська, О. А. (2022). Дезінформація: поняття та сутність. Адміністративне право і процес, 3 (38), 32-45. https://ela.kpi.ua/handle/123456789/49917

199. Свєшніков, С., Бочарніков, В., Прима, А., & Дергільова, О. (2021). Чинники безпекового середовища, важливі для розвитку сил оборони України. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, 25-32.

200. Сінґер, Р. (2019). Війна лайків. Зброя в руках соціальних мереж. Х : Клуб сімейного дозвілля

201. Тарасюк, В. М. (2018). Політико-правові засади застосування інформаційних технологій в умовах гібридної війни [Кваліфікаційна наукова праця на правах рукопису, Доктор філософії, Кваліфікаційна наукова праця, Національний університет "Києво-Могилянська академія", Факультет політичних наук]. Київ. URL: http://idpnan.org.ua/files/tarasyuk-v.m.-politiko-pravovi-zasadi-zastosuvannya-informatsiynih-tehnologiy-v-umovah-gibridnoyi-viyni-_d_.pdf

202. ТЕКСТи. Інфовійна. URL: https://texty.org.ua/tag/dezinformatsija/

203. ТЕКСТи. Тролесфера. URL: https://texty.org.ua/d/fb-trolls/

204. Тертичка, В. (2002). Державна політика: аналіз та здійснення в Україні. Київ: Видавництво Соломії Павличко “Основи”.

205. Тертичка, В. (2007). Суспільна політика: чи стала вона сферою наукового пошуку і прикладних досліджень в Україні? Політичний менеджмент, 1, 10-23.

206. Тимчасове положення про Раду національної безпеки України: Розпорядження Президента України від 03 липня 1992 року № 117/92-рп. URL: https://zakon.rada.gov.ua/laws/show/117/92-рп

207. Ткачук, Н. І. (2020). Аналітична складова в інституціональному забезпеченні оцінки ризиків і загроз національній безпеці України. Інформаційна безпека людини, суспільства, держави, 1-3 (28-30), 38-44.

208. Ткачук, Т.Ю. (2019). Правове забезпечення інформаційної безпеки в умовах євроінтеграції України [Докторська дисертація, ДВНЗ «Ужгородський національний університет»]. Ужгород. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/19617

209. Турчак, А. (2019). Основні складові інформаційної безпеки держави. Аспекти публічного управління, 7(5), 44-56.

210. Указ Президента України (1994). Про Положення про Раду національної безпеки при Президентові України. Від 23 серпня 1994 року № 469/94 URL: https://zakon.rada.gov.ua/laws/show/469/94

211. Указ Президента України (1994). Про утворення Міністерства України у справах преси та інформації. Від 18 листопада 1994 року № 689/94. URL: http://zakon5.rada.gov.ua/laws/show/689/94

212. Указ Президента України (1996). Про затвердження Положення про Апарат Ради національної безпеки і оборони України. Від 4 жовтня 1996 року №927/96. URL: https://ips.ligazakon.net/document/U927_96?an=9

213. Указ Президента України (1996). Про Раду національної безпеки і оборони України. Від 30 серпня 1996 року №727/96. URL: https://zakon.rada.gov.ua/laws/show/772/96#Text

214. Указ Президента України (1998). Про Положення про Комісію з питань інформаційної безпеки. М. Київ, 27 березня 1998 р., №224/98. URL: https://zakon.rada.gov.ua/laws/show/76/98#Text

215. Указ Президента України (2007). Про Стратегію національної безпеки України» від 12 лютого 2007 року. URL: https://www.president.gov.ua/documents/1052007-5496

216. Указ Президента України (2012). Про питання Апарату Ради національної безпеки і оборони України. № 251/2012. URL: https://zakon.rada.gov.ua/laws/show/251/2012#Text

217. Указ Президента України (2012). Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Стратегії національної безпеки України". URL: https://zakon.rada.gov.ua/laws/show/389/2012#Text

218. Указ Президента України (2012). Про рішення Ради національної безпеки і оборони України від 29 грудня 2012 року "Про Стратегічний оборонний бюлетень України". URL: https://zakon.rada.gov.ua/laws/show/771/2012#n16

219. Указ Президента України (2014). Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України". URL: https://zakon.rada.gov.ua/laws/show/449/2014#n2

220. Указ Президента України (2015). Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". №287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text

221. Указ Президента України (2015). Про рішення Ради національної безпеки і оборони України від 25 січня 2015 року "Про створення та забезпечення діяльності Головного ситуаційного центру України". Від 28 лютого 2015 року № 115/2015. URL: https://zakon.rada.gov.ua/laws/show/115/2015#n2

222. Указ Президента України (2016). Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України". URL: https://zakon.rada.gov.ua/laws/show/240/2016#n257

223. Указ Президента України (2016) Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» № 47/2017 від 25.02.2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

224. Указ Президента України (2019). Питання європейської та євроатлантичної інтеграції від 20 квітня 2019 року №155/2019. URL: https://www.president.gov.ua/documents/1552019-26586

225. Указ Президента України (2020). Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України". URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

226. Указ Президента України (2021). Про питання Центру протидії дезінформації. №187/2021. URL: https://www.president.gov.ua/documents/1872021-38841

227. Указ Президента України (2021). Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". Від 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

228. Указ Президента України (2021). Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року "Про створення

Центру протидії дезінформації". Від 19 березня 2021 року №106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text

229. Указ Президента України (2021). Про Стратегію комунікації з питань євроатлантичної інтеграції України на період до 2025 року. Від 11 серпня 2021 року № 348/2021. URL: https://zakon.rada.gov.ua/laws/show/348/2021#top

230. Указ Президента України (2022). Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». Від 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

231. Урядовий портал. (2021). Презентовано Центр стратегічних комунікацій та інформаційної безпеки. URL: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki

232. Фільтр (2021). Національний проєкт з медіаграмотності. URL: https://www.facebook.com/filterproject2021/posts/200851855641888

233. Фурашев, В. М. (2012). Сутність та визначення понять "інформаційна безпека" і "безпека інформації". Правова інформатика, 2(34), 51-59.

234. Хакімова, В. Т. (2021). Європейський Союз в епоху постправди: діяльність East StratCom Task Force.

235. Харарі, Ю. Н. (2022). 21 урок для 21 століття. Київ: BookChef.

236. Цвєтков, В. В. (2007). Демократія і державне управління: теорія, методологія, практика. Київ: Юридична думка.

237. Центр Медіареформи. Про нас. URL: https://www.stopfake.org/uk/pro-nas/

238. Центр стратегічних комунікацій та інформаційної безпеки. Про нас. URL: https://spravdi.gov.ua/pro-nas/

239. Ципердюк, І. (2020). Від холодної війни до російської військової агресії: 65 років українській редакції радіо „Свобода”. Теле-та радіожурналістика, (19)

240. Чарльз В. Форд (2022) "Психологія обману. Як, чому і навіщо брешуть навіть чесні люди? URL: https://polygraph.ua/charlz-v-ford-psihologija-obmana-kak-pochemu-i-zachem-lgut-dazhe-chestnye-ljudi/

241. Шевчук, П. (2014). Інформаційно-психологічна війна Росії проти України: як їй протидіяти. Демократичне врядування, (13).

242. Шемчук, В. (2019). Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. Філософські та методологічні проблеми права, 17(1), 51-59.

243. Шлапаченко, В. М. (2013). Дезінформація як спосіб інформаційно-психологічного впливу. Інформаційна безпека людини, суспільства, держави, 2(12), 78-86. URL: http://nbuv.gov.ua/UJRN/iblsd_2013_2_15

244. Шпига, П. С., & Рудник, Р. М. (2014). Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин, 8, 326-339. - С.328. URL: http://nbuv.gov.ua/UJRN/Pmv_2014_8_22

245. Шумка, А. В., & Черник, П. П. (2015). Теоретичні аспекти інформаційних війн та національна безпека. Науково-теоретичний альманах «Грані», 18(9), 10-16.

246. Янг, Е., & Квінн, Л. (2003). Як написати дієвий аналітичний документ у галузі державної політики: практичний посібник для радників з державної політики у Центральній і Східній Європі (С. Соколик, пер., О. Кілієвич, Наук. ред.). Київ: К.І.С.

247. Aitton, S., & Posetti, J. (2018). Journalism, "Fake News," and Disinformation: A Guide for Academic and Professional Training of Journalists. UNESCO. Retrieved from

248. Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), 211-236.

249. Allison, G., & Zelikow, F. (1999). Essence of the Decision: Explaining the Cuban Missile Crisis. New York: Longman.

250. Anderson, A. (1979). J. E. Public Policy Making. NY: Holt, Rinehart and Winston

251. Ayee, J. (2015). The Politics of Public Sector Performance: Pockets of Effectiveness in Developing Countries. European Journal of Development Research, 27(2), 333–335. https://doi.org/10.1057/ejdr.2014.49

252. Becker, J. (2004). Lessons from Russia: A Neo-Authoritarian Media System. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.1860&rep=rep1&type=pdf

253. Bednar, P., & Welch, C. (2008). Bias, misinformation and the paradox of neutrality. Informing Science, 11(11), 85–106.

254. Bredemeier, K. (2005). Schwarze Rhetorik: Macht und Magie der Sprache. Goldmann Verlag.

255. Brzezinski, Z. (1970). Between Two Ages: America's Role in the Technetronic Era. New York: The Viking Press.

256. Bundesregierung.de. (n.d.). Дезінформація: Пояснення поняття. Retrieved from https://www.bundesregierung.de/breg-de/themen/umgang-mit-desinformation/%D0%B4%D0%B5%D0%B7%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F-%D0%BF%D0%BE%D1%8F%D1%81%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BF%D0%BE%D0%BD%D1%8F%D1%82%D0%B8%D1%8F-1911052

257. Cambridge University Press. Definition of disinformation from the Cambridge Advanced Learner's Dictionary & Thesaurus. Retrieved from https://dictionary.cambridge.org/dictionary/english/disinformation

258. Castells, M. (2004). The Network Society: A Cross-cultural Perspective. Cambrian Typesetters, Frimley, Surrey.

259. Castells, M. (2010). The Information Age Economy, Society, and Culture. Printed in Singapore by Markono Print Media Pte Ltd. Retrieved from https://urb.bme.hu/wp-content/uploads/2014/05/manuel_castells_the_rise_of_the_network_society bookfi-org.compressed.pdf

260. Central Intelligence Agency. (1994). The CIA under Harry Truman – History Staff Center For the Study of Intelligence. Washington, DC. Retrieved from https://www.cia.gov/static/4b3a27a7e8c4933c856045ee3453c8b3/CIA-Under-Harry-Truman-CIA-Documents-1994-Complete-web.pdf

261. CSC. (2021). Countering disinformation in the United States. CSC White Paper #6. Retrieved from file:///C:/Users/%D0%90%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80/Downloads/863779.pdf

262. Davis, C. C., & Bittman, L. (1985). The KGB and Soviet Disinformation: An Insider's View. Pergamon-Brassey's.

263. Deutsche Welle. Дезінформація. URL: https://www.dw.com/ru/%D0%B4%D0%B5%D0%B7%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/t-37276895

264. Dictionary.com. Misinformation. URL: https://www.dictionary.com/browse/misinformation

265. Disinformation Observatory. Retrieved from www.disinfobservatory.org/

266. DNI Office of the Director of National Intelligence. (2017). Background to “Assessing Russian Activities and Intentions in Recent US

Elections": The Analytic Process and Cyber Incident Attribution [PDF file]. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

267. EU vs Disinfo. (n.d.). Disinformation Review. Retrieved from https://euvsdisinfo.eu/disinfo-review/

268. EU vs Disinfo. Retrieved from https://euvsdisinfo.eu/about/

269. European Commission. (2018). Code of Practice on Disinformation. Retrieved from https://digital-strategy.ec.europa.eu/en/news/code-ractice-disinformation

270. European Commission. (2018). EU Code of Practice on Disinformation. Retrieved from https://digital-strategy.ec.europa.eu/en/library/2018code-practice-disinformation

271. European Commission. (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. On the European democracy action plan. COM/2020/790 final.

272. European Commission. (2022). Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1978

273. European Commission. (2022). The 2022 Code of Practice on Disinformation. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/code-practicedisinformation

274. European Commission. (2022). The Strengthened Code of Practice on Disinformation 2022. Retrieved from https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

275. European Council. (2015). Conclusions adopted by the European Council at the European Council meeting on 19 and 20 March 2015. Retrieved from https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015en.pdf

276. European Court of Human Rights. (1976). Case of Handyside v. the United Kingdom (Application no. 5493/72): Judgment. Retrieved from http://hudoc.echr.coe.int/rus?i=001-57499

277. European Digital Media Observatory. (2021). EDMO – United against disinformation. Retrieved from https://edmo.eu/

278. European Parliament resolution of 23 November 2016 on "Countering Propaganda Supporting Radicalization and Terrorism" (2016/2030(INI)).

279. European Parliament. (2016). Draft report on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)). Committee on Foreign Affairs. Retrieved from https://www.europarl.europa.eu/doceo/document/AFETPR-582060_EN.pdf?redirect

280. European Union External Action Service. Don't be deceived: EU acts against fake news and disinformation. Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage/32408/dont-bedeceived-eu-acts-against-fake-news-and-disinformation_en

281. European Union. (2016). Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats a European Union Response. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

282. European Union. (2017). Joint Staff Working Document: EU Operational Protocol for Countering Hybrid Threats – 'EU Playbook'. SWD(2016) 227 final.

283. European Union. (2018). Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Action Plan against Disinformation. Brussels, 5.12.2018. JOIN(2018) 36 final.

284. Economic encyclopedia. Disinformation. URL: https://slovnyk.me/dict/economics_encyclopedia/%D0%B4%D0%B5%D0%

B7%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F

285. Fallis, D. (2009). A Conceptual Analysis of Disinformation. Retrieved from https://www.ideals.illinois.edu/items/15210

286. Fallis, D. (2015). What is disinformation? Library Trends, 63(3), 401–426. Retrieved from http://www.u.arizona.edu/~fallis/LIB%2063.3%2005.%20fallis%20401_426.pdf

287. FBI. Combating Foreign Influence. Retrieved from https://www.fbi.gov/investigate/counterintelligence/foreign-influence

288. Fetzer, J. H. (2004). Information: Does it Have To Be True? Minds and Machines, 14(2), 223-229. Retrieved from file:///C:/Users/%D0%9A%D1%81%D1%8E%D1%88%D0%B0/Downloads/Information_Does_it_Have_To_Be_True.pdf

289. Floridi, L. (2005). Semantic conceptions of information. In Stanford Encyclopedia of Philosophy. Retrieved from http://plato.stanford.edu/entries/information

290. Floridi, L. (2011). The philosophy of information. New York: Oxford University Press.

291. Fox, C. J. (1983). Information and misinformation. Westport, CT: Greenwood Press.

292. Franke, H. W. (1964). Der manipulierte Mensch. Grundlagen der Werbung und der Meinungsbildung. Wiesbaden: F. A. Brockhaus.

293. Freedom House. (2019). Policy Brief "Should Ukraine Drop Sanctions against Russian Tech Companies?" Retrieved from https://freedomhouse.org/report/policy-brief/2019/should-ukraine-drop-sanctions-against-russian-tech-companies

294. French Government. (2018). LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. Retrieved from https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559

295. German Federal Gazette. (2017). Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG). Retrieved from https://www.gesetze-im-internet.de/netzdg/BJNR335210017.htm

296. Government Communication Service. (2019). Resilience against misinformation and disinformation toolkit. Retrieved from https://gcs.civilservice.gov.uk/wp-content/uploads/2019/08/6.5177_CO_RESIST-Disinformation-Toolkit_finaldesign_accessible-version.pdf

297. Hartley, J. (1999). Information Warfare and Security. McGraw-Hill Education.

298. High Level Expert Group. (2018). A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation. Brussels. Retrieved from https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

299. Hoffman, F. (2011). Future Threats and Strategic Thinking. Infinity Journal, No Fall 2011, 17.

300. Hogan, M. J. (1987). The Marshall Plan: America, Britain and the Reconstruction of Western Europe 1947–1952. Cambridge: Cambridge University Press.

301. Hybrid CoE. About us. Retrieved from https://www.hybridcoe.fi/who-what-and-how/

302. InformNapalm. About. Retrieved from https://informnapalm.org/ua/about

303. Katz, J. E. (2018). Commentary on News and Participation through and beyond Proprietary Platforms in an Age of Social Media. Media and Communication, 6(4), 103–106.

304. Kennedy, M. D. (2015). The Evolution of Cyber War: International Norms for Emerging-Technology Weapons. Potomac Books.

305. Khan, I. (2021). Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/47/25. Retrieved from https://undocs.org/A/HRC/47/25

306. Libicki, M. C. (1995). What is Information Warfare? Washington, D.C.: National Defense University Press.

307. Lippmann, W. (1949). Public Opinion. New York, London: The Free Press. A Division of Macmillan Publishing Co., Inc.; Collier Macmillan Publishers.

308. Lippmann, W. (1993). The Phantom Public (International Organizations Series). New York: Transaction Publishers.

309. Marcuse, H. (1964). One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society. Beacon Press.

310. Martens, B., Aguiar, L., Gomez-Herrera, E., & Mueller-Langer, F. (2018). The digital transformation of news media and the rise of disinformation and fake news — An economic perspective. Digital Economy Working Paper 2018—02. JRC Technical Reports. Seville. Retrieved from https://ec.europa.eu/jrc/communities/sites/jrccties/files/dewp_201802_digital_transformation_of_news_media_and_the_rise_of_fake_news_final_180418.pdf

311. Mattelart, A. (2003). The Information Society: An Introduction (1st ed.). New York: SAGE Publications Ltd.

312. McLuhan M. (1964). Understanding Media: The Extensions of Man. — N.Y. : McGraw Hill. — 1964 с.

313. McLuhan, M. (1962). The Gutenberg Galaxy: The Making of Typographic Man. University of Toronto Press.

314. MediaLab. Про нас. URL: https://medialab.online/aboutus/

315. Merriam-Webster . The Real Story of 'Fake News'. URL: https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news

316. NATO. (2009). Strasbourg/Kehl Summit Declaration. Retrieved from https://www.nato.int/cps/en/natolive/news_52837.htm

317. NATO. (2019). NATO's role in cyberspace. Retrieved from https://www.nato.int/docu/review/uk/articles/2019/02/12/rol-nato-v-kberprostor/index.html

318. NATO. (2023). Cyber protection. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

319. Neuman, R. (1991). The Future of the Mass Audience. Cambridge

320. Oxford Living Dictionaries. (2022). Definition of disinformation in English. Retrieved from https://en.oxforddictionaries.com/definition/disinformation

321. Prav, R. (2018). Monitoring of the development of information infrastructure in Ukraine. Technology Audit and Production Reserves, 3(4(47)), 12–18. https://doi.org/10.15587/2312-8372.2019.169592

322. RAND Corporation. (2018). The Diminishing Role of Facts in American Public Life. Retrieved from https://www.rand.org/blog/2018/01/the-diminishing-role-of-facts-in-american-public-life.html

323. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1925

324. Riker, W. (1986). The Art of Political Manipulation. New Haven: Yale University Press.

325. Ron, T. (2003). Smart War: The Logic of Conflict in the 21st Century. New York: Brassey's.

326. Rona, T. (1976). Weapon Systems and Information War. Seattle, WA: Boeing Aerospace Co.

327. Schiller, Herbert I. (1973). The Mind Managers. Boston: Beacon Press

328. Schiller, Herbert I. (1992). Mass Communication and American Empire (2nd ed.). Boulder: Westview Press.

329. Shostrom, E. L. (2003). Man, the Manipulator: The Inner Journey from Manipulation to Actualization. К.: PSYLIB

330. Shultz, R. H., & Godson, R. (1984). Dezinformatsia: Active Measures in Soviet Strategy. Pergamon-Brassey's

331. Sigal, Adam. (2012). Advancing Adversary Thinking: Approaches and Applications. National Defense University Press.

332. Stahl, B. C. (2006). On the Difference or Equality of Information, Misinformation, and Disinformation: A Critical Research Perspective. Informing Science, 9(9), 83-96. https://doi.org/10.28945/473

333. StopFake. (2019). Дезінформація – це не тільки брехня. Так працює Sputnik [Електронний ресурс]. URL: https://www.stopfake.org/uk/dezinformatsiya-tse-ne-tilky-brehnya-tak-pratsyuye-sputnik/

334. Sun Tzu. (2003). The Art of War. (S. B. Griffith, Trans.). Oxford University Press

335. Toffler, A. (1980). The Third Wave. New York: Bantam Books.

336. Toffler, A. (1990). Power Shift. New York, NY: Bantam Books.

337. Trump, D. [@realDonaldTrump]. (2017, February 25). FAKE NEWS media knowingly doesn't tell the truth. Retrieved from: https://twitter.com/realDonaldTrump/status/835325771858251776?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E835325771858251776%7Ctwgr%5E9e2d5927c3bdcbbfb700c27efc8ca0918d17e808%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fnv.ua%2Fworld%2Fcountries%2Ftramp-the-new-york-times-i-cnn-prevratilis-v-anekdot-707504.html

338. Tudjman, M., & Mikelic, N. (2003). Information Science: Science about Information, Misinformation and Disinformation. In Proceedings of Informing Science and Information Technology Education Joint Conference, Pori, Finland. Retrieved from http://proceedings.informingscience.org/IS2003Proceedings/docs/204Tudjm.pdf

339. U.S. Congress, House of Representatives. (1980). Soviet Covert Action. Hearings before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence, 96th Congress, 2nd Session, February 6, 19

340. U.S. Department of State. Global Engagement Center. Retrieved from https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/

341. UNESCO. (2018). Journalism, "Fake News" & Disinformation: Handbook for Journalism Education and Training. Retrieved from https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf

342. Versluis, E., van Mendeltje, K., & Stephenson, P. (2011). Analyzing the European Union Policy Process. Houndmills: Palgrave Macmillan.

343. VoxCheck. Про VoxCheck. URL: https://voxcheck.voxukraine.org

344. Vrij, A. (2001). Detecting Lies and Deceit. New York: Wiley. - 483 p.

345. Wardle, C. (2017). Fake news. It’s complicated. Retrieved from https://firstdraftnews.org/articles/fake-news-complicated/

346. We’re in This Together. Mis-, Dis-, and Malinformation Stops with You. URL: https://www.cisa.gov/sites/default/files/publications/election-disinformation-toolkit_508_0.pdf

347. Wiener, N. (1950). The Human Use of Human Beings. Houghton Mifflin Company

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових фахових виданнях України

1. **Животова К. В.** Особливості нормативно-правового регулювання сфери інформаційної безпеки: проблемні питання та термінологічні колізії в Україні. *Демократичне врядування.* 2021. №2 (28). URL: https://science.lpnu.ua/uk/dg/vsi-vypusky/vypusk-228-2021/osoblyvosti-normatyvno-pravovogo-regulyuvannya-sfery-informaciynoyi *(0,45 д.а.).*

2. Карпенко О., **Животова К. В.** Концептуальні підходи до формування інформаційних механізмів запобігання та розв'язання міжнаціональних конфліктів. *Аспекти публічного управління.* 2022. № 10(6). С. 14-18. DOI: https://doi.org/10.15421/152238. *(0,43 д.а., особисто автору 0,25 д.а., проаналізовано концептуальні підходи до розуміння інформаційних механізмів, які базуються на використанні різноманітних теорій, концепцій та моделей, таких як теорії медіа, комунікації, масової інформації, політичної комунікації, комунікації в конфліктах тощо).*

3. **Животова К. В.** Механізми протидії дезінформації в сучасному інформаційному середовищі: економічний аспект. *Стратегія економічного розвитку України.* № 52. С. 5-16. URL: https://doi.org/10.33111/sedu.2023.52.005.016 *(0,62 д.а.).*

В інших виданнях

1. **Животова К. В.** Інфодемія «Пандемія CoVID-19»: проблеми та перспективи організації реагування на поширення дезінформації. *Соціогуманітарний вимір сучасних трансформацій*. Збірник матеріалів Всеукраїнської науково-практичної конференції (м. Чернігів, 29 жовтня 2021 р.). Науково-освітній інноваційний центр суспільних трансформацій,

м.Чернігів. Суми: ТОВ НВП «Росток А. В.Т.». 2021. 96 с. С. 12-14 URL: https://reicst.com.ua/asp/article/view/conf_gum_2021_03 *(0,13 д.а.).*

2. **Животова К. В.**, Пискун І. В. Інформаційна оборона органів влади як складова національної безпеки України. *Інформаційно телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання.* Матеріали науково-практичної конференції (м. Київ, 24-25 листопада 2021 р.). К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 316 с. С .22. *(0,2 д.а.)*

3. **Животова К. В.**, Трофименко В. М. Боротьба з кіберзлочинністю в умовах дії воєнного стану: аналіз нових законодавчих норм. *Кібербезпека державних інституцій та подолання кризових станів:* Матеріали І Міжнародної науково-практичної конференції. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2022. 321 с. С. 294-295. *(0,15 д.а.).*

4. **Животова К.В.** Особливості використання цифрових інструментів в інформаційному протиборстві. *Кібербезпека державних інституцій та подолання кризових станів.* Матеріали ІІ Міжнародної науково-практичної конференції в 2 т. Том 2. Особливості діяльності органів державної влади в умовах кризи зб. Тез наук.доп. (Київ – Вроцлав. Травень 2023). [Електронне видання]. Київ : «Офіс цифрового врядування», 2023. Т.2. 148 с. С. 36-37. *(0,15 д.а.).*

5. **Животова К. В.** Дезінформаційні кампанії РФ як спроба зірвати поставки зброї ВСУ та шляхи протидії з боку України. *Політичні технології пропаганди та контрпропаганди у російсько-українській війні* : зб. матеріалів Круглого столу з міжнар. участю, до річниці повномасштаб. вторгнення, м. Київ, 21 лютого 2023 р. / М-во освіти і науки України, Ком. з питань свободи слова Верховної Ради України [та ін.] ; [орг. ком.: Гапоненко В. А. та ін.]. Київ : КНЕУ, 2023. С. 133–136. URL: https://ir.kneu.edu.ua:443/handle/2010/40436 *(0,18 д.а.).*

Україна
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені Вадима Гетьмана
03057, м. Київ, пр-т Берестейський, 54/1. e-mail: office@kneu.edu.ua
Тел.: (044) 456-50-55, (044) 371-61-19. ЄДРПОУ: 02070884

23.04.24 № 01/13-428

На №_____

ДОВІДКА

про впровадження результатів дисертаційного дослідження Животової Ксенії Вікторівни за темою: «Механізми вироблення державної політики у сфері протидії дезінформації» в навчальний процес Київського національного економічного університету імені Вадима Гетьмана

Довідка видана у підтвердження того, що результати дисертаційного дослідження сформульовані в роботі Животової Ксенії Вікторівни за темою: «Механізми вироблення державної політики у сфері протидії дезінформації» використано в навчальному процесі кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана при підготовці та викладанні навчальних дисциплін «Інформаційна політика та комунікації в публічному управлінні» та «Інформаційні війни та цифрова культура».

Заслуговують на увагу запропоновані здобувачем науково обґрунтовані підходи щодо формування державних механізмів протидії дезінформації в умовах інформаційної війни, зокрема у запровадженні інноваційних складових програми підвищення медіаграмотності населення України.

Проректор
з науково-педагогічної роботи,
доктор економічних наук, професор Анатолій КОЛОТ

003369

ДЕРЖАВНИЙ КОМІТЕТ ТЕЛЕБАЧЕННЯ І РАДІОМОВЛЕННЯ УКРАЇНИ
вул. Прорізна, 2, м. Київ, 01001, Тел. (044) 239-63-89, факс 279-44-50
E-mail: office@comin.gov.ua, www.comin.kmu.gov.ua

«12» 03 2024 р. № 724/28/3-1 На № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження аспірантки кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана **Животової Ксенії Вікторівни** за темою: **«Механізми вироблення державної політики у сфері протидії дезінформації»** на здобуття ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування»

Результати дисертаційного дослідження Животової Ксенії Вікторівни за темою: «Механізми вироблення державної політики у сфері протидії дезінформації» використано Державним комітетом телебачення і радіомовлення України. Враховано науково обґрунтовані пропозиції щодо оптимізації механізмів вироблення та реалізації державної політики у сфері протидії дезінформації, що відображено у створенні нових інструментів моніторингу та аналізу інформаційного простору, а також у виробленні Плану заходів уряду з реалізації Стратегії інформаційної безпеки на період до 2025 року (заходів, спрямованих на розвиток співпраці між органами влади, громадськістю та ЗМІ з метою побудови ефективної стратегії протидії дезінформації для забезпечення інформаційної безпеки України).

Рекомендації, що містяться в дисертації, також було використано у процесі розробки «Закону про медіа», який набув чинності 31 березня 2023 року, що сприяло підвищенню ефективності системи регулювання медіа простору з урахуванням важливості боротьби з дезінформацією та забезпеченням інформаційної безпеки суспільства.

Голова **Олег НАЛИВАЙКО**

НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОГО УПРАВЛІННЯ ПРИ ПРЕЗИДЕНТОВІ УКРАЇНИ
Ідентифікаційний код 23696843
25 січня 2021 р.
№ 269
м.Київ-57, вул. Ежена Потьє, 20

ДОВІДКА
про участь у науково-дослідних роботах

Видана ЖИВОТОВ Й Ксенії Вікторівні з підтвердженням про те, що вона дійсно брала участь у виконанні науково-дослідних робіт за комплексним науковим проектом "Державне управління та місцеве самоврядування" (державний реєстраційний номер 0199U002827) Національної академії державного управління при Президентові України, а саме:

- у 2019 та 2020 роках – виконавець на громадських засадах, технік (накази: від 14 березня 2019 року № 143-ос "Про призначення виконавців науково-дослідних робіт"; від 09 жовтня 2020 року № 673-ос "Про призначення виконавців науково-дослідних робіт") науково-дослідної роботи "Сервісна діяльність органів публічної влади в умовах розвитку цифрового суспільства", державний реєстраційний номер 0119U101449.

Керівник науково-дослідної роботи,
д.держ.упр., доцент Олександр КАРПЕНКО

Директор Інституту
експертно-аналітичних
та наукових досліджень
д.держ.упр., доцент Ольга ПЕТРОЄ

Підпис Петроє О.І.
засвідчую
"25" 01 2021 р.
ВІДДІЛ РОБОТИ З ПЕРСОНАЛОМ